Biometric Antispoofing Methods: A Survey in Face Recognition

Article *in* IEEE Access · January 2014

DOI: 10.1109/ACCESS.2014.2381273

CITATIONS
225

READS
4,436

3 authors:

Javier Galbally
European Commission
131 PUBLICATIONS **3,424** CITATIONS
SEE PROFILE

Sébastien Marcel
Idiap Research Institute
222 PUBLICATIONS **7,296** CITATIONS
SEE PROFILE

Julian Fierrez
Universidad Autónoma de Madrid
607 PUBLICATIONS **9,247** CITATIONS
SEE PROFILE

IEEE Access
The journal for rapid open access publishing

Received November 6, 2014, accepted November 20, 2014, date of publication December 18, 2014, date of current version January 7, 2015.

Digital Object Identifier 10.1109/ACCESS.2014.2381273

Biometric Antispoofing Methods: A Survey in Face Recognition

JAVIER GALBALLY[1], SÉBASTIEN MARCEL[2], (Member, IEEE), AND JULIAN FIERREZ[3]

[1]Joint Research Centre of the European Commission, Institute for the Protection and Security of the Citizen, Ispra 21027, Italy
[2]Centre du Parc, IDIAP Research Institute, Martigny CH-1920, Switzerland
[3]Biometric Recognition Group, Escuela Politécnica Superior, Universidad Autonoma de Madrid, Madrid 28049, Spain

Corresponding author: J. Galbally (javier.galbally@jrc.ec.europa.eu)

This work was supported in part by the CAM under Project S2009/TIC-1485, in part by the Ministry of Economy and Competitiveness through the Bio-Shield Project under Grant TEC2012-34881, in part by the TABULA RASA Project under Grant FP7-ICT-257289, in part by the BEAT Project under Grant FP7-SEC-284989 through the European Union, and in part by the Cátedra Universidad Autonoma de Madrid-Telefónica.

ABSTRACT In recent decades, we have witnessed the evolution of biometric technology from the first pioneering works in face and voice recognition to the current state of development wherein a wide spectrum of highly accurate systems may be found, ranging from largely deployed modalities, such as fingerprint, face, or iris, to more marginal ones, such as signature or hand. This path of technological evolution has naturally led to a critical issue that has only started to be addressed recently: the resistance of this rapidly emerging technology to external attacks and, in particular, to spoofing. Spoofing, referred to by the term presentation attack in current standards, is a purely biometric vulnerability that is not shared with other IT security solutions. It refers to the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting a synthetic forged version of the original biometric trait to the sensor. The entire biometric community, including researchers, developers, standardizing bodies, and vendors, has thrown itself into the challenging task of proposing and developing efficient protection methods against this threat. The goal of this paper is to provide a comprehensive overview on the work that has been carried out over the last decade in the emerging field of antispoofing, with special attention to the mature and largely deployed face modality. The work covers theories, methodologies, state-of-the-art techniques, and evaluation databases and also aims at providing an outlook into the future of this very active field of research.

INDEX TERMS Biometrics, security, anti-spoofing, face.

I. INTRODUCTION

"Fingerprints cannot lie, but liars can make fingerprints". Unfortunately, this paraphrase of an old quote attributed to Mark Twain[1] has been proven right in many occasions now. And not only for fingerprints, but also for many other biometric traits such as face, iris, voice or even gait.

Every technology has its own time. Since the first pioneering works on automatic voice and face recognition over 40 years ago [1]–[3], steady and continuous progress has been made in the development of biometric technology. Driven by the very appealing new security biometric paradigm "*forget about cards and passwords, you are your own key*", researchers from many different fields such as image processing, computer vision or pattern recognition, have applied the newest techniques in each of these areas to improve the performance of biometric systems [4]. This path of technological evolution has permitted the use of biometrics in many diverse activities such as forensics, border and access control, surveillance or on-line commerce.

In this scenario of constant expansion, and as a consequence of its own natural progress, new concerns are arising regarding biometric technology different from the mere improvement of its recognition performance. Among these new issues and challenges that have emerged around biometrics, its resilience against external threats has lately drawn a significant level of attention.

Currently it is an accepted fact that, as the deployment of biometric systems keeps growing year after year in such different environments as airports, laptops or mobile phones, users are also becoming more familiar with their use in everyday life and, as a result, their security weaknesses are better

[1]Figures do not lie, but liars do figure.

known to the general public. Nowadays, it is not difficult to find websites with tutorial videos which give detailed guidance on how to create fake masks, fingerprints or irises that may be used to fool biometric systems.

Attacks are not any more restricted to a mere theoretical or academic sphere, but are starting to be carried out against real operational applications. The fairly easy hacking of the long anticipated new iPhone 5S fingerprint reader, just a day after it hit the shelves and using a regular and well-known type of fingerprint spoof [5], is only another example in the list of practical attacks and vulnerabilities of biometric systems that are being reported to the public from hacking groups attempting to get recognition [6]–[10], from real criminal cases [11]–[14], or even from live demonstrations at biometric and security specific conferences [15], [16].

As a consequence, in recent years, there has been an increasing interest on the evaluation of biometric systems security, which has led to the creation of numerous and very diverse initiatives focused on this field of research [17], [18]: publication of many research works disclosing and evaluating different biometric vulnerabilities [19]–[24]; proposal of new protection methods [25]–[28]; related books and book chapters [29]–[31]; PhD and MSc Theses which propose and analyse different biometric spoofing and anti-spoofing techniques [32]–[39]; publication of several standards in the area [40]–[42] and of different Supporting Documents and Protection Profiles in the framework of the security evaluation standard Common Criteria for the objective assessment of commercial systems [43], [44]; certification of different commercial products in the framework of the Common Criteria [45]–[47]; patented anti-spoofing mechanisms for biometric systems [48]–[50]; specific tracks, sessions and workshops in biometric-specific and general signal processing conferences [51]–[53]; organization of competitions focused on vulnerability assessment [54]–[56], acquisition of specific datasets [57]–[59]; creation of groups and laboratories specialized in the evaluation of biometric security [60]–[62]; European Projects with the biometric security topic as their main research interest [63], [64].

All these initiatives clearly highlight the effort put by all parties involved in the development of biometrics (i.e., researchers, developers and industry) to improve the systems' security in order to bring this technology to comparable deployment levels to other well established security-related solutions.

Among the different vulnerabilities analyzed, intensive research efforts have been focused on the study of *direct* or *spoofing* attacks. Spoofing is a purely biometric vulnerability that is not shared with other IT security solutions. In these attacks, intruders use some type of synthetically produced artefact (e.g., face mask, gummy finger or printed iris image) or try to mimic the behaviour of genuine users (e.g., gait, signature), to fraudulently access the biometric system. This way, *spoofing* takes advantage of the fact that our fingerprints, face, iris, voice or even our DNA, are publicly available data. This is one of the well-known drawbacks of biometrics: ''*biometric traits are not secrets*'' [6], [65]–[67].

Such public dimension of biometrics is one of the main reasons why spoofing has attracted a lot of interest not only from researchers but also from general users who are seduced by the ''do-it-yourself'' nature of these attacks. It is precisely this characteristic that renders spoofing really dangerous, as it transforms every user into a potential attacker.

The public, low-cost and low-tech features of spoofing are well reported in the literature, where it has been shown in different works that many, if not all, biometric modalities are vulnerable to this threat [59], [68]–[76]. Therefore, nowadays the question is not any more whether or not biometrics can be copied or forged, but rather to what extent systems are robust to these attacks and if they incorporate the necessary countermeasures to detect them. However, counterfeiting this type of threats is not a straight forward problem. As they are performed in the analog domain and interaction with the acquisition device is done following the regular protocol, usual digital protection mechanisms are not effective (e.g., encryption, digital signature or watermarking). As a result, specific countermeasures that allow biometric systems detecting fake samples and rejecting them have to be developed.

The spoofing biometric security context described above has promoted in the last 10 years a significant amount of research which has resulted in publications in journals, conferences and media, describing new anti-spoofing algorithms and systems that intend to make this technology safer. This has been specially the case for some of the most deployed, popular and mature modalities such as face, fingerprints and iris, which have also been shown to be the most exposed to spoofing. At the moment, the amount of new contributions and initiatives in the area of anti-spoofing requires a significant condensation effort to keep track of all new information in order to form a clear picture of the state-of-the-art as of today. As an example, a series of chronological milestones related to the evolution of biometric spoofing are shown in Fig. 1. We are aware that there are other works that merit being included in the diagram, however, due to space restrictions, we have focused on those that, from our point of view, can better help the reader to see the progress of anti-spoofing algorithms both from a technological and a performance perspective.

Similarly to what has been recently published for the fingerprint modality [77]–[79], the current article is an attempt to contribute to this difficult review task. It presents a comprehensive survey of anti-spoofing methodologies proposed until mid 2014 in the widely used face modality, following a systematic categorization. It also provides an overview of publicly available evaluation benchmarks for face anti-spoofing approaches, summarizing the detection rates achieved by state-of-the-art methods in the international competitions that have been organized up to date. The article concludes with an outline of the lessons learnt in these more than 10 years of intensive anti-spoofing research, and with a personal vision of

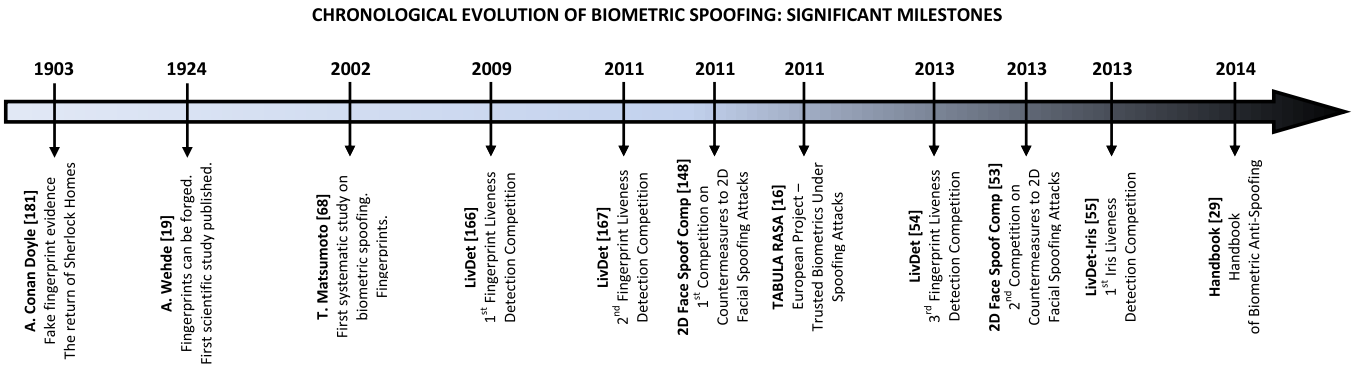


FIGURE 1. **Chronological evolution of biometric spoofing and anti-spoofing with a series of significant milestones that have been covered in this field so far. All events are referenced throughout the article.**

the challenges to be faced and possible future research lines that may contribute to the general improvement of the security level offered by biometric systems against spoofing.

In brief, the paper is thought as a tool to provide biometric researchers, either newcomers or experts in security related aspects of this technology, an overall picture of the current panorama in biometric anti-spoofing with special focus on the face trait. It also aims at presenting the current strengths, shortcomings and challenges of these security protection techniques. Although the work is thought to be self-contained, some previous general knowledge on biometrics can help to better understand some of the concepts introduced in the article.

The rest of the paper is structured as follows. In Sect. II some general anti-spoofing concepts are summarized and the techniques classification that will be followed throughout the paper is presented. In Sect. III the reader can find a comprehensive survey of the different research works that have been presented until mid 2014 in face anti-spoofing. Sect. IV addresses the important issue of anti-spoofing evaluation and presents the datasets that are publicly available for this purpose in the face modality. To conclude, the summary and discussion, with some insight into the future, are given in Sect. V.

II. BIOMETRIC ANTI-SPOOFING

In spite of some ongoing efforts and proposals to reach a unified and standardized nomenclature for vulnerability related concepts, the biometric community has still not reached a general agreement on the best terminology to be used in each case [42], [80], [81].

In light of the absence of a closed definition, the present article will follow the specialised literature where *biometric spoofing* is widely understood as the ability to fool a biometric system into recognizing an illegitimate user as a genuine one by means of presenting to the sensor a synthetic forged version (i.e., artefact) of the original biometric trait. Such attacks, also referred to in some cases as *direct* attacks [33] fall within the larger category "presentation attacks", defined in the latest draft of the ISO/IEC 30107 standard as "*presentation of an artefact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system*" [42]. Such a wider group of attacks also includes the presentation to the acquisition device of human characteristics (and not only synthetic artefacts) such as dead fingers, mutilated traits, real living traits under coercion or a different living trait (i.e., *zero-effort* impostor attempts that try to take advantage of the False Acceptance Rate, FAR, of biometric systems) [80].

Therefore, spoofing consists in using an artificial trait to impersonate a different user or to create a new genuine identity. Several scenarios are typically conceived for spoofing attacks depending on the type of biometric system considered. (*i*) Verification system: In the most common case, spoofing is carried out at the time of authentication by presenting to the sensor a fake physical copy of the genuine's user trait. Such artefact is acquired and matched to the enrolled real template of the genuine user. (*ii*) Verification system/Identification system in closed set: Spoofing may also be performed at the enrolment stage by generating a new identity with an artefact (not necessarily imitating any real user's trait) which can later be used by different users to access the system. (*iii*) Identification system in open set: Typically this case corresponds to look-up systems where a new identity is created using the spoofing artefact to avoid being found in a watch list (e.g., to obtain a VISA for illegally entering a country).

Given the above spoofing definition, an *anti-spoofing* method is usually accepted to be any technique that is able to automatically distinguish between real biometric traits presented to the sensor and synthetically produced artefacts containing a biometric trait. As in the spoofing case, although it is a very extended one, this nomenclature is not carved in stone and, very often, anti-spoofing approaches are also referred to in the literature by the terms *liveness detection* or *vitality detection* techniques. Rigorously speaking, both terms (i.e., anti-spoofing and liveness detection) are not fully equivalent, as not all anti-spoofing methods are necessarily based on cues directly related to living features of biometric traits. However, in practice, they are used as synonyms in the majority of cases. Therefore, in the present article we will not

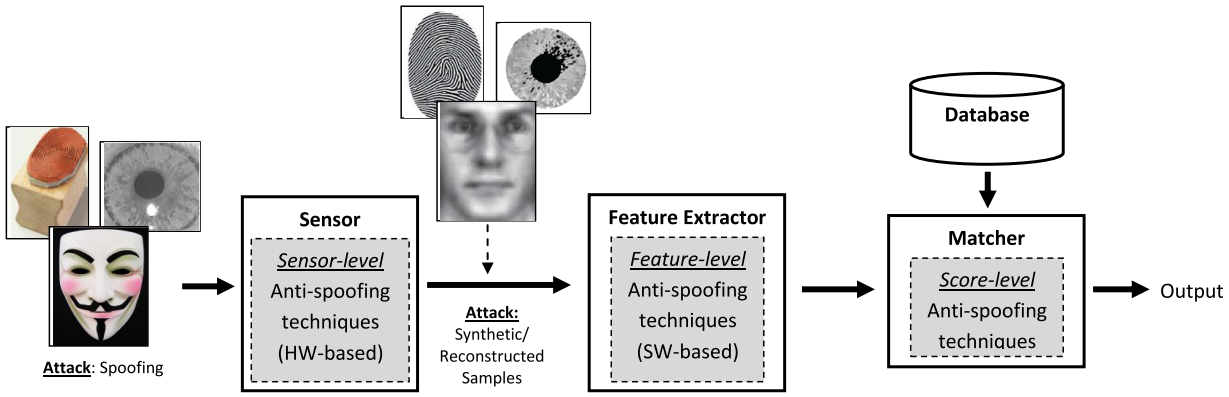


FIGURE 2. General diagram of a biometric system specifying the modules where the three types of anti-spoofing techniques may be integrated (sensor-level, feature-level and score-level). Also displayed are the two different type of attacks for which anti-spoofing techniques may offer protection: spoofing and attacks carried out with synthetic or reconstructed samples.

make any difference between them. It is also worth noting that certain anti-spoofing techniques may also be highly effective to detect other types of presentation attacks (e.g., dead or mutilated traits).

Anti-spoofing methods represent a challenging engineering problem as they have to satisfy certain demanding requirements [82]: (*i*) non-invasive: these techniques should in no case be harmful or require an excessive contact with the user; (*ii*) user friendly: users should not be reluctant to interact with them; (*iii*) fast: results should be generated in a reduced lapse of time as users' interaction with the sensor should be kept as short as possible; (*iv*) low cost: wide use cannot be expected if the cost is excessively high; (*v*) performance: in addition to a good fake detection rate, the protection scheme should not degrade the recognition performance of the biometric system (e.g., false rejection).

From a general perspective, anti-spoofing techniques may be classified into one of three groups depending on the biometric system module in which they are integrated (see Fig. 2):

- **Sensor-Level Techniques**. Usually referred to in the literature by the term *hardware-based* techniques. These methods add some specific device to the sensor in order to detect particular properties of a living trait (e.g., facial thermogram, blood pressure, fingerprint sweat, or specific reflection properties of the eye). As shown in Fig. 2, such techniques are integrated in the biometric sensor. In general, hardware-based approaches measure one of three characteristics, namely: (*i*) intrinsic properties of a living body, including physical properties (e.g., density or elasticity), electrical properties (e.g., capacitance, resistance or permittivity), spectral properties (e.g., reflectance and absorbance at given wavelengths) or even visual properties (e.g., colour and opacity); (*ii*) involuntary signals of a living body which can be attributed to the nervous system. Good examples are the pulse, blood pressure, perspiration, pupillary unrest (hippus), brain wave signals (EEG) or electric heart signals; (*iii*) responses to external stimuli, also known as *challenge-response* methods, which require the user cooperation as they are based on detecting voluntary (behavioural) or involuntary (reflex reactions) responses to an external signal. Examples of such methods can be the pupil contraction after a lighting event (reflex), or the head movement following a random path determined by the system (behavioural).
  In the present work multibiometric techniques are included in this category [34], [83], [84], although, in some cases, they could reasonably be classified as well in the feature-level methods (described next). Multibiometric anti-spoofing is based on the hypothesis that the combination of different biometrics will increase the robustness to direct attacks, as, in theory, generating several fake traits is presumed to be more difficult than an individual trait. Following this assumption, multimodal approaches fuse different modalities. Generally, the strategy followed is to use complementary traits in terms of performance and vulnerabilities. Accordingly, very accurate traits vulnerable to spoofing (e.g., fingerprints) are combined with traits robust to spoofing with low recognition rates (e.g., the finger vein pattern). Such a strategy requires additional hardware acquisition devices, therefore these techniques may be included in the sensor-level group of anti-spoofing methods. Note that the above hypothesis (i.e., circumventing a multibiometric system implies breaking all unimodal modules) has already been shown to be untrue as, in many cases, bypassing just one of the unimodal subsystems is enough to gain access to the complete application [75], [85]–[88]. Therefore, multibiometry by itself does not necessarily guarantee a higher level of protection against spoofing attacks. As such, specific protection schemes for multibiometric systems have started to be recently studied [32], [89].
- **Feature-Level Techniques**. Usually referred to in the literature by the term *software-based* techniques. In this case the fake trait is detected once the sample has been

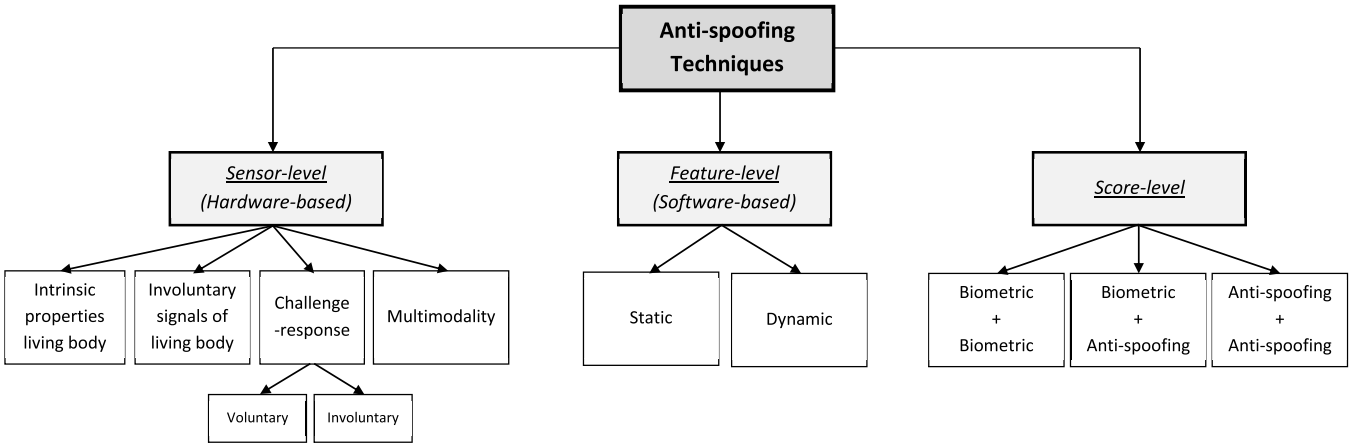


FIGURE 3. General classification of anti-spoofing methods considered in the present article with the three main groups depicted in Fig. 2: sensor-level, feature-level and score-level techniques.

acquired with a standard sensor. As such, features used to distinguish between real and fake traits are extracted from the *biometric sample* (usually images, as in the case of face, or some kind of time-functions, as in the case of speech), and not directly from the human body as in the case of sensor-level techniques. These methods are integrated after the sensor, usually functioning as part of the feature extractor module (as shown in Fig. 2). They can be further classified into *static* and *dynamic* anti-spoofing methods, depending on whether they work with only one instance of the biometric trait, or with a sequence of samples captured over time [90]. Although they may present some degradation in performance, in general, static features are preferable over dynamic techniques as they usually require less cooperation from the user, which makes them faster and less intrusive. Such a subdivision into static and dynamic approaches is of special interest in face recognition, where there exist systems working on single facial images (e.g., passport picture) and on video sequences (e.g., surveillance camera).

Although, for clarity, multimodality will be considered in the article as a sensor-level type of anti-spoofing countermeasure, some of these approaches can also be included in the present group. For instance, from just one single high resolution image of a face we may perform both face and iris recognition. In this particular case, a multimodal strategy is being applied at the feature extractor level, with no need of any additional hardware or sensing device.

An appealing characteristic of software-based techniques is that, as they operate directly on the acquired sample (and not on the biometric trait itself), they are potentially capable of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks. For instance, feature-level methods can protect the system against the injection of reconstructed or synthetic samples[2] into the communication channel between the sensor and the feature extractor as depicted in Fig. 2 [91]–[93].

- **Score-Level Techniques**. Recently, a third group of protection methods which falls out of the traditional two-type classification (software- and hardware-based), has started to be analyzed in the field of fingerprint anti-spoofing. These protection techniques, much less common than the previous two categories, are focused on the study of biometric systems at *score-level* in order to propose fusion strategies that increase their resistance against spoofing attempts. Due to their limited performance, they are designed as supplementary measures to the sensor-level and feature-level techniques presented above, and are usually integrated in the matcher (as shown in Fig. 2). The scores to be combined may come from: *i*) two or more unimodal biometric modules; *ii*) unimodal biometric modules and anti-spoofing techniques; or *iii*) only results from anti-spoofing modules.

A graphical diagram of the categorization proposed above is given in Fig. 3. Although the present article will follow this three-group taxonomy, this is not a closed classification and some techniques may fall into one or more of these groups (e.g., as already mentioned, some multibiometric methods could be a good border-line example). Nonetheless, we believe that this taxonomy can help to get a clearer picture of the current biometric anti-spoofing scene. As well, the reader should be aware that, even though this is a quite extended and accepted classification, others are also possible.

It is also worth highlighting that the three types of anti-spoofing approaches presented here are not exclusive, and may be coupled in order to improve the overall security of the system. In fact, the two most deployed methods described above (hardware- and software-based), have certain

[2]Please note the difference between a synthetic *artefact* (physical) used in spoofing attacks, and a synthetic *sample* (digital)

IEEE Access
The journal for rapid open access publishing

TABLE 1. Coarse comparison between the types of anti-spoofing techniques considered in the work (see Fig. 3) according to their general compliance with the requirements defined in [82]. The last column shows the potential ability of anti-spoofing techniques to detect eventual non-spoofing attacks such as the ones carried out with synthetic or reconstructed samples as shown in Fig. 2.

High-level comparison of anti-spoofing techniques						
Type	Subtype	Performance	Low-cost	User friendly	Non-invasive	Protection vs other attacks
Sensor-level	Intrinsic properties	++	+	-	-	-
	Involuntary signals	++	-	-	-	-
	Challenge response	++	-	-	-	-
	Multimodality	+	-	+	+	-
Feature-level	Static	+	+	+	++	+
	Dynamic	+	+	-	-	+
Score-level	Biom. + Biom.	- -	+	+	++	-
	Biom. + Anti-Spoof.	- -	+	+	++	-
	Anti-Spoof. + Anti-Spoof.	- -	+	+	++	-

advantages and drawbacks so that, in general, a combination of both would be the most desirable protection strategy to increase the security of biometric systems. As a coarse comparison, sensor-level schemes usually present a higher fake detection rate, while feature-level techniques are in general less expensive (as no extra device is needed), less intrusive and more user-friendly since their implementation is transparent to the user. As already mentioned, score-level protection techniques present a much lower performance and are designed only to support sensor- or feature-level protection measures.

As general reference, Table 1 presents a comparative summary, for the three classes considered in the article, of some of the most relevant characteristics that are desirable in anti-spoofing protection schemes [82]. The table should be understood only as a very broad indication of their capabilities. Therefore, in practice, a specific individual study should be carried out for each proposed anti-spoofing algorithm in order to determine its level of compliance with each of these features.

In the following, as a concrete and very representative example of the research carried out in the field of spoofing, we present a comprehensive review of the most successful and popular anti-spoofing methods which have been proposed in the literature for the face biometric.

III. STATE-OF-THE-ART IN FACE ANTI-SPOOFING

Two main reasons have driven us to select the face biometric as the focal point of the present anti-spoofing survey:

- On the one hand, according to the International Biometric Group (IBG), face is the second most largely deployed biometric at world level in terms of market quota right after fingerprints [94]. It is also adopted in most official identification documents such as the ICAO-compliant biometric passport [95] or national ID cards [96]. As such, nowadays face is one of the biometric traits with the highest potential impact both from an economic and a social point of view.
- On the other hand, together with the fingerprint trait, it is very likely the biometric where most spoofing-related research has been conducted, leading to a very large amount of published works. However, unlike in the fingerprint case [77]–[79], there is still no rigorous and comprehensive survey covering all the anti-spoofing methods proposed in the field of face recognition. The current article attempts to fill this gap.

Before reviewing the different works that have been proposed as protection methods against direct attacks, a brief summary of the most common face spoofing techniques is presented. This initial short overview on spoofing can be useful to understand the rationale behind the design of some anti-spoofing techniques later presented and also to understand the structure of the evaluation databases described in Sect. IV.

A. FACE SPOOFING

The use of masks or facial disguises to avoid being recognized is a practice which has been observed for centuries in the vast majority of known civilizations. Following this trend, probably the most modern version of this long-going tradition to change oneself's physical appearance, is the use of plastic surgery, which is becoming more and more popular thanks to the availability of advanced technology, its affordable cost, and the speed with which these procedures are now performed. Recently, it has been shown that, in spite of some efforts to develop specific algorithms robust to facial surgery changes [97]–[99], the problem of recognizing a person after undergoing this type of operations is still an open challenge for automatic face authentication systems [100]. Even without turning to irreversible treatments, some works have also shown that face-based biometric systems may be circumvented just by wearing regular make-up [101].

The afore mentioned techniques (i.e., face masks, plastic surgery and make-up) are usually used to hide the user's own identity (i.e., Bob denies being Bob) and not to perform an attack in which Bob tries to impersonate John. However, it has recently been shown at a live demonstration in a biometric-dedicated conference that this security scenario could change, and that methods such as surgery or make-up may be successfully used to perform direct attacks. In this conference, a female intruder was able to access a face recognition system in the place of a male user just by wearing some adequate make-up [16].

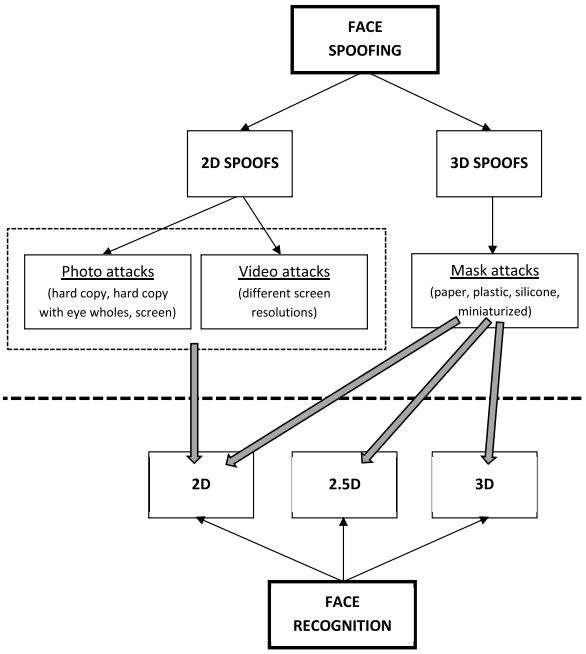


FIGURE 4. General classification of face spoofing techniques studied in the literature. Grey arrows indicate the face recognition technology for which each attack represents a potential threat.

Apart from these still limited examples on the potential use of disguise techniques for spoofing purposes, the vast majority of face direct attacks reported in the literature may be classified in one of two groups, as shown in Fig. 4, depending on whether the artefacts used are: *i*) 2D surfaces (e.g., photo, video) which are successful against 2D face recognition systems (see grey arrows in Fig. 4), or *ii*) 3D volumes (e.g., masks) which may be used to attack 2D, 2.5D and 3D face recognition technology. Such artefacts have been used to carry out three main types of attacks which present an increasing level of spoofing potential:

- **Photo Attacks**. These fraudulent access attempts are carried out presenting to the recognition system a photograph of the genuine user. The photograph may have been taken by the attacker using a digital camera, or even retrieved from the internet after the user himself uploaded it to one of the very popular online social networks available today [67].
  The image can then be printed on a paper (i.e., print attacks, which were the first to be systematically studied in the literature) or may be displayed on the screen of a digital device such as a mobile phone or a tablet (i.e., digital-photo attacks) [15], [59], [102]. A slightly more advanced type of photo-attack that has also been studied is the use of photographic masks. These masks are high resolution printed photographs where eyes and mouth have been cut out. At the time of the attack the impostor is placed behind [103], so that certain face movements such as eye blinking are reproduced.
- **Video Attacks**. Also referred in some cases as *replay attacks*. They represent a more sophisticated version of the simple photo spoofs. In this case, the attacker does not use a still image, but replays a video of the genuine client using a digital device (e.g., mobile phone, tablet or laptop) [104], [105]. Such attacks appeared as a further step in the evolution of face spoofing and are more difficult to detect, as not only the face 2D texture is copied but also its dynamics.
- **Mask Attacks**. In these cases the spoofing artefact is a 3D mask of the genuine client's face, increasing the difficulty to find accurate countermeasures against them. Since the complete 3D structure of the face is imitated, the use of depth cues which could be a solution to prevent the previous two types of attacks (carried out with flat surfaces), becomes inefficient against this particular threat.
  Although the possibility to bypass a biometric system wearing a mask imitating the face of a different user is an idea that has been circulating for some time [106], these attacks are far less common than the previous two categories. Face-mask spoofing has only started to be systematically studied with the acquisition of the first mask-specific datasets [107], [108], which include masks of different materials and sizes [109], [110].
  In part, the scarcity of research works addressing this potential threat may be put down to the technical and economic difficulty posed by the generation of large databases of realistic masks. However, these obstacles have been significantly lessened with the recent emergence of some companies where such 3D face models may be obtained for a reasonable price.[3] Furthermore, self-manufacturing a face mask is also becoming more feasible and easier each day with the new generation of affordable 3D acquisition sensors,[4] dedicated scanning software[5] and the price decrease of 3D printing devices.[6]

All previous attacks have a number of variants depending on the resolution of the spoofing device, the type of support used to present the fake copy (e.g., handheld or fixed support), or the external variability allowed (e.g., illumination or background conditions). These different attack versions may be found in the face spoofing databases available for research [54], [59], [102], [105], [107], [108], [111], which are reviewed in Sect. IV-C.

It is also worth highlighting that face recognition systems may also be subjected to attacks from identical twins claiming to be the same person. Strictly speaking these are not spoofing attacks (as there is no physical artifact involved) but rather zero-effort impostor attempts in which Bob presents his own biometric trait while trying to access the system as John. Although some of the anti-spoofing techniques that will be reviewed in the following sections could potentially be used against this particular vulnerability, it will not be treated in

[3] www.thatsmyface.com; https://shapify.me; www.sculpteo.com
[4] http://en.wikipedia.org/wiki/Kinect; http://en.wikipedia.org/wiki/PrimeSense
[5] www.skanect.com; www.kscan3d.com; www.fablitec.com
[6] www.sharebot.it/; http://cubify.com

the present article. We refer the interested reader to some specific works on this topic to understand the implications and performance of face recognition systems in the presence of twins [112]–[115].

B. FACE ANTI-SPOOFING

Although the first face anti-spoofing works date back more than a decade [129], it has not been until the last three years that this technology has experimented a real revolution under the umbrella of the TABULA RASA European project focused on the study of spoofing attacks to biometric systems [64]. Another decisive factor for the development of new protection methods against direct attacks has been the acquisition and distribution of several public face spoofing databases, that have made possible for researchers to focus on the design of efficient countermeasures and not on data acquisition issues [102], [104], [105], [107]. Both factors have fostered the recent publication of multiple techniques in 2D face anti-spoofing and to initiate a promising research line in new protection algorithms for 3D face recognition systems against mask attacks.

In the next sections we review the works that have addressed so far the challenging problem of face anti-spoofing. To this end, we follow the general categorization presented in Sect. II and depicted in Fig. 3. As overall reference, the advantages and drawbacks of each general group of techniques are summarized in Table 3. However, to understand the specific potential uses of every particular algorithm readers are referred to corresponding works.

As may be seen in Table 3, it is difficult to clearly select one technique over the others, as their performance is highly dependent on the attacks and the use case considered. It is commonly observed that anti-spoofing methods fail to perform consistently across databases, experimenting a significant loss of accuracy when they are tested under different conditions to those for which they were designed. As such, usually the best results are achieved through the combination of several complementary algorithms or features, so that the weaknesses of some are covered by the strengths of others and viceversa [54], [130].

1) FACE ANTI-SPOOFING: FEATURE LEVEL DYNAMIC APPROACHES

One of the pioneer feature-level protection approaches in 2D face recognition appeared as a countermeasure to the first attacks studied which made use of static face printouts (i.e., print attacks). Such anti-spoofing techniques, which still remain quite popular against print attacks, rely on the detection of motion over a face video sequence. In particular, they are based on the trajectory analysis of specific face segments. Such dynamic features reveal valuable information to discriminate between real faces and spoofed static copies. Typical cues used in this type of anti-spoofing methods, some of them involving challenge-response strategies, are: eye blinking [119], [123], [131]–[133]; face and head gestures (e.g., nodding, smiling, looking in different directions) detected trough face and gaze tracking [134], [135] or through optical flow estimation [27], [103], [136], [137]. These techniques are usually highly effective to detect photo-attacks but lose accuracy against illegal access attempts carried out with replayed videos where not only the face appearance but also its movements are forged.

In order to overcome this shortcoming, some dynamic liveness detection techniques have been specifically proposed to detect video-based attacks: exploiting the 3D structure of the face through the analysis of several 2D images with different head poses [124], [138]; using context-based analysis in order to take advantage of non-facial information available from acquired samples such as motion features from the scene (e.g., background *vs* foreground motion) [59], [139]–[141]; estimating the noise produced during the recapturing process (i.e., fixed pattern noise and the noise resulting from the photo-responsiveness of non-uniform light-sensitive cells) [142]; using modified versions of the popular Local Binary Patterns (LBP), in order to take into account temporal information present in video sequences [125] or to analyse the dynamics of facial texture in comparison to rigid objects such as photos or masks [143]; applying the recently proposed Eulerian video magnification algorithm to enhance motion in video as a previous step to anti-spoofing feature extraction [126].

Given that they are designed to exploit both spatial and temporal information of face videos, dynamic-based anti-spoofing schemes usually achieve very competitive performance. However, as a limitation, they cannot be used in systems where only a single face image of the user is available (e.g., passport related applications). Moreover, even in scenarios where video data has been recorded (e.g., surveillance applications), it is not rare to find that only a very few non-consecutive frames are suitable for facial analysis, which also limits their final use and accuracy.

2) FACE ANTI-SPOOFING: FEATURE LEVEL STATIC APPROACHES

As mentioned on the previous section, dynamic anti-spoofing schemes need a temporal face sequence of sufficient duration to achieve high accuracy. This restriction has motivated the appearance of a second group of approaches for the detection of spoofing access attempts to 2D face recognition systems, focused on the analysis of a single static image and not of video data. These techniques are in general faster than their dynamic counterparts and, therefore, more convenient for the user, at the cost, in some cases, of a certain performance loss.

The vast majority of feature-level static methods are based on the analysis of the face texture using different image processing tools such as: the Fourier Spectrum [144]; multiple Difference of Gaussian (DoG) filters to extract specific frequency information [105] which has also been combined with features obtained from the Lambertian model [102] proving remarkable performance even under bad illumination conditions [111]; partial least squares to analyse specific information from low-level descriptors [145];

TABLE 2. Summary of the most relevant face anti-spoofing techniques presented in Sect. III. Column "subtype" shows the algorithm subtype within each of the three main categories considered in the work (sensor-level, feature-level and score-level) as shown in the taxonomy in Fig. 3. Column "attack" refers to the type of face spoofing attacks considered in the work as defined in Sect. III-A: photo, video or mask attacks. for clarity, public databases are just referenced the first time they appear in the table, in successive entries only their name is given (for further information on these public databases please see Sect. IV-C). Database sizes that appear in column "database" are approximate and are given just as an indication of their order of magnitude (for the exact structure and size the reader should consult the corresponding reference). The same applies for results, as the ones shown in the table are an approximation of the different scenarios considered in each work. Works are ordered chronologically within the same subtype.

Face anti-spoofing techniques: General overview					
Sensor-Level techniques					
Reference	**Subtype**	**Features and methodology**	**Attack**	**Database**	**Error**
2005, Chetty and Wagner [116]	Multibio.	Face + Voice	Video	Public, VidTIMIT DB [117] (43 identities, 500 samples) and UCBN DB [118] (30 identities, 30 samples)	2%
2008, Kollreider et al. [119]	Challenge-response	Motion detection	Photo, Video	Proprietary, 15 identities, 390 samples	3.5%
2011, Zhang et al. [120]	Intrinsic prop-erty	Reflectance using multispectral lighting in 2D images	Photo, Video, Mask	Proprietary, 40 identities, 1,000 samples	7%
2013, Kose and Dugelay [121]	Intrinsic prop-erty	Reflectance in 3D scans	Mask	Proprietary, 20 identities, 400 samples	5.5%
2013, Dhamecha et al. [122]	Invol. body signal	Thermal images	Mask	Public (still to be released), 75 identities, 1,362 samples	13%
Feature-Level techniques					
Reference	**Subtype**	**Features and methodology**	**Attack**	**Database**	**Error**
2007, Pan et al. [123]	Dynamic	Eye blink detection using Conditional Random Fields (CRF)	Photo	Public, NUAA Photograph Imposter DB [102], 15 identities, 75 samples	2%
2009, Kollreider et al. [27]	Dynamic	Face motion detection using Optical Flow of Lines (OFL)	Photo	Proprietary, 100 identities, 800 samples	0.5%
2011, Anjos et al. [59]	Dynamic	Context-based using correlation between face motion vs background motion	Photo	Public, PRINT-ATTACK DB [59], 50 identities, 400 samples	10%
2012, Marsico et al. [124]	Dynamic	3D structure inferred from 2D images using geometric invariants	Photo	Public, NUAA Photograph Imposter DB	0.3%
2012, Freitas et al. [125]	Dynamic	Dynamics of the facial texture using LBPs	Photo, Video	Public, REPLAY-ATTACK DB [104], 50 users, 1,000 samples	7.5%
2013, Bharadwaj et al. [126]	Dynamic	Motion detection using Histogram of Oriented Optical Flows (HOOF) after video Eulerian magnification	Photo, Video	Public, REPLAY-ATTACK DB	1.25%
2010, Tan et al. [102]	Static	Face texture using the Lambertian model	Photo	Public, NUAA Photograph Imposter DB	15%
2012, Zhiwei et al. [105]	Static	Face texture frequency analysis using Difference of Gaussians (DoG) filters	Photo, Video	Public, CASIA Face Anti-Spoofing DB [105], 50 identities, 600 samples	15%
2012, Chingovska et al. [104]	Static	Face texture using LBPs	Photo, Video	Public, REPLAY-ATTACK DB, NUAA Photograph Imposter DB, CASIA Face Anti-Spoofing DB	15%
2012, Maatta et al. [127]	Static	Texture + Shape combining LBPs + Gabor Wavelets + HOG	Photo	Public, NUAA Photograph Imposter DB, REPLAY-ATTACK DB, YALE-RECAPTURED DB [111] (10 users, 2,500 samples)	0.5%
2013, Komulainen et al. [128]	Static	Context-based using upper body and spoof support detection	Photo, Video	Public, NUAA Photograph Imposter DB, CASIA Face Anti-Spoofing DB	3%

TABLE 3. Coarse comparison of the advantages and drawbacks of the three main groups of face spoofing countermeasures reviewed in Sects III-B.1, III-B.2 and III-B.3. The table should be understood only as a very general reference. for specific details on a particular algorithm the reader should refer to the corresponding reference.

	Advantages	Drawbacks
Feature-level dynamic	Exploit video spatial and temporal features High accuracy Very effective against photo-attacks	Not usable in single face image scenarios (e.g., passports) Slow Lose accuracy against video attacks
Feature-level static	Usable with single image or video Fast Totally transparent to the user	Based only on image spatial information Lower accuracy
Sensor-level	Can be effective against photo, video and mask attacks Very high accuracy	Expensive Usually slower Higher level of cooperation required

combination of low-level and high-level face component descriptors [146]; a recent trend based on the use of Local Binary Patterns (LBP) to detect photo-attacks [104], [147], which has been successfully combined with other texture descriptors such as Gabor Wavelets and with shape related information extracted using Histogram Oriented Gradients (HOG) in [127]; detection of paper microtextures present in print-attacks either by analysing the specular components of the facial image [148] or by using LBPs as features [104], [149]; as in the case of video sequences, context-based approaches have also been proposed for the static scenario, focusing in this case on the detection of the user's upper body and the attack support (e.g., paper or tablet) [128]; or pixel difference evaluation between two consecutive pictures taken with different focus values [150] (although this last method requires two different face images, we include it in the static category as it does not use any temporal information).

These static-based anti-spoofing approaches may as well be applied to the case in which a video sequence is available. In this scenario, the analysis is performed on a frame-by-frame basis, using fusion techniques (e.g., majority voting) in a later stage to combine the individual scores obtained from each frame in order to generate a unique final decision. Although such a strategy is feasible, in general, it is less efficient than the schemes specifically designed to work with videos, as no temporal information is exploited (e.g., trajectories of facial features).

Some of the previous techniques have been successfully fused at feature level showing improved accuracy compared to individual parameters [119], [151]. A comparative study of several of these dynamic and static approaches may be found in the 2011 and 2013 Competitions on Countermeasures to 2D facial spoofing attacks [54], [130], where it was shown that, wherever possible (i.e., scenarios with availability of facial video data), the feature-level fusion of both types of techniques (static and dynamic) draws the best performance. Further reading on the results and databases used in these competitions may be found in Sect. IV-C.

3) FACE ANTI-SPOOFING: SENSOR LEVEL APPROACHES

Regarding sensor-level anti-spoofing techniques, the number of contributions is still not comparable to that of software-based approaches. However, some interesting methods have been proposed base on imaging technology outside the visual spectrum, such as: complementary infrared (IR) or near infrared (NIR) images, which are even claimed to provide sufficient information to distinguish between identical twins [129], [152]; comparing the reflectance information of real faces and fake materials using a specific set-up of LEDs and photodiodes at two different wavelengths [106], [120].

In addition to the previous works, there are other technologies, initially proposed for personal authentication purposes, that could also be used as sensor-level anti-spoofing techniques. Although in most cases no rigorous study has yet been carried out regarding their performance under liveness detection scenarios, such potentially useful mechanisms for face anti-spoofing would include: thermal imaging [153], [154], detection of the facial vein pattern [155], or 3D face acquisition [156]. For instance, 3D sensors can be very robust against attacks carried out with flat surfaces (e.g., photo or video attacks) as almost no depth difference is detected compared to real faces. On the other hand, their performance under mask-attacks has just started to be investigated using texture analysis inspired on 2D protection methods based on LBPs [157], [158] and also on the analysis of the reflectance components that can be computed from 3D scans [121]. Similarly, systems based on the detection of the face thermogram would be, in principle, very accurate detecting all three types of major face spoofing attacks (i.e., photo, video and mask attacks), as no thermal difference is expected in fake faces. Some initial efforts to study thermal imaging for liveness detection have already been carried out [159], including the acquisition of a significantly large database of thermal images for standard and disguised access attempts where very promising results have been obtained [122]. Still, it would be necessary to capture further face thermogram data under normal operational conditions and under spoofing attacks in order to validate these initial findings.

The fact that these techniques (i.e., 3D and thermal face recognition) already present solid backgrounds for personal authentication, can become an added advantage for their development as security enhancing alternatives, since both tasks (i.e., recognition and anti-spoofing) could be performed from the same sample.

Multimodality has also been explored as a sensor-level liveness detection approach. Many multibiometric anti-spoofing techniques consider the combination of face

and voice, as they are two easily measurable traits. Such methods exploit the correlation between the lips movement and the speech being produced [116], [160]–[162] or use specific information obtained from the lip movement in the utterance of a preassigned pin code [163].

The latter method could also be classified in the challenge-response category, as the user is asked to respond to a system command. Other studied challenge-response strategies consider voluntary eye blinking and mouth movement following a request from the system [119] (included in the present survey among the feature-level dynamic-based approaches, see Sect. III-B.1).

4) FACE ANTI-SPOOFING: SCORE LEVEL APPROACHES

Recently, some research has also been carried out in the field of score-level anti-spoofing strategies for 2D face recognition systems. In one of these first works, the authors study the impact of anti-spoofing measures on the performance of practical face recognition systems. To this end, they analyse different score fusion techniques for the protection and authentication modules under a three-case classification scenario: clients, impostors and spoofing attacks [164]. In addition, several fusion strategies for the combination of outputs from anti-spoofing modules have been analysed in order to reduce the performance gap that can be observed when the evaluation database is changed [165]. Following a similar trend, the combination of scores given by dynamic-based and static-based anti-spoofing approaches has also been considered in [66] and [67], showing a very significant improvement with respect to the individual systems, even for simple classifiers.

In order to give a general overview of the different methods studied so far in face anti-spoofing, Table 2 presents a summary of some illustrative works referenced in the present section. The table should be understood as a tool for quick reference and in no case as a strict comparative study, since results shown in the last column have been obtained on different databases. The objective of the table is to schematically show the most relevant characteristics (i.e., type of anti-spoofing system, type of features used, evaluation database, results, etc.) of several representative articles, in order to help readers to gain, at a glance, an overall perspective of the different approaches studied so far in the field of face anti-spoofing. For an exhaustive and complete list of all published articles in the area the reader should refer to the inline text in this Sect. III.

For further details on anti-spoofing evaluation, large publicly available datasets and comparative results from the face anti-spoofing competitions organized so far, readers are referred to Sect. IV.

IV. ANTI-SPOOFING EVALUATION

"*In God we trust; all others must bring data*". This quote commonly attributed to William Edwards Deming[7] may be applied to the evaluation of any machine learning or pattern recognition problem. Furthermore, these data should be public so that results can be reproduced and fairly compared, in order to avoid reaching the situation illustrated by another well known machine learning principle: give me the performance figure you want to reach and I will provide you the database that meets it.

Certainly, one of the key challenges faced nowadays by the rapidly evolving biometric industry is the need for publicly available standard datasets that permit the objective and reproducible evaluation of different aspects related to biometric recognition systems (e.g., performance, security, interoperability or privacy). This is particularly relevant for the assessment of spoofing attacks and their corresponding anti-spoofing protection methodologies.

In addition to data acquisition and distribution another key factor for developing the anti-spoofing technology is the organization of competitive evaluations. Such contests give a clear snapshot of systems performance at a given point and help to achieve a better understanding of the different algorithms accuracy. Furthermore, most public datasets are acquired in the framework of such competitions.

The next sections review: (*i*) important aspects related to general anti-spoofing database acquisition (Sect. IV-A); (*ii*) overall characteristics of anti-spoofing evaluation campaigns (Sect. IV-B); and (*iii*) the general context for anti-spoofing assessment introduced in the previous two sections is particularized for the case of face anti-spoofing in Sect. IV-C.

A. ANTI-SPOOFING DBS: GENERAL ASPECTS

The present section gives an overview of the current publicly available anti-spoofing databases that may be used for the development and evaluation of new protection measures against direct attacks in the field of face recognition. Results from the latest face anti-spoofing competitive evaluations are also given for reference in order to provide an updated view of face anti-spoofing performance as of today.

In relation to spoofing, only recently has the biometric community started to devote some important efforts to the acquisition of large and statistically meaningful anti-spoofing databases. In most cases, these datasets have been generated in the framework of international evaluation competitions such as the series of Fingerprint Liveness Detection Competitions, LivDet, held biennially since 2009 [55], [169], [170], or the more recent 2D Face Anti-Spoofing contests that started in 2011 [54], [130]. Such initiatives provide public benchmarks for developers and researchers to objectively evaluate their proposed anti-spoofing solutions and compare them to other existing or future approaches. This way, the public availability of standardized datasets is fundamental for the evolution of the state-of-the-art.

In spite of the increasing interest in the study of vulnerabilities to direct attacks, the availability of spoofing databases is still scarce. This may be explained from both a technical and a legal point of view. (*i*) From a technical perspective,

[7](W.E.D, 1900-1993). On the Web, this quote has been widely attributed to Deming, however, as stated in the introduction of [168]: ironically enough, we could find no "data" confirming this end.

the acquisition of spoofing-related data presents an added challenge to the usual difficulties encountered in the acquisition of standard biometric databases (i.e., time-consuming, expensive, human resources needed, cooperation from the data subjects…): the generation of a large amount of fake artefacts which are in many cases tedious and slow to generate on large scale (e.g., face masks, gummy fingers, or printed iris lenses). (*ii*) Legal aspects related to data protection make the distribution of biometric databases among research groups or industries tedious and difficult. These legal restrictions have forced most laboratories working in the field of spoofing to acquire their own proprietary (and usually small) datasets on which to evaluate their protection methods. Although these are valuable efforts, they have limited scientific impact, since results may not be compared or reproduced by other researchers.

Both public and proprietary datasets acquired for anti-spoofing evaluation are generally constructed according to one of the following three approaches:

- **Different Real/Fake Users**. The spoofing database is constructed using real samples of a previously existing dataset. Then, fake samples of different new users are added. Anti-spoofing is a two class classification problem, therefore, from a theoretical point of view, such an approach is valid for the evaluation of liveness detection techniques, as the database contains samples of both classes. However, this type of database is not advisable and should be avoided, as it presents two major problems: on one hand, it has the limitation of not allowing spoofing vulnerability studies where the intruder tries to access the system using a fake biometric trait of a genuine user (as real and fake samples were not produced by the same subjects); on the other hand, real and fake samples do not only correspond to different persons but may have also been acquired with different sensors, at different locations, or following different protocols, which could potentially lead to biased results. Examples of works using such databases are [28], [171], and [172].
- **Same Real/Fake Users, But Different Acquisition Conditions**. As in the previous case, the spoofing database is constructed based on real samples of a previous dataset. However, in this case, those real samples are the ones used to produce the fake spoofs, consequently, both real and fake users coincide. This could be, for instance, the case of a face spoofing database where the artefacts used to carry out the fraudulent access attempts are printed photographs of an already publicly available real face image database. Again, the problem in this case is that anti-spoofing evaluation results may be biased due to changes in the acquisition environment (e.g., sensor, illumination, distance to the sensor, pose, pressure, size, resolution, etc.) In such conditions, liveness detection algorithms may detect those contextual variations, and not the intrinsic differences between real and fake samples. Examples of works using such databases include [111], [173], and [174].
- **Same Real/Fake Users and Same Acquisition Conditions**. This is the most advisable way to proceed in an anti-spoofing evaluation. In this case, the database is captured from scratch for the same real and fake users under the same acquisition environment. Most of the works presented in the face literature review in Sect. III and all the competitive anti-spoofing evaluation campaigns follow this approach.

B. ANTI-SPOOFING EVALUATION CAMPAIGNS: GENERAL ASPECTS

In the area of anti-spoofing assessment, as in other biometric-related scenarios [175], two main types of evaluations are possible: (*i*) *algorithm-based*, also referred in the literature as *technology evaluation* [175], thought to evaluate liveness detection modules or algorithms, independently of the rest of the system. This type of evaluation is therefore well suited to assess feature-level techniques; (*ii*) *system-based*, also known as *scenario evaluation* [175], designed to evaluate biometric systems as a whole, including the scanner. Adequate therefore to assess sensor-level schemes where acquisition devices are specific for each system.

The advantage of algorithm-based evaluations is that the same data and protocol may be used to assess all techniques. Furthermore, this benchmark can be made public, so that future software-based methods may be directly compared to the evaluation results. On the other hand, system-based evaluations are just restricted to the scope of a given competition, and no further comparison may be established with future systems, as new data would have to be acquired for each specific sensor. That is, due to their intrinsic hardware-based nature, it is not possible to acquire a single distributable database that satisfies the particular hardware acquisition requirements of each different sensor-based approach.

However, it is important to highlight that it is possible to carry out competitive evaluations of complete liveness detection systems (including the acquisition sensor) and not just of independent anti-spoofing algorithms or modules. Such system-based evaluations have already started up at the fingerprint LivDet 2011 and 2013 and at the iris LivDet 2013 competitions [55], [56], [170]. In these three contests, the two evaluation modalities mentioned above (i.e., algorithm- and sensor-based) were offered to the participants: (*i*) submission of anti-spoofing software-based algorithms (i.e., only the liveness detection module), that were evaluated on the same prerecorded data following the same protocol (now publicly available); (*ii*) submission of complete functional biometric systems, that were tested on the spot performing a fixed number of real access attempts and spoofing access attempts (i.e., direct attacks), carried out with the same, or very similar artefacts to those used for the generation of the software-based database. In the latter case, a number of important factors should be taken into account in order to obtain comparable results: using the same spoofs to evaluate all systems, enrolling the same live subjects, same acquisition

conditions (e.g., background, pose or illumination), controlling the possible spoofs degradation.

Compared to algorithm-based evaluations, system-based ones provide a better estimation of the anti-spoofing capabilities of fully functional biometric systems, and not just of liveness detection algorithms. Such type of assessment also gives very valuable information regarding the real robustness against spoofing of commercial biometric applications which, in practice, are released as a complete finalized product and not as a group of independent modules. Furthermore, system-based evaluations represent a closer approximation to spoofing attacks that could be carried out in a real-world scenario.

Another important observation worth highlighting in the field of anti-spoofing assessment, is the distribution of fake samples across datasets. Up to date, in all algorithm-based competitions that have been organised (two in face, three in fingerprint and one in iris), the train and test sets distributed to the participants contained the same type of spoofs. This means that algorithms may be trained on the same type of data that will later be used for testing. However, in a real operational scenario, algorithms have to face artefacts which are unknown to them. This way, results obtained under laboratory conditions may be an optimistic estimate of the real performance of the anti-spoofing methods being tested.

This potential bias in the evaluation results between laboratory and real environments was addressed in the systems category of the LivDet 2011 and 2013 competitions [55], [170]. In these two contests, participants did not receive any training data and were just given some general information about the three types of spoofs that would be used to attack their systems. Then, in the testing phase, in addition to these three known artefacts, two more, totally new to the systems, were also used for evaluation. A similar approach could be followed in algorithms-based assessment by limiting the diversity of fake training data compared to that used for testing.

C. FACE ANTI-SPOOFING EVALUATION AND DATABASES

Based on the general context for anti-spoofing evaluation described above (see Sects. IV-A and IV-B), the present section gives an overview of he current exiting initiatives in face anti-spoofing assessment with special attention to public databases and competition results.

Currently there are six large public face anti-spoofing databases that comprise most attacking scenarios described in Sect. III-A: the NUAA PI DB, the YALE-RECAPTURED DB, the PRINT-ATTACK DB, the CASIA FAS DB, the REPLAY-ATTACK DB and the 3D MASK-ATTACK DB (described in the following subsections). The chronology of all six databases illustrates in a very good manner the state-of-the-art evolution in the field of face spoofing and anti-spoofing, showing how attacks have become gradually more sophisticated and how protection methods have adapted to the new challenges in order to increase their accuracy.

The first effort to generate a large public face anti-spoofing DB was reported in [102] with the NUAA PI DB, which contains still-images of real access attempts and print-attacks of 15 users. The YALE-RECAPTURED DB appeared soon after, and added the difficulty of varying illumination conditions as well as considering LCD spoofs (i.e., the attacks were carried out showing face images on LCD screens) instead of classic print attempts [111]. This database, however, is still quite restricted in terms of number of users (10), and it only comprises real and fake static images. Furthermore, it was captured from an already existing dataset (the Yale Face DB-B), with the limitations entailed as discussed in Sect. IV-A. The PRINT-ATTACK DB represents yet another step in the evolution of face spoofing, both in terms of size (50 different users were captured) and of data acquired (it contains video sequences instead of still images). However, it still only considers the case of photo attacks [59]. This feature is improved by both the REPLAY-ATTACK DB [54] and the CASIA FAS DB [105], which contain not only photo attacks with different supports (e.g., paper, mobile phones and tablets) but also replay video attacks. In addition, these last two databases are complementary, as the REPLAY-ATTACK DB was acquired with one single sensor using different attack devices of increasing quality under varying illumination and background conditions, while the CASIA FAS DB was captured with sensors of different quality under a uniform acquisition setting. To date, the last contribution in the field of public face spoofing databases, is the 3D MASK-ATTACK DB [109], which has initiated the path of 3D face acquisition under mask attacks (all previous datasets comprise only 2D data and photo or video attacks). Table 5 shows a comparison of the most important features of these six face spoofing databases.

From the six previous databases, the REPLAY-ATTACK DB is probably the most significant one, not only for its size, multiple and well defined protocols and attacks covered, but also because it was used in the last edition of the Competition on Countermeasures to 2D Facial Spoofing Attacks held in 2013 [54]. For these reasons, as an illustrative example of spoofing attacks carried out against face recognition systems, in Fig. 5 we show some typical images (frames extracted from videos) of real and fake access attempts from the REPLAY-ATTACK DB (mobile, print and highdef attack scenarios are defined in Sect. IV-C.5).

For completeness, the results of the 2013 Competition on Countermeasures to 2D Facial Spoofing Attacks are shown in Table 4, in terms of the percentage of correctly classified samples. All the information in this table has been directly extracted from [54]. We refer the reader to that work for further details on the competition.

The contest only considered an algorithm-based evaluation, therefore, only feature-level approaches were submitted (see Sect. IV-B for a general classification and characteristics of anti-spoofing evaluations). The competition database (a subset of the REPLAY-ATTACK DB) was divided into: a train set, to tune and train the algorithms; a development set, to fix the decision threshold between real and fake classes; and a test set, where the final results were computed. The same spoofs were present in all three sets.

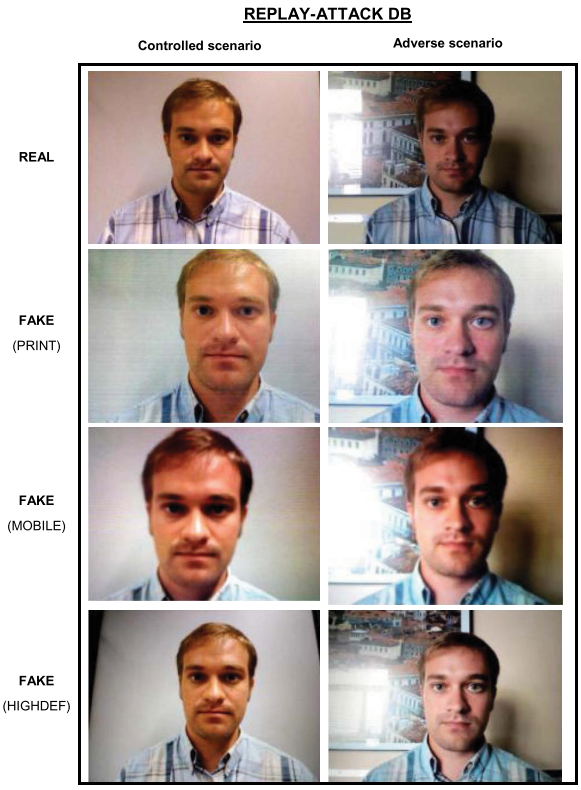


FIGURE 5. Typical examples of real and fake (mobile, print and highdef attacks) face images that can be found in the public REPLAY-ATTACK DB. Images were extracted from videos acquired in two illumination and background scenarios: controlled and adverse. For further details on types of attacks and acquisition settings please see Sect. IV-C.5.

The last column of Table 4 shows, in percentage, the algorithms accuracy on the test set, computed as 100-HTER, where HTER stands for the Half Total Error Rate. The previous two columns indicate the feature classes (static or dynamic) used by each of the algorithms. The results show that the fusion of static and dynamic features draws the best results, with the two top algorithms reaching 100% accuracy even under the multiple attack scenario that was featured in the competition: several illumination and background conditions, different spoof devices (print, mobile phone, tablet) and different attacking methods (photo, video). Interestingly, the best static-based algorithms are able to perform almost at the same level as the fused approaches, with a 99% classification rate, significantly higher than the only dynamic technique that was presented to the competition, algorithm 2, which obtained an accuracy of 91%.

1) NUAA PI DB

The NUAA Photograph Imposter DB [102] is publicly available from the Pattern Recognition and Neural Computing Group of the Nanjing University of Aeronautics an Astronautics (ParNeC-NUAA).[8]

This database contains still images of both real-access and spoofing attack attempts of 15 subjects. Samples are extracted

[8]http://parnec.nuaa.edu.cn/xtan/data/NUAAImposterDB.html

TABLE 4. Results obtained by the 8 algorithms that participated in the 2013 competition on countermeasures to 2D facial spoofing attacks. HTER stands for half total error rate. for a more detailed description of the database used in the evaluation please see Sect. IV-C.5. The information displayed in the table has been directly extracted from [54].

	2D Face Anti-spoofing 2013, Results Correctly classification rate (%)		
	Static	Dynamic	100-HTER (test)
Alg1	✓	✓	100.0
Alg2		✓	90.9
Alg3	✓	✓	97.5
Alg4	✓	✓	100.0
Alg5	✓		98.7
Alg6	✓		98.7
Alg7	✓		88.0
Alg8	✓		84.4

from videos captured with a cheap generic webcam (the model is not specified) with a resolution of 640 × 480 pixels. The database was acquired under uncontrolled illumination conditions in three different sessions separated two weeks from each other. The amount of data among sessions is unbalanced as not all the subjects participated in the three acquisition campaigns.

During real access attempts, subjects were asked to stay as still as possible with no evident face movements such as eye blinking, in order to simulate the characteristics of typical print attacks.

All attacks were carried out with printed copies of high definition face close-ups of the users, captured with a standard Canon camera (model is not specified). Three different hard-copies of each photograph were generated to attack the system: (*i*) professional developing on photographic paper of size 6.8cm × 10.2cm; (*ii*) professional developing on photographic paper of size 8.9cm × 12.7cm; (*iii*) home generated copy using a standard color ink HP printer and A4 70gr paper. During the attacks the printed images were moved in different forms, trying to imitate the typical behaviour of real access attempts: back and forth, vertically and horizontally, slightly warped around in the vertical and horizontal axis.

The database is divided into a train and a test set: the train set comprises images from the two first acquisition sessions, while the test set only contains samples of the last one, therefore there is no overlap between them in terms of samples. However, some users do appear in both sets.

2) YALE-RECAPTURED DB

The YALE-RECAPTURED database [111] is publicly available under request from the University of Campinas.[9]

The dataset consists of 640 static images of real access attempts and 1,920 attack samples, acquired from 10 different users. The genuine subset is taken from the previously existing Yale Face DB-B [176], where each user was acquired under 64 different illumination conditions.

Attack attempts were carried out displaying real images on three different LCD monitors: *i*) LG Flatron L196WTQ

[9]http://www.ic.unicamp.br/rocha/

TABLE 5. Comparative summary of the most relevant features corresponding to the six face spoofing databases described in Sect. IV-C. # indicates number, *Samp* stands for samples, *LQ* for 2D low quality, *SQ* for 2D standard quality, *HQ* for 2D high quality, *Ph* for photo, *Vd* for video, *Mk* for mask, *Hh* for handheld, *Fx* for fixed, *Cont* for controlled and *Adv* for adverse.

	Comparative summary: Public Face Spoofing DBs														
	Overall Info. (Real/Fake)			Sensor Info.					Types			Supp.		Illum.	
	# IDs	# Samp	Type	#	*LQ*	*SQ*	*HQ*	3D	Ph	Vd	Mk	Hh	Fx	Cont.	Adv
NUAA PI DB [102]	15/15	5,105/7,509	Images	1		✓			✓			✓			✓
YALE-RECAPT DB [111]	10/10	640/1,920	Images	2		✓	✓		✓				✓	✓	✓
PRINT-ATTACK DB [59]	50/50	200/200	Videos	1	✓				✓			✓	✓	✓	✓
CASIA FAS DB [105]	50/50	150/450	Videos	3	✓	✓	✓		✓	✓		✓			✓
REPLAY-ATTACK DB [104]	50/50	200/1000	Videos	1	✓				✓	✓		✓	✓	✓	✓
MASK-ATTACK DB [107]	17/17	170/85	Videos	2		✓		✓			✓	✓		✓	

Wide 19'', *ii*) a CTL 171Lx 1700 TFT, and *iii*) a DELL Inspiron 1545 notebook. Then, the images were recaptured with two different cameras, a Kodak C813 with a resolution of 8.2 megapixels and a Samsung Omnia i900 of 5 megapixels. After the recapture process, samples were cropped and normalized to grey-scale images of size 64×64.

The multiple illumination conditions make this database a quite challenging one. However, since the genuine and fake subsets were acquired in different settings and with different devices, results obtained on it may be biased due to these contextual differences (see Sect. IV-B for further reading on anti-spoofing databases acquisition).

3) PRINT-ATTACK DB

The PRINT-ATTACK database [59] is publicly available from the IDIAP Research Institute website[10]. This database was used on the 2011 Competition on Countermeasures to 2D Facial Spoofing Attacks [130].

It consists of 200 videos of real accesses and 200 videos of print attack attempts from 50 different users. The database is divided into a train, a development and a test set which coincide with those used in the 2011 competition.

Real and attack access video sequences were captured with a 320×240 pixel (QVGA) resolution camera of a MacBook laptop, at 25 frames-per-second with an average duration of around 10 seconds and stored in mov format. Videos were recorded under two different background and illumination conditions: *i*) *controlled*, with a uniform background and indoor homogeneous lighting coming from a fluorescent lamp; *ii*) *adverse*, in this case the background is not uniform (regular office-like background) and the scene has day-light illumination.

Attacks were carried out with hard copies of high resolution photographs of the 50 users, printed on plain A4 paper with a Triumph-Adler DCC 2520 color laser printer. The photographs were taken during real access attempts, under the same illumination and background setting, with a 12.1 megapixel Canon PowerShot SX150 IS camera. For the attacks, printouts are held in front of the acquisition sensor (i.e., MacBook laptop camera) using two different supports: hand-held attack (i.e., the intruder holds the photograph with his hands) or fixed support attack (i.e., pictures are stuck to the wall so that there is no movement).

4) CASIA FAS DB

The CASIA Face Anti-Spoofing DB [105] is publicly available from the Chinese Academy of Sciences (CASIA) Center for Biometrics and Security Research (CASIA-CBSR).[11]

This database contains short videos (around 10 seconds in avi format) of both real-access and spoofing attack attempts of 50 subjects, divided into a train and a test set with no overlap between them (in terms of users and samples). Samples were acquired with three devices with different resolutions: *i*) *low resolution*, with an old 640×480 USB web camera (model is not specified); *ii*) *normal resolution*, with a modern 480×640 USB web camera (model is not specified); and *iii*) *high resolution*, using a 1920×1080 Sony NEX-5 high definition camera.

Three different attacks were considered: *i*) *warped*, illegal access attempts are carried out with slightly curved hard copies on copper paper (which has a higher quality than regular A4 printing paper) of high-resolution digital photographs of the genuine users (taken with the Sony NEX-5 camera); *ii*) *cut*, the attacks are performed using hard copies of high-resolution digital photographs of the genuine users (as before), where the eyes have been cut out and the face of the attacker is placed behind (i.e., so that eye blinking is forged); *iii*) *video*, in this case high resolution videos of the genuine users are replayed in front of the acquisition device using an iPad.

5) REPLAY-ATTACK DB

The REPLAY-ATTACK DB [104] is publicly available at the IDIAP Research Institute website.[12]

The database was acquired as an extension of the PRINT-ATTACK DB, therefore it also contains short videos (around 10 seconds in mov format) of both real-access and spoofing attack attempts of 50 different subjects, acquired with a 320×240 resolution webcam of a 13-inch MacBook Laptop. The recordings were carried out under two different

[10] http://www.idiap.ch/dataset/printattack

[11] http://www.cbsr.ia.ac.cn/english/index.asp

[12] http://www.idiap.ch/dataset/replayattack

conditions: *i*) *controlled*, with a uniform background and artificial lighting; and *ii*) *adverse*, with natural illumination and non-uniform background.

In this case three different attacks with an increasing level of resolution were considered: (*i*) *print*, illegal access attempts are carried out with hard copies of high-resolution digital photographs (this data subset corresponds to the PRINT-ATTACK DB described in Sect. IV-C.3); (*ii*) *mobile*, attacks are performed using photos and videos taken with the iPhone using the iPhone 4 screen; *iii*) *highdef*, similar to the mobile subset but in this case the photos and videos are displayed using an iPad screen with a 1024 × 768 pixel resolution.

In addition, access attempts in the three attack subsets (mobile, print and highdef) were recorded in two different modes depending on the strategy followed to hold the attack replay device (mobile phone, paper or tablet): (*i*) hand-based, and (*ii*) fixed-support.

The database is distributed with an associated protocol which divides the database into a train, a development and a test set with no overlap between them (in terms of users and samples). The database also contains an enrollment subset with 100 videos corresponding only to real access attempts. This subset is provided as a means to evaluate the recognition performance of systems whose vulnerabilities to spoofing attacks will be later evaluated on the rest of the database.

The 2013 edition of the Competition on Countermeasures to 2D Facial Spoofing Attacks was held using a subset of all the available attacks on the REPLAY-ATTACK DB (not just the print data as in the 2011 edition). The exact data and protocol followed on this second edition are also released with the database [54]. The results of the competition are given in Table 4.

6) 3D MASK-ATTACK DB

The 3D MASK-ATTACK DB [107], [109] is publicly available at the IDIAP Research Institute website.[13] It constitutes the first public database that considers mask attacks and that, in addition to 2D data, provides as well depth information.

It comprises genuine and attack access attempts of 17 different users. The attacks were performed by one single operator wearing the real-size 3D masks of the genuine subjects. Masks were manufactured using the service provided by ThatsMyFace.com,[14] which only requires a frontal and two profile pictures of each person to generate a 3D mask. These three pictures (frontal and profiles) are also distributed with the database.

The database was captured in three different sessions: two real-access sessions held two weeks apart and a third session in which the mask attacks were performed. In each session and for each user, five videos of 10 seconds were captured using the Microsoft Kinect for Xbox 360. This sensor provides both regular 2D RGB data (8-bit) and depth data (11-bit), with a resolution of 640 × 480 pixels at 30 frames per second.

Therefore, the data available are: 255 color videos of 300 frames (170 real sequences and 85 mask attacks), and as many 2.5D sequences with the corresponding depth information. Such diversity of data permits a great flexibility for research in the field of face security to direct attacks, since it gives the possibility to study both 2D and 3D anti-spoofing algorithms and their fusion.

V. SUMMARY AND DISCUSSION: LESSONS, FACTS AND CHALLENGES

In ''Skyfall'', the latest movie in the James Bond saga, 007 is given a gun that only he can fire: It works by recognising his palmprint, rendering it useless when it falls into a baddy's hands. This is just another example of the multiple uses which have been given to biometrics in films, TV and books, in most cases assuming a zero-error and perfect security performance.

However, as usually happens in terms of technical advances, reality is still some distance away from fiction: *"On September 2013, the world witnessed a long anticipated event, heralding a paradigm shift in mobile security: Apple's launch of the new iPhone 5S with a fingerprint reader underneath the home button. The use case: to unlock the phone and authorize purchases in Apple's iStore. One day after the iPhone hit the shelves, a hacker team claimed to have circumvented the biometric system through getting the phone to accept a fake 'spoofed' fingerprint."* [177]

As reviewed in the present work, a great amount of research has been carried out concerning the vulnerabilities of biometric systems to direct attacks and multiple techniques to secure them against this threat have been proposed. Moreover, different independent evaluations have shown that some of these protection techniques are able to achieve very competitive results when assessed in laboratory conditions. However, in spite of all these efforts, commercial products, even those developed by the most advanced technological companies, keep failing to withstand the challenges posed by hackers. How can this situation be explained? Like in most cases, a simple answer is not possible as a number of factors have contributed to reach the current status.

On one hand, in all issues related to spoofing, the biometric community has followed from the beginning the *security through transparency principle*, first formulated in the field of cryptography and then generalized to all other security areas as *"the enemy knows your system"* [178]. This principle states that the fewer and simpler the things one needs to keep secret in order to ensure the security of a given system, the easier it is to maintain that security. In other words, there is no point in trying to deny or cover the vulnerabilities of biometric systems to spoofing because, sooner or later, attackers will discover them and the consequences will be unpredictable [179]. Therefore, quoting the Biometric Working Group already in 2003: ''*public exposure of countermeasures and vulnerabilities will lead to a more mature and responsible attitude from*

[13] https://www.idiap.ch/dataset/replayattack
[14] http://www.thatsmyface.com/

the biometrics community and promote the development of more secure systems in the future'' [180]. Such a philosophy will undoubtedly pay off in the long-run, however, in the short term, each user becomes a potential and well-informed hacker every time a new biometric product is released, which leads to situations such as the one described for the iPhone 5S.

On the other hand, although some efforts have been made in the frame of the Common Criteria [41], [181] and there is on-going work to release the first ISO standard specifically focused on spoofing [42], still no largely extended standard exists regarding the evaluation of biometric vulnerabilities. This has resulted in very sparse certifications of biometric-based security commercial products compared to other technologies with a long standardization trajectory such as smart cards or cryptography [45]–[47]. A clear and well defined certification methodology to assess biometric security would certainly help developers in designing more robust and reliable systems.

Also, we should not forget that the ''worst case scenario'' is specially sensitive in spoofing. Let's take for instance the example of face. It is not rare to find that an anti-spoofing technique is extremely accurate detecting certain spoofs (e.g., printed images), but that consistently fails when it is confronted with a different type of fake artefacts (e.g., videos), referred to in some cases as ''golden fakes''. In a real case, if the attacker finds this vulnerability, and following the transparency principle it should be assumed that he will, the system will be compromised. In this worst case scenario, even if the anti-spoofing method, on average, has an extremely high performance, the reality is that it will be easily spoofed.

The ''worst case scenario'' presented above for face can be extended to all biometric traits, and makes spoofing evaluation a very difficult matter. It is especially challenging to recreate real attacking conditions in a laboratory evaluation. Under controlled conditions, systems are tested against a restricted number of typical spoofing artefacts, as it is unfeasible to collect a database with all the different possibilities that may be found in the market. Furthermore, assessment databases are usually divided into a train and a test set in which both of them contain examples of the same spoofs, therefore, protection techniques can be specifically tuned on the train set to detect what they already know will be present in the test set. However, the real world represents an open set evaluation with no constraints on the spoofs used to attack. In this scenario, what can be expected from the performance of protection techniques against *any* type of spoof and not only those for which it has been trained?

In addition to the afore mentioned issues, so far, biometric spoofing questions have been addressed mainly relying on empirical testing carried out by individual research groups to evaluate the performance of specific techniques, often with small-scale datasets acquired in an ad-hoc way. Although this learn-by-doing approach allows gaining some insight into the new spoofing problem, there is still not enough understanding of how to quantitatively address fundamental performance tradeoffs and limits, for no ''theory on spoofing'' has been established yet.

In the current spoofing context described above, and bearing in mind all lessons learned in more than 10 years of spoofing research, some still open questions are: Where do we go from here? What are the future challenges to be faced in biometric spoofing? What are the issues which still need to be looked into and further explored? What new lines of research can be foreseen in this field?

In order to answer these questions, it cannot be neglected that absolute security does not exist: given funding, willpower and the proper technology, every security system can be compromised. However, there are a number of steps that can be taken in order to continue improving the security offered by biometric systems against spoofing attacks, so that the effort and resources needed to break them, exceed the benefit gained by the attacker.

Probably, at this stage, one of the most urgent needs is to define a clear methodology to assess the ''spoofability'' of systems. This is not a straight forward problem, as there are new variables involved when the spoofing dimension is introduced. Although it is not yet generally deployed, an evaluation protocol which is gaining popularity for the assessment of biometric spoofing, defines two possible working scenarios [80], [107], [164], [182], [183]:

- *Licit Scenario*, considered in classic recognition evaluations, it only takes into account genuine access attempts and zero-effort impostor access attempts. In this scenario performance is typically reported in terms of the FRR (False Rejection Rate, number of genuine access attempts wrongly rejected) and the FAR (False Acceptance Rate, number of zero-effort impostor access attempts wrongly accepted).
- *Spoofing Scenario*, in which access attempts are either genuine or spoofing attacks. Although for this case there is still no agreed method for reporting results, two metrics which have been proposed and are starting to be used are the FRR (defined as in the licit scenario) and the SFAR (Spoofing False Acceptance Rate, corresponding to the number of spoofing attacks wrongly accepted).

All these three metrics (i.e., FRR, FAR and SFAR) should be strictly assessed before carrying out any further evaluation concerning liveness detection techniques. This way, the real threat posed by a spoofing database to a certain recognition system can be determined. When a countermeasure is introduced in the system, all three previous measures should be recomputed considering the anti-spoofing module, so that they can be compared to the case with no protection against direct attacks. As such, the real impact of the liveness detection technique on the system performance can be fully characterized.

Currently, when it comes to the evaluation of a new anti-spoofing countermeasure, in most cases, its performance is measured as an independent module and reported in terms of its classification rates, usually referred to as FFR (False Fake Rate, number of real samples classified as fake) and

FLR (False Living Rate, number of fake samples classified as real). This stand-alone assessment constitutes a first necessary step towards the evaluation of the countermeasure but, as specified above, it should be complemented with further analyses. In fact, a liveness detection algorithm will, in general, not operate on its own, but integrated in a recognition system. In this framework, to perform an exhaustive assessment, other questions which are very rarely answered in current state-of-the-art works, should be addressed: What is the impact of the FFR and FLR on the system performance (i.e., FRR, FAR and SFAR)? This issue can be addressed to a great extent following the two-scenario (i.e., licit and spoofing) evaluation protocol defined above.

Although the above methodology would already represent a big advance if it was widely adopted or implemented into a standard, it still opens some new interesting topics for research which have just started to be explored: What is the best way to combine matching and liveness-detection scores [164], [184]? What would be the impact of this fusion in multibiometric systems [182]? Can the performance of a system under both operating scenarios (i.e., licit and spoofing) be reported with one single metric? How can the above two-scenario methodology be generalized to the real case where all three score classes (i.e., genuine, zero-effort and spoofing) are present at the same time? Although current preliminary efforts in the study of spoofing assessment principles are hugely valuable, there is still quite limited theoretical foundation in this field to be able to answer some of the fundamental questions listed above. Accordingly, the biometric community needs to confront the existing challenges in order to build a solid theoretical background that allows further developing this area.

Another shortcoming of most current anti-spoofing techniques, that should be analysed in the near future, is their lack of interoperability across databases. To date, the competitions organised have shown that top-ranked algorithms are able to achieve an accuracy close to 100%, however, their performance drops significantly when the testing dataset is changed. An interesting lesson may be learned from these results: There exists no clearly superior anti-spoofing technique. Selecting one particular protection method depends on the nature of the attack scenarios and acquisition conditions. Therefore, it is important to find complementary countermeasures and study the best fusion approaches in order to develop liveness-detection techniques that succeed at achieving a high performance over different spoofing data [165], [185].

In addition to the above mentioned research topics aligned with spoofing fundamental theory, practical studies should not be forgotten. As technology progresses, new hardware devices and signal processing techniques continue to emerge. It is important to keep track of this rapid technological progress since some of the advances can be the key to develop novel and efficient anti-spoofing techniques. For example, just a few years ago, 3D acquisition scanners were unsuitable for liveness detection purposes due to their cost, size and level of cooperation required from the user. However, nowadays, there exist sensors which provide accurate depth information, with the size of a regular webcam and almost for its same price. Should they become integrated in biometric readers, such sensors could become in the near future a definitive solution against 2D photo and video attacks to face-based systems.

The anti-spoofing community should also consider engaging in new fundamental research regarding the biological dimension of biometric traits, in order to break with the current popular trend embraced by many of the latest research where some well known sets of features (e.g, LBP, LPQ, HOG or BSIF) are extracted from images in public databases and passed through a classifier. Although such a methodology is valid, in most cases it brings little new insight into the spoofing problem. A greater progress could potentially be obtained from new studies exploiting intrinsic biological differences between real and fake traits such as, for instance, the thermogram or the facial blood flow.

The impact of spoofing should also be considered in other biometric-related fields such as forensics. Sir Arthur Conan Doyle already foresaw the possibility of fake fingerprint forensic evidence in one of his renowned Sherlock Holme's short stories over a century ago [186]. Since then, different works have tested the ability of forensic examiners to distinguish between real and fake latent fingerprints [187], [188]. However, only recently have some interesting research works addressed the *automatic* detection of fake finger-marks deliberately left behind at crime scenes [189]–[191]. This is a research line that can gain a lot of strength and importance in the years to come.

Another more philosophical question to be addressed in the field of spoofing, is the balance between security and convenience. It is undeniable that one of the most important motivations, if not *the* most important reason, for the deployment and development of biometrics, is its security dimension. We want to secure access to information and biometrics represents a good alternative: you are your own key. In this context, spoofing gains great relevance: if the system is spoofed, the information is compromised. Therefore, it is clear that spoofing analysis is a key issue in the development of biometrics. However, it is important to keep in mind the final product where a biometric system will be integrated and its ultimate purpose within that product, as security is just one side of the coin. The other side is convenience. For certain applications, from the end-user perspective, some risk of spoofability may be acceptable if, in return, he obtains a greater gain in convenience. Let's go back to the iPhone 5S example. At the end of the day, are we sure it was meant to be unspoofable (even by simple known methods)? Was it worth making it more secure at the cost of increasing its price and the inconvenience to the user (more false rejections)? If someone is ready to go through the tedious process of lifting a latent fingerprint and casting a fake finger just to "unlock our phone", wouldn't he also be ready to obtain our 4 digit PIN (perhaps just by looking over our shoulder) if no biometrics were integrated in the device? In fact, it is estimated

that over 50% of users had not set any security mechanism to unlock their mobile phones before the introduction by apple of the *convenient* fingerprint reader. If such percentage is decreased with the use of biometrics, it may be argued that a convenient and spoofable system has increased the overall security of mobile phones. Yes, the iPhone 5S can be spoofed, but, in practice, how many of them will be spoofed? Wouldn't they be hacked all the same without biometrics?

As a wrap up conclusion it may be stated that, although a great amount of work has been done in the field of spoofing detection and many advances have been reached, attacking methodologies have also evolved becoming more and more sophisticated. As a consequence, there are still big challenges to be faced in the protection against direct attacks, that will hopefully lead in the coming years to a new generation of more secure biometric systems.

In the meanwhile, Mr Bond will still have to wait some time until he gets a gun that he can *fully trust* to be the only one who can fire it.

REFERENCES

[1] W. W. Bledsoe, "The model method in facial recognition," Panoramic Res., Inc., Palo Alto, CA, USA, Tech. Rep. PRI:15, 1964.
[2] M. D. Kelly, "Visual identification of people by computer," Stanford AI Project, Stanford, CA, USA, Tech. Rep. AI-130, 1970.
[3] K. H. Davis, R. Biddulph, and S. Balashek, "Automatic recognition of spoken digits," *J. Acoust. Soc. Amer.*, vol. 24, no. 6, pp. 637–642, 1952.
[4] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 2, pp. 125–143, Jun. 2006.
[5] The Guardian. (2013). *iPhone 5S Fingerprint Sensor Hacked by Germany's Chaos Computer Club*. [Online]. Available: http://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked
[6] The Register. (2008). *Get Your German Interior Minister's Fingerprint Here*. [Online]. Available: http://www.theregister.co.uk/2008/03/30/german_interior_minister _fingerprint_appropriated/
[7] The CNN. (2010). *Man in Disguise Boards International Flight*. [Online]. Available: http://edition.cnn.com/2010/WORLD/americas/11/04/canada.disguised.passenger/
[8] PRA Laboratory. (2013). *Fingerprint Spoofing Challenge, YouTube*. [Online]. Available: http://www.youtube.com/watch?v=vr0FmvmWQmM
[9] Discovery Channel. (2011). *Mythbusters: Fingerprints Cannot be Busted, YouTube*. [Online]. http://www.youtube.com/watch?v=3Hji3kp-i9k
[10] Chaos Computer Club Berlin. (2013). *Hacking iPhone 5S Touchid, YouTube*. [Online]. Available: http://www.youtube.com/watch?v=HM8b8d8kSNQ
[11] Sky News. (2013). *Fake Fingers Fool Hospital Clock-in Scanner*. [Online]. Available: http://news.sky.com/story/1063956/fake-fingers-fool-hospital-clock-in-scanner
[12] Tech Crunch. (2009). *Woman Uses Tape to Trick Biometric Airport Fingerprint Scan*. [Online]. Available: http://techcrunch.com/2009/01/02/woman-uses-tape-to-trick-biometric-airport-fingerprint-scan/
[13] BBC News. (2005). *Malaysia Car Thieves Steal Finger*. [Online]. Available: http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm
[14] The Daily Mail. (2012). *The Man in the Latex Mask*. [Online]. Available: http://www.dailymail.co.uk/news/article-2153346/Black-armed-robber-disguised-white-man-using-latex-mask.html
[15] N. M. Duc and B. Q. Minh, *Your Face is NOT Your Password. Face Authentication Bypassing Lenovo—Asus—Toshiba*. San Francisco, CA, USA: Black Hat, 2009.
[16] Tabula Rasa. (2013). *Tabula Rasa Spoofing Challenge*. [Online]. Available: http://www.tabularasa-euproject.org/evaluations/tabula-rasa-spoofing-challenge-2013
[17] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
[18] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognit.*, vol. 35, no. 12, pp. 2727–2738, 2002.
[19] A. Wehde and J. N. Beffel, *Finger-Prints Can be Forged*. Chicago, IL, USA: Tremonia Publishing Company, 1924.
[20] L. Thalheim, J. Krissler, and P.-M. Ziegler, "Body check: Biometric access protection devices and their programs put to the test," *c't Mag.*, vol. 11, pp. 114–121, Nov. 2002.
[21] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, "An evaluation of indirect attacks and countermeasures in fingerprint verification systems," *Pattern Recognit. Lett.*, vol. 32, no. 12, pp. 1643–1651, 2011.
[22] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," *Pattern Recognit.*, vol. 43, no. 3, pp. 1027–1038, 2010.
[23] P. Mohanty, S. Sarkar, and R. Kasturi, "From scores to face templates: A model-based approach," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 12, pp. 2065–2078, Dec. 2007.
[24] C. Rathgeb and A. Uhl, "Attacking iris recognition: An efficient hill-climbing technique," in *Proc. 20th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 2010, pp. 1217–1220.
[25] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, Jan. 2008, Art. ID 579416.
[26] B. Toth, "Biometric liveness detection," *Inf. Secur. Bull.*, vol. 10, no. 8, pp. 291–297, 2005.
[27] K. Kollreider, H. Fronthaler, and J. Bigun, "Non-intrusive liveness detection by face images," *Image Vis. Comput.*, vol. 27, no. 3, pp. 233–244, 2009.
[28] Z. Wei, X. Qiu, Z. Sun, and T. Tan, "Counterfeit iris detection based on texture analysis," in *Proc. 19th IAPR Int. Conf. Pattern Recognit. (ICPR)*, Dec. 2008, pp. 1–4.
[29] S. Marcel, M. S. Nixon, and S. Z. Li, Eds., *Handbook of Biometric Anti-Spoofing*. New York, NY, USA: Springer-Verlag, 2014.
[30] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," in *Handbook of Biometrics*. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.
[31] G. Pan, Z. Wu, and L. Sun, "Liveness detection for face recognition," in *Recent Advances in Face Recognition*. Rijeka, Croatia: InTech, 2008, pp. 236–252.
[32] Z. Akhtar, "Security of multimodal biometric systems against spoof attacks," Ph.D. dissertation, Dept. Elect. Electron. Eng., Univ. Cagliari, Cagliari, Italy, 2012.
[33] J. G. Herrero, "Vulnerabilities and attack protection in security systems based on biometric recognition," Ph.D. dissertation, Dept. Ingeniería Inf., Univ. Autonoma Madrid, Madrid, Spain, 2009.
[34] E. Marasco, "Secure multibiometric systems," Ph.D. dissertation, Dept. Inf. Sistemistica, Univ. Naples Federico II, Naples, Italy, 2010.
[35] P. Coli, "Vitality detection in personal authentication systems using fingerprints," Ph.D. dissertation, Dept. Ingegneria Elettr. Elettron., Univ. Cagliari, Cagliari, Italy, 2008.
[36] M. Sandström, "Liveness detection in fingerprint recognition systems," M.S. thesis, Dept. Comput. Inf. Sci., Linköping Univ., Linköping, Sweden, 2004.
[37] M. Lane and L. Lordan, "Practical techniques for defeating biometric devices," M.S. thesis, Dublin City Univ., Glasnevin, Ireland, 2005.
[38] J. Blommé, "Evaluation of biometric security systems against artificial fingers," M.S. thesis, Dept. Comput. Inf. Sci., Linköping Univ., Linköping, Sweden, 2003.
[39] R. Derakhshani, "Determination of vitality from a non-invasive biomedical measurement for use in integrated biometric devices," M.S. thesis, Dept. Comput. Sci. Elect. Eng., West Virginia Univ., Morgantown, WV, USA, 1999.
[40] *Information Technology—Security Techniques—Security Evaluation of Biometrics*, ISO/IEC Standard ISO/IEC 19792:2009, 2009.
[41] *Biometric Evaluation Methodology. v1.0*, BEM, 2002.
[42] *Information Technology—Biometrics—Presentation Attack Detection—Part 1: Framework*, ISO/IEC Standard ISO/IEC CD 30107-1, 2016.
[43] Centro Criptologico Nacional (CCN), "Characterizing attacks to fingerprint verification mechanisms CAFVM v3.0," Common Criteria Portal, Tech. Rep., 2011.
[44] Bundesamt fur Sicherheit in der Informationstechnik (BSI), "Fingerprint spoof detection protection profile FSDPP v1.8," Common Criteria Portal, Tech. Rep., 2008.

[45] Federal Office for Information Security, "Certification report, BSI-DSZ-CC-0511-2008 for PalmSecure SDK version 24 premium from Fujitsu limited," Fed. Office Inf. Secur., Bonn, Germany, Tech. Rep. BSI-DSZ-CC-0511-2008, 2008.

[46] Centro Criptologico Nacional, "Certification report, 2009-30-INF-515 v1 for AuthenTest server v1.2.6 from AuthenWare Corp.," Ministerio Defensa España, Madrid, Spain, Tech. Rep. 2009-30-INF-515, 2010.

[47] Federal Office for Information Security, "Certification report, BSI-DSZ-CC-0790-2013 for MorphoSmart optic 301, version 1.0 from Safran Morpho," Fed. Office Inf. Secur., Bonn, Germany, Tech. Rep.BSI-DSZ-CC-0790-2013, 2013.

[48] P. D. Lapsley, J. A. Less, D. F. Pare, Jr., and N. Hoffman, "Anti-fraud biometric scanner that accurately detects blood flow," U.S. Patent 5 737 439, Apr. 7, 1998.

[49] E. Diaz-Santana and G. Parziale, "Liveness detection method," European Patent EP1 872 719, Jan. 2, 2008.

[50] J. Kim, H. Choi, and W. Lee, "Spoof detection method for touchless fingerprint acquisition apparatus," Korea Patent 1 054 314, 2011.

[51] *Proc. Int. Joint Conf. Biometrics (IJCB)*, 2011.

[52] *Proc. Int. Biometric Perform. Test. Conf.*, 2012. [Online]. Available: http://www.nist.gov/itl/iad/ig/ibpc2012.cfm

[53] *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, 2013. [Online]. Available: http://www.icassp2013.com/SpecialSessions.asp

[54] I. Chingovska *et al.*, "The 2nd competition on counter measures to 2D face spoofing attacks," in *Proc. IAPR Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–6.

[55] L. Ghiani *et al.*, "LivDet 2013 fingerprint liveness detection competition 2013," in *Proc. IAPR Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–6.

[56] D. Yambay, J. S. Doyle, K. W. Bowyer, A. Czajka, and S. Schuckers, "LivDet-iris 2013—Iris liveness detection competition 2013," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Sep./Oct. 2014.

[57] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Direct attacks using fake images in iris verification," in *Proc. COST Workshop Biometrics Identity Manage. (BioID)*, vol. LNCS-5372. 2008, pp. 181–190.

[58] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," *Telecommun. Syst.*, vol. 47, nos. 3–4, pp. 243–254, 2011.

[59] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–7.

[60] Biometrics Inst. (2011). *Biometric Vulnerability Assessment Expert Group*. [Online]. Available: http://www.biometricsinstitute.org/pages/biometric-vulnerability-assessment-expert-group-bvaeg.html

[61] NPL. (2010). *National Physical Laboratory: Biometrics*. [Online]. Available: http://www.npl.co.uk/biometrics

[62] CESG. (2001). *Communications-Electronics Security Group—Biometric Working Group (BWG)*. [Online]. Available: https://www.cesg.gov.uk/policyguidance/biometrics/Pages/index.aspx

[63] BEAT. *BEAT: Biometrics Evaluation and Testing*. (2012). [Online]. Available: http://www.beat-eu.org/

[64] TABULA RASA. (2010). *Trusted Biometrics Under Spoofing Attacks*. [Online]. Available: http://www.tabularasa-euproject.org/

[65] B. Schneier, "Biometrics: Truths and fictions," in *Proc. Crypto-Gram Newslett.*, 1998. [Online]. Available https://www.schneier.com/crypto-gram-9808.html#biometrics

[66] B. Schneier, "Inside risks: The uses and abuses of biometrics," *Commun. ACM*, vol. 48, no. 8, p. 136, 1999.

[67] Y. Li, K. Xu, Q. Yan, Y. Li, and R. H. Deng, "Understanding OSN-based facial disclosure against face authentication systems," in *Proc. ACM Asia Symp. Inf., Comput. Commun. Security (ASIACCS)*, 2014, pp. 413–424.

[68] J. Galbally *et al.*, "An evaluation of direct attacks using fake fingers generated from ISO templates," *Pattern Recognit. Lett.*, vol. 31, no. 8, pp. 725–732, 2010.

[69] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial 'gummy' fingers on fingerprint systems," in *Proc. SPIE, Opt. Secur. Counterfeit Deterrence Techn. IV*, vol. 4677. Apr. 2002, pp. 275–289.

[70] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in *Proc. IAPR Int. Conf. Biometrics (ICB)*, 2007, pp. 366–375.

[71] B. B. Mjaaland, P. Bours, and P. Gligoroski, "Walk the walk: Attacking gait biometrics by imitation," in *Proc. 13th Int. Conf. Inf. Security (ISC)*, 2010, pp. 361–380.

[72] H. Chen, H. Valizadegan, C. Jackson, S. Soltysiak, and A. K. Jain, "Fake hands: Spoofing hand geometry systems," in *Proc. Biometrics Consortium Conf. (BCC)*, 2005.

[73] F. Alegre, R. Vipperla, N. Evans, and B. Fauve, "On the vulnerability of automatic speaker recognition to spoofing attacks with artificial signals," in *Proc. Eur. Signal Process. Conf. (EUSIPCO)*, Aug. 2012, pp. 36–40.

[74] Q. Bin, P. Jian-Fei, C. Guang-Zhong, and D. Ge-Guo, "The anti-spoofing study of vein identification system," in *Proc. Int. Conf. Comput. Intell. Secur. (ICCIS)*, Dec. 2009, pp. 357–360.

[75] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in *Proc. IEEE 5th Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep. 2012, pp. 283–288.

[76] P. Tome, M. Vanoni, and S. Marcel, "On the vulnerability of finger vein recognition to spoofing," in *Proc. IEEE Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2014.

[77] A. Al-Ajlan, "Survey on fingerprint liveness detection," in *Proc. Int. Workshop Biometrics Forensics (IWBF)*, Apr. 2013, pp. 1–5.

[78] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: A survey," *IET Biometrics*, vol. 3, no. 4, pp. 219–233, Dec. 2014.

[79] E. Marasco and A. Ross, "A survey on anti-spoofing schemes for fingerprints," *ACM Comput. Surv.*, vol. 47, no. 2, pp. 1–36, 2014.

[80] P. Johnson, R. Lazarick, E. Marasco, E. Newton, A. Ross, and S. Schuckers, "Biometric liveness detection: Framework and metrics," in *Proc. NIST Int. Biometric Perform. Conf. (IBPC)*, Mar. 2012.

[81] R. Lazarick, "Spoofs, subversion and suspicion: Terms and concepts," in *Proc. NIST Int. Biometric Perform. Conf. (IBPC)*, 2012.

[82] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. Berlin, Germany: Springer-Verlag, 2009.

[83] A. M. Namboodiri, S. Saini, X. Lu, and A. K. Jain, "Skilled forgery detection in on-line signatures: A multimodal approach," in *Proc. Int. Conf. Biometric Authentication (ICBA)*, 2004, pp. 505–511.

[84] J. Fierrez-Aguilar, "Adapted fusion schemes for multimodal biometric authentication," Ph.D. dissertation, Dept. Señales, Sist. Radiocomun., Univ. Politecnica Madrid, Madrid, Spain, 2006.

[85] R. N. Rodrigues, N. Kamat, and V. Govindaraju, "Evaluation of biometric spoofing in a multimodal system," in *Proc. 4th IEEE Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep. 2010, pp. 1–5.

[86] P. A. Johnson, B. Tan, and S. Schuckers, "Multimodal fusion vulnerability to non-zero effort (spoof) imposters," in *Proc. IEEE Int. Workshop Inf. Forensics Security (WIFS)*, Dec. 2010, pp. 1–5.

[87] B. Biggio, Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks," *IET Biometrics*, vol. 1, no. 1, pp. 11–24, Mar. 2012.

[88] Z. Akhtar, M. Rizwan, and S. Kale, "Multimodal biometric fusion: Performance under spoof attacks," *J. Intell. Syst.*, vol. 20, no. 4, pp. 353–372, 2011.

[89] Z. Akhtar, C. Micheloni, C. Piciarelli, and G. L. Foresti, "MoBio-LivDet: Mobile biometric liveness detection," in *Proc. IEEE Int. Conf. Adv. Video Signal-Based Surveill. (AVSS)*, Aug. 2014, pp. 187–192.

[90] P. Coli, G. L. Marcialis, and F. Roli, "Fingerprint silicon replicas: Static and dynamic features for vitality detection using an optical capture device," *Int. J. Image Graph.*, vol. 8, pp. 495–512, Jan. 2008.

[91] R. Cappelli, D. Maio, A. Lumini, and D. Maltoni, "Fingerprint image reconstruction from standard templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 9, pp. 1489–1503, Sep. 2007.

[92] S. Shah and A. Ross, "Generating synthetic irises by feature agglomeration," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Oct. 2006, pp. 317–320.

[93] J. Galbally, R. Plamondon, J. Fierrez, and J. Ortega-Garcia, "Synthetic on-line signature generation. Part I: Methodology and algorithms," *Pattern Recognit.*, vol. 45, no. 7, pp. 2610–2621, 2012.

[94] IBG, "Biometrics market and industry report 2009-2014," International Biometrics Group, Virginia, USA, Tech. Rep., Nov. 2008.

[95] B. Gipp, J. Beel, and I. Rössling, *ePassport: The World's New Electronic Passport*. Scotts Valley, CA, USA: CreateSpace, 2007.

[96] Ministerio del Interior, Gobierno de Espana. (2013). *DNI Electronico*. http://www.dnielectronico.es/Asi_es_el_dni_electronico/descripcion.html

[97] G. Aggarwal, S. Biswas, P. J. Flynn, and K. W. Bowyer, "A sparse representation approach to face matching across plastic surgery," in *Proc. Workshop Appl. Comput. Vis. (WACV)*, Jan. 2012, pp. 113–119.

[98] H. S. Bhatt, S. Bharadwaj, R. Singh, and M. Vatsa, "Recognizing surgically altered face images using multiobjective evolutionary algorithm," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 89–100, Jan. 2013.

[99] Y. Sun, M. Tistarelli, and D. Maltoni, "Structural similarity based image quality map for face recognition across plastic surgery," in *Proc. IEEE Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep./Oct. 2013, pp. 1–8.

[100] R. Singh, M. Vatsa, H. S. Bhatt, S. Bharadwaj, A. Noore, and S. S. Nooreyezdan, "Plastic surgery: A new dimension to face recognition," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 441–448, Sep. 2010.

[101] A. Dantcheva, C. Chen, and A. Ross, "Can facial cosmetics affect the matching accuracy of face recognition systems?" in *Proc. IEEE 5th Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep. 2013, pp. 391–398.

[102] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in *Proc. Eur. Conf. Comput. Vis. (ECCV)*, vol. LNCS 6316. 2010, pp. 504–517.

[103] K. Kollreider, H. Fronthaler, and J. Bigun, "Evaluating liveness by face images and the structure tensor," in *Proc. IEEE Workshop Autom. Identificat. Adv. Technol. (AutoID)*, Oct. 2005, pp. 75–80.

[104] I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," in *Proc. IEEE Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2012, pp. 1–7.

[105] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, and S. Z. Li, "A face antispoofing database with diverse attacks," in *Proc. IAPR Int. Conf. Biometrics (ICB)*, Mar./Apr. 2012, pp. 26–31.

[106] Y. Kim, J. Na, S. Yoon, and J. Yi, "Masked fake face detection using radiance measurements," *J. Opt. Soc. Amer.*, vol. 26, no. 4, pp. 760–766, Apr. 2009.

[107] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," in *Proc. IEEE Biometrics, Theory, Appl. Syst. (BTAS)*, Sep./Oct. 2013, pp. 1–6.

[108] N. Kose and J.-L. Dugelay, "On the vulnerability of face recognition systems to spoofing mask attacks," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2013, pp. 2357–2361.

[109] N. Erdogmus and S. Marcel, "Spoofing face recognition with 3D masks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 7, pp. 1084–1097, Jul. 2014.

[110] N. Erdogmus and S. Marcel, "Spoofing 2D face recognition systems with 3D masks," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2013, pp. 1–8.

[111] B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad illumination conditions," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2011, pp. 3557–3560.

[112] V. Vijayan *et al.*, "Twins 3D face recognition challenge," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–7.

[113] P. J. Phillips *et al.*, "Distinguishing identical twins by face recognition," in *Proc. IEEE Int. Conf. Autom. Face Gesture Recognit. Workshops (FG)*, Mar. 2011, pp. 185–192.

[114] B. Klare, A. A. Paulino, and A. K. Jain, "Analysis of facial features in identical twins," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–8.

[115] Z. Sun, A. A. Paulino, J. Feng, Z. Chai, T. Tan, and A. K. Jain, "A study of multibiometric traits of identical twins," in *Proc. SPIE, Biometric Technol. Human Identification (BTHI)*, vol. 7667. Apr. 2010, p. 76670T.

[116] G. Chetty and M. Wagner, "Liveness detection using cross-modal correlations in face-voice person authentication," in *Proc. Annu. Conf. Int. Speech Commun. Assoc. (INTERSPEECH)*, 2005, pp. 2181–2184.

[117] C. Sanderson, "The VidTIMIT database," IDIAP Inst. Res., Martigny, Switzerland, Tech. Rep. Idiap-Com-06-2002, 2002.

[118] G. Chetty and M. Wagner, "UCBN: A new audio-visual broadcast news corpus for multimodal speaker verification studies," in *Proc. Austral. Int. Conf. Speech Sci. Technol. (AICST)*, 2005, pp. 281–286.

[119] K. Kollreider, H. Fronthaler, and J. Bigun, "Verifying liveness by multiple experts in face biometrics," in *Proc. IEEE Int. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2008, pp. 1–6.

[120] Z. Zhang, D. Yi, Z. Lei, and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," in *Proc. IEEE Int. Conf. Autom. Face Gesture Recognit. (AFGR)*, Mar. 2011, pp. 436–441.

[121] N. Kose and J.-L. Dugelay, "Reflectance analysis based countermeasure technique to detect face mask attacks," in *Proc. IEEE Int. Conf. Digit. Signal Process. (DSP)*, Jul. 2013, pp. 1–6.

[122] T. I. Dhamecha, A. Nigam, R. Singh, and M. Vatsa, "Disguise detection and face recognition in visible and thermal spectrums," in *Proc. IEEE Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–8.

[123] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera," in *Proc. IEEE 11th Int. Conf. Comput. Vis. (ICCV)*, Oct. 2007, pp. 1–8.

[124] M. de Marsico, M. Nappi, D. Riccio, and J. Dugelay, "Moving face spoofing detection via 3D projective invariants," in *Proc. IEEE Int. Conf Biometrics (ICB)*, Mar./Apr. 2012, pp. 73–78.

[125] T. de Freitas Pereira, A. Anjos, J. M. de Martino, and S. Marcel, "LBP-TOP based countermeasure against face spoofing attacks," in *Proc. Int. Workshop Comput. Vis. Local Binary Pattern Variants (ACCV)*, Nov. 2012, pp. 1–12.

[126] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in *Proc. IEEE Int. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2013, pp. 105–110.

[127] J. Määttä, A. Hadid, and M. Pietikäinen, "Face spoofing detection from single images using texture and local shape analysis," *IET Biometrics*, vol. 1, no. 1, pp. 3–10, Mar. 2012.

[128] J. Komulainen, A. Hadid, and M. Pietikainen, "Context based face anti-spoofing," in *Proc. IEEE 6th Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep./Oct. 2013, pp. 1–8.

[129] I. Pavlidis and P. Symosek, "The imaging issue in an automatic face/disguise detection system," in *Proc. IEEE Workshop Comput. Vis. Beyond Vis. Spectr., Methods Appl.*, Jun. 2000, pp. 15–24.

[130] M. M. Chakka *et al.*, "Competition on counter measures to 2-D facial spoofing attacks," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–6.

[131] H.-K. Jee, S.-U. Jung, and J.-H. Yoo, "Liveness detection for embedded face recognition system," *Int. J. Biol. Life Sci.*, vol. 1, no. 4, pp. 235–238, 2005.

[132] J.-W. Li, "Eye blink detection based on multiple Gabor response waves," in *Proc. IEEE Int. Conf. Mach. Learn. Cybern. (ICMLC)*, Jul. 2008, pp. 2852–2856.

[133] L. Wang, X. Ding, and C. Fang, "Face live detection method based on physiological motion analysis," *Tsinghua Sci. Technol.*, vol. 14, no. 6, pp. 685–690, Dec. 2009.

[134] J. Bigun, H. Fronthaler, and K. Kollreider, "Assuring liveness in biometric identity authentication by real-time face tracking," in *Proc. IEEE Int. Conf. Comput. Intell. Homeland Secur. Pers. Safety (CIHSPS)*, Jul. 2004, pp. 104–111.

[135] A. Ali, F. Deravi, and S. Hoque, "Liveness detection using gaze collinearity," in *Proc. IEEE Int. Conf. Emerg. Secur. Technol. (ICEST)*, Sep. 2012, pp. 62–65.

[136] W. Bao, H. Li, N. Li, and W. Jiang, "A liveness detection method for face recognition based on optical flow field," in *Proc. Int. Conf. Image Anal. Signal Process. (ICIASP)*, Apr. 2009, pp. 233–236.

[137] A. Anjos, M. M. Chakka, and S. Marcel, "Motion-based countermeasures to photo attacks in face recognition," *IET Biometrics*, vol. 3, no. 3, pp. 147–158, Sep. 2014.

[138] T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection using 3D structure recovered from a single camera," in *Proc. IEEE/IAPR Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–6.

[139] Y. Kim, J.-H. Yoo, and K. Choi, "A motion and similarity-based fake detection method for biometric face recognition systems," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2011, pp. 171–172.

[140] G. Pan, L. Sun, Z. Wu, and Y. Wang, "Monocular camera-based face liveness detection by combining eyeblink and scene context," *Telecommun. Syst.*, vol. 47, nos. 3–4, pp. 215–225, 2011.

[141] J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Z. Li, "Face liveness detection by exploring multiple scenic clues," in *Proc. 12th Int. Conf. Control, Autom., Robot. Vis. (ICARCV)*, Dec. 2012, pp. 188–193.

[142] A. da Silva Pinto, H. Pedrini, W. Schwartz, and A. Rocha, "Video-based face spoofing detection through visual rhythm analysis," in *Proc. 25th Conf. Graph., Patterns Images (SIBGRAPI)*, Aug. 2012, pp. 221–228.

[143] J. Komulainen, A. Hadid, and M. Pietikäinen, "Face spoofing detection using dynamic texture," in *Proc. Asian Conf. Comput. Vis. Workshops (ACCV-W)*, vol. 7728. 2012, pp. 146–157.

[144] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra," in *Proc. SPIE, Biometric Technol. Human Identification (BTHI)*, vol. 5404. Aug. 2004, pp. 296–303.

[145] W. R. Schwartz, A. Rocha, and H. Pedrini, "Face spoofing detection through partial least squares and low-level descriptors," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–8.

[146] J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection with component dependent descriptor," in *Proc. IEEE/IAPR Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–6.

[147] N. Kose and J. Dugelay, "Classification of captured and recaptured images to detect photograph spoofing," in *Proc. IEEE Int. Conf Inform., Electron. Vis. (ICIEV)*, May 2012, pp. 1027–1032.

[148] J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, "Is physics-based liveness detection truly possible with a single image?" in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May/Jun. 2010, pp. 3425–3428.

[149] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–7.

[150] S. Kim, S. Yu, K. Kim, Y. Ban, and S. Lee, "Face liveness detection using variable focusing," in *Proc. IEEE/IAPR Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–6.

[151] G. Kim, S. Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J. Kim, "Face liveness detection based on texture and frequency analyses," in *Proc. 5th IAPR Int. Conf. Biometrics (ICB)*, Mar./Apr. 2012, pp. 62–72.

[152] F. J. Prokoski and R. B. Biel, "Infrared identification of faces and body parts," in *Biometrics: Personal Identification in Networked Society*. Boston, MA, USA: Kluwer, 1999, pp. 191–212.

[153] P. Buddharaju, I. T. Pavlidis, P. Tsiamyrtzis, and M. Bazakos, "Physiology-based face recognition in the thermal infrared spectrum," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 613–626, Apr. 2007.

[154] G. Hermosilla, J. Ruiz-del-Solar, R. Verschae, and M. Correa, "A comparative study of thermal face recognition methods in unconstrained environments," *Pattern Recognit.*, vol. 45, no. 7, pp. 2445–2459, 2012.

[155] A. Seal, S. Ganguly, D. Bhattacharjee, M. Nasipuri, and D. K. Basu, "Automated thermal face recognition based on minutiae extraction," *Int. J. Comput. Intell. Stud.*, vol. 2, no. 2, pp. 133–156, 2013.

[156] K. W. Bowyer, K. Chang, and P. Flynn, "A survey of approaches and challenges in 3D and multi-modal 3D+2D face recognition," *Comput. Vis. Image Understand.*, vol. 101, no. 1, pp. 1–15, 2006.

[157] N. Kose and J.-L. Dugelay, "Shape and texture based countermeasure to protect face recognition systems against mask attacks," in *Proc. IEEE Int. Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2013, pp. 111–116.

[158] N. Kose and J.-L. Dugelay, "Countermeasure for the protection of face recognition systems against mask attacks," in *Proc. 10th IEEE Int. Conf. Workshops Autom. Face Gesture Recognit. (FG)*, Apr. 2013, pp. 1–6.

[159] L. Sun, W. Huang, and M. Wu, "TIR/VIS correlation for liveness detection in face recognition," in *Proc. 14th Int. Conf. Comput. Anal. Images Pattern (CAIP)*, 2011, pp. 114–121.

[160] C. C. Chibelushi, F. Deravi, and J. S. D. Mason, "A review of speech-based bimodal recognition," *IEEE Trans. Multimedia*, vol. 4, no. 1, pp. 23–37, Mar. 2002.

[161] G. Chetty and M. Wagner, "'Liveness' verification in audio-video authentication," in *Proc. 8th Int. Conf. Spoken Lang. Process. (ICSLP)*, 2004, pp. 2509–2512.

[162] E. A. Rúa, H. Bredin, C. G. Mateo, G. Chollet, and D. G. Jiménez, "Audio-visual speech asynchrony detection using co-inertia analysis and coupled hidden Markov models," *Pattern Anal. Appl.*, vol. 12, no. 3, pp. 271–284, 2009.

[163] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-time face detection and motion analysis with application in 'liveness' assessment," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 548–558, Sep. 2007.

[164] I. Chingovska, A. Anjos, and S. Marcel, "Anti-spoofing in action: Joint operation with a verification system," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2013, pp. 98–104.

[165] T. de Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "Can face anti-spoofing countermeasures work in a real world scenario?" in *Proc. IEEE Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–8.

[166] R. Tronci *et al.*, "Fusion of multiple clues for photo-attack detection in face recognition systems," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Oct. 2011, pp. 1–6.

[167] J. Komulainen, A. Hadid, M. Pietikainen, A. Anjos, and S. Marcel, "Complementary countermeasures for detecting scenic face spoofing attacks," in *Proc. IEEE/IAPR Int. Conf. Biometrics (ICB)*, Jun. 2013, pp. 1–7.

[168] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*. New York, NY, USA: Springer-Verlag, 2001.

[169] G. L. Marcialis *et al.*, "First international fingerprint liveness detection competition—LivDet 2009," in *Proc. 15th IAPR Int. Conf. Image Anal. Process. (ICIAP)*, 2009, pp. 12–23.

[170] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers, "LivDet 2011—Fingerprint liveness detection competition 2011," in *Proc. Int. Joint Conf. Biometrics (IJCB)*, 2011.

[171] R. Bodade and S. Talbar, "Dynamic iris localisation: A novel approach suitable for fake iris detection," *Int. J. Comput. Inf. Syst. Ind. Manage. Appl.*, vol. 2, pp. 163–173, 2010.

[172] H. Zhang, Z. Sun, and T. Tan, "Contact lens detection based on weighted LBP," in *Proc. 20th Int. Conf. Pattern Recognition (ICPR)*, 2010, pp. 4279–4282.

[173] H. Zhang, Z. Sun, T. Tan, and J. Wang, "Learning hierarchical visual codebook for iris liveness detection," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, 2011, pp. 1–6.

[174] R. Bodade and S. Talbar, "Fake iris detection: A holistic approach," *Int. J. Comput. Appl.*, vol. 19, p. 1, Apr. 2011.

[175] A. J. Mansfield and J. L. Wayman, "Best practices in testing and reporting performance of biometric devices," CESG, Nat. Phys. Lab., Teddington, U.K., NPL Tech. Rep. CMSC 14/02, Aug. 2002. [Online]. Available: http://www.npl.co.uk/upload/pdf/biometrics_bestprac_v2_1.pdf

[176] A. S. Georghiades, P. N. Belhumeur, and D. J. Kriegman, "From few to many: Illumination cone models for face recognition under variable lighting and pose," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 6, pp. 643–660, Jun. 2001.

[177] EAB, "iPhone 5S: Heralding a paradigm shift?" Eur. Assoc. Biometrics, Naarden, The Netherlands, Tech. Rep., 2013. [Online]. Available: http://www.eab.org/

[178] A. Kerckhoffs, "La cryptographie militaire," *J. Sci. Militaires*, vol. 9, pp. 5–83, Jan./Feb. 1883. [Online]. Available: http://www.petitcolas.net/fabien/kerckhoffs/#english

[179] B. Schneier, *Secrets & Lies: Digital Security in a Networked World*. New York, NY, USA: Wiley, 2000.

[180] BWG, "Biometric security concerns, v1.0," CESG, London, U.K., Tech. Rep., 2003.

[181] B. Fernandez-Saavedra, R. Sanchez-Reillo, R. Alonso-Moreno, and C. Sanchez-Avila, "Evaluation methodology for fake samples detection in biometrics," in *Proc. 42nd Annu. IEEE Int. Carnahan Conf. Secur. Technol. (ICCST)*, Oct. 2008, pp. 233–240.

[182] E. Marasco, P. Johnson, C. Sansone, and S. Schuckers, "Increase the security of multibiometric systems by incorporating a spoofing detection algorithm in the fusion mechanism," in *Proc. 10th Int. Workshop Multiple Classifier Syst. (MCS)*, 2011, pp. 309–318.

[183] A. Rattani and N. Poh, "Biometric system design under zero and non-zero effort attacks," in *Proc. Int. Conf. Biometrics (ICB)*, 2013, pp. 1–8.

[184] E. Marasco, Y. Ding, and A. Ross, "Combining match scores with liveness values in a fingerprint verification system," in *Proc. IEEE 5th Int. Conf. Biometrics, Theory, Appl. Syst. (BTAS)*, Sep. 2012, pp. 418–425.

[185] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," *IEEE Trans. Image Process.*, vol. 23, no. 2, pp. 710–724, Feb. 2014.

[186] A. C. Doyle, "The adventure of the Norwood builder," in *The Return of Sherlock Holmes*, Strand Magazine, London, U.K., 1903.

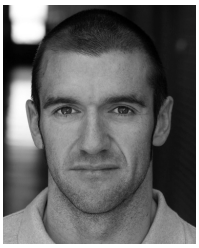
[187] H. Cummins, "Counterfeit finger-prints," *J. Criminal Law Criminol.*, vol. 25, no. 4, pp. 665–671, 1934.

[188] B. Geller, J. Almog, and P. Margot, "Fingerprint forgery—A survey," *J. Forensic Sci.*, vol. 46, no. 3, pp. 731–733, 2001.

[189] S. Kiltz, M. Hildebrandt, J. Dittmann, C. Vielhauer, and C. Kraetzer, "Printed fingerprints: A framework and first results towards detection of artificially printed latent fingerprints for forensics," in *Proc. SPIE, Image Quality Syst. Perform. VIII (IQSP)*, vol. 7867. Jan. 2011, p. 78670U.

[190] M. Hildebrandt, S. Kiltz, J. Sturm, J. Dittmann, and C. Vielhauer, "High-resolution printed amino acid traces: A first-feature extraction approach for fingerprint forgery detection," in *Proc. SPIE, Media Watermarking, Secur., Forensics (MWSF)*, vol. 8303. Feb. 2012, p. 83030J.

[191] M. Hildebrandt, S. Kiltz, and J. Dittmann, "Printed fingerprints at crime scenes: A faster detection of malicious traces using scans of confocal microscopes," in *Proc. SPIE, Media Watermarking, Secur., Forensics (MWSF)*, vol. 8665, Mar. 2013, p. 866509.



JAVIER GALBALLY received the M.Sc. degree in electrical engineering from the Universidad de Cantabria, Santander, Spain, in 2005, and the Ph.D. degree in electrical engineering from the Universidad Autónoma de Madrid, Madrid, Spain, in 2009, where he was an Assistant Professor until 2012. In 2013, he joined the Joint Research Centre of the European Commission, Seville, Spain, where he is currently a Post-Doctoral Researcher. He has carried out different research internships at worldwide leading groups in biometric recognition, such as BioLab, Universitá di Bologna, Bologna, Italy, the IDIAP Research Institute, Martigny, Switzerland, and the Scribens Laboratory, École Polytechnique de Montréal, Montreal, QC, Canada, or the Integrated Pattern Recognition and Biometrics Laboratory, West Virginia University, Morgantown, WV, USA. His research interests are mainly focused on the security evaluation of biometric systems, but also include pattern and biometric recognition, synthetic generation of biometric traits, and inverse biometrics. He is actively involved in European projects focused on biometrics. He was a recipient of a number of distinctions, including the IBM Best Student Paper Award at ICPR 2008, a finalist of the EBF European Biometric Research Award 2009, and the Best Ph.D. Thesis Award by the Universidad Autónoma de Madrid 2010.

SÉBASTIEN MARCEL received the Ph.D. degree in signal processing from the Research Center of France Telecom (now Orange Labs), CNET, Université de Rennes I, Rennes, France, in 2000. He is currently a Senior Research Scientist with the IDIAP Research Institute, Martigny, Switzerland, where he leads the Biometrics Group and conducts research on multimodal biometrics, including face recognition, speaker recognition, vascular recognition, and spoofing and anti-spoofing. In 2010, he was appointed as a Visiting Professor with the University of Cagliari, Cagliari, Italy, where he taught a series of lectures in face recognition. In 2013, he was a Lecturer with the École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, where he taught Fundamentals in Statistical Pattern Recognition. He was the main organizer of a number of special scientific events or competitive evaluations all involving in biometrics, and serves as an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He is also the Principal Investigator of international research projects, including MOBIO, TABULA RASA, and BEAT. He leads the development of BOB, the signal processing and machine learning toolbox.

JULIAN FIERREZ received the M.Sc. and Ph.D. degrees in telecommunications engineering from the Universidad Politecnica de Madrid, Madrid, Spain, in 2001 and 2006, respectively. Since 2002, he has been affiliated with the Biometric Recognition Group (ATVS), Universidad Politecnica de Madrid, and the Universidad Autónoma de Madrid, Madrid, since 2004, where he is currently an Associate Professor. From 2007 to 2009, he was a Visiting Researcher with Michigan State University, East Lansing, MI, USA, under a Marie Curie Fellowship. His research interests and areas of expertise include signal and image processing, pattern recognition, and biometrics, with an emphasis on signature and fingerprint verification, multibiometrics, biometric databases, and system security. He has been and is actively involved in European projects focused on biometrics, and was a recipient of a number of distinctions for his research, including the Best Ph.D. Award in computer vision and pattern recognition from 2005 to 2007 by the IAPR Spanish Liaison (AERFAI), the Motorola Best Student Paper at ICB in 2006, the EBF European Biometric Industry Award in 2006, the IBM Best Student Paper at ICPR in 2008, and the EURASIP Best Ph.D. Award in 2012.