A Survey in Presentation Attack and Presentation Attack Detection

Anas Husseis, Judith Liu-Jimenez, Ines Goicoechea-Telleria, Raul Sanchez-Reillo

University Group for Identification Technologies

Carlos III University of Madrid

Madrid, Spain

{ahusseis, jliu, igoicoec, rsreillo}@ing.uc3m.es

***Abstract*—Biometric-based recognition has been replacing conventional recognition methods in security systems. Modern electronic devices such as smartphones and online services have been employing biometric systems because of their security, acceptability, and usability. However, the wide deployment of Biometrics raises security concerns including attacks that aim to interfere with a system's operation. This paper provides a review of potential threats which may affect biometric systems' security, particularly, Presentation Attack (PA). A general taxonomy of presentation attacks is proposed to cover different biometric modalities considering the attacker's intention and the presentation instrument. Moreover, Presentation Attack Detection (PAD) mechanisms that aim to eliminate or mitigate those attacks are also taxonomized. The taxonomy analyzes PAD mechanisms wherein the biometric trait pattern is considered to classify PAD methods. A state of the art study has been carried out to investigate PA and PAD for six biological and behavioral modalities.**

Keywords*— *Vulnerabilities, spoofing, presentation attack detection, liveness detection.

I. Introduction

Conceptually, Biometrics comes up with unparalleled physiological information (fingerprint, iris, face, etc.) and behavioral traits (signature, gait, keystroke, etc.) that can be used for the recognition process. Nonetheless, biometric systems are subject to attacks. Hence, many studies have exposed how vulnerable biometric systems are. Results have proved that an accurate biometric system is vulnerable due to the possibility of forging fake alternatives, which can be accepted by the system as genuine. On the other hand, PAD mechanisms have been also explored to distinguish the genuine from the forged biometric presentations, thus, the risk is mitigated.

Attacks on biometric systems may take place at any point on the system scheme. The first category of attacks is performed by presenting a manipulated trait at the biometric sensor, during the data collection process. A trait presentation that may interfere the system operation is defined as Presentation Attack (PA) [1], also known as direct attack or spoofing attack. Interfering with the system decision has two cases: (a) an attacker seeks to be recognized as a known individual to the system other than him/herself (imposter), (b) an attacker tries to conceal his/her identity to avoid being recognized as a known individual to the system (concealer).

The second attack category takes place within the digital processes of the system's interior parts, to be specific, seven points of digital attacks in the general biometric system are exposed in [2].

Note that in commercial devices that employ biometric sensors, biometric systems are considered as black boxes, since the operation inside the device is not publicly known. In this case, the potential attack is presentation attack, and the resulting decision, i.e. match or non-match, is the only obtained information.

Common Criteria evaluations analyze attacks potential to estimate the risk of specific attacks. Many factors impact the risk of an attack on any vulnerability [3], [4]: (1) Elapsed time: The required time to identify and exploit a vulnerability. (2) Expertise: attacker's knowledge about the target system and victim's biometric information. (3) Equipment and tools: the required hardware equipment and software tools to identify and exploit a vulnerability, which varies from standard to bespoke requirements. (4) the window of opportunity.

This survey contributes to the literature by compiling previous studies on biometric systems' security. Special attention is invested in exploring PA and PAD for different modalities, as well to illustrate security performance when PAD mechanisms take place. In fact, the generic taxonomies are not only limited to the covered modalities, PAs and PAD mechanisms but also it will be easy to fit any other modality or new PA/PAD method in the taxonomies.

Next section overviews biometric PAD evaluations and defines generic terms considering ISO/IEC 30107 standard parts. Section III outlines a general taxonomy for presentation attacks and presentation attack detection. Further exposition is provided in section IV and V about main up-to-date threats and solutions for physiological and behavioral modalities. Section VI conducts a discussion and summary of this article.

978-1-7281-1576-4/19/$31.00 ©2019 European Union

Part	Scope
Part 1: Framework	Provides a foundation for PA by setting up terms and definitions which helps to analyze and evaluate PAD mechanisms.
Part 2: Data formats	Setup data formats for conveying the type of approach used in PAD and for conveying the results of PAD mechanisms.
Part 3: Testing and reporting	(i) Principles and methods for performance assessments of PAD mechanisms. (ii) Reporting methodology for testing results from evaluations of PAD mechanisms. (iii) Categorization of known attacks.
Part 4: Profile for evaluation of mobile devices	assess the performance of PAD mechanisms on mobile devices. This part is currently under development.

Table 1 ISO/IEC 30107 parts [1], [6], [7].

II. BIOMETRIC SYSTEM SECURITY PERFORMANCE

Evaluations start with identifying two main foundations: the subject to be evaluated and the purpose of evaluation [5]. As this work focus on PA/PAD, we define the biometric sensor as the Item Under Test (IUT), and vulnerability assessment is the purpose of evaluation. Accordingly, Biometric testing and reporting working group (WG5) from the joint committee ISO/IEC JTC 1/SC 37, has recommended the standard ISO/IEC 30107 ‘‘Biometric presentation attack detection’’ for the aforementioned purpose.

ISO/IEC 30107 is four parts [1], [6], [7] that have been developed to provide a foundation about presentation attack detection, defines data formats and sets principles, methods and error metrics that assess PAD algorithms and mechanisms. The standard is divided into three parts as reported in Table 1.

A group of metrics has been established to be employed through PAD evaluation in biometric recognition systems. The proposed metrics aim to provide statistical measures that deal with three elements: (1) bona fide user (the legal user), (2) attacker, and (3) biometric system response.

Terms and metrics employed in this study are given in ISO/IEC (2382-37 and 30107), and here we expose the most used in this work:

- Biometric representation: a presentation of biometric sample or biometric feature set to the biometric sensor. Could be bona fide or attack presentation.
- Presentation Attack Instrument (PAI): class of presentation attack instruments created using a common production method. Many studies use the term ‘‘spoof’’, which informally refers to PAI;
- Attack type: element and characteristic of a presentation attack.
- Item Under Test IUT: an implementation that is the object of a test assertion or test case. The equivalent in Common Criteria evaluations is Target of Evaluation (ToE);
- Attack potential: a measure of the capability to attack a TOE;
- Attack Presentation Classification Error Rate (APCER): the proportion of attack presentations incorrectly classified as bona fide presentations;
- Bona Fide Presentation Classification Error Rate (BPCER): the proportion of bona fide presentations incorrectly classified as presentation attacks;
- Correct Classification Rate (CCR): The percentage of presentations Correctly Classified; (not defined in the standards, but it is used in previous studies as classifier’s accuracy measure)
- PAD subsystem evaluation: a measure of the PAD subsystem’s ability to correctly classify both attack presentations and bona fide presentations;
- Full system evaluation: a measure of the overall system’s ability to correctly recognize subjects, considering both PAD decision and matching score.
- Spoof, spoofing and anti-spoofing: informal vocabularies which are used in literature instead of PAI, PA, and PAD; subsequently.

III. PRESENTATION ATTACK AND PRESENTATION ATTACK DETECTION

What information does the sensor collect? And how does it capture the distinguishable information? Are The first two questions the attacker tries to answer, to raise the attack potential. The different elements of attack presentation resemble while investigating various biometric modalities, technologies, and sensors. The resemblance is due to the fact that claiming an identity requires presenting a PAI that contains the features of the bona fide user. Likewise, evading an identity necessitate manipulating the features of the real biometric trait. That implies that the only difference between attacking different biometric systems takes place while creating the PAI.

Various classifications such as [8]–[11], are proposed in literature to study PA and PAD mechanisms in individual modalities. Moreover, PAD mechanisms are mainly classified in literature as software or hardware solutions.

This study proposes a general taxonomy for presentation attack and presentation attack detection to cover all state of the art investigations in a way that helps to classify attacks and countermeasures. The proposed taxonomy leads to generalizing countermeasures which are sufficiently secured against different attack types.

A. *Presentation Attack Taxonomy*

Presentation attack is performed on the analogical domain, independently from the digital process of the biometric system. Therefore, digital protection mechanisms such as watermarking, hashing, digital signature, etc. are not helpful.

On the other hand, perceiving the intended meaning of performing a presentation is critical in analyzing presentation attacks. Two main classes can be established for presentation attack based on the user intent. Each class consists of different subclasses of attacks, taking into account the attack type (see Figure 1).

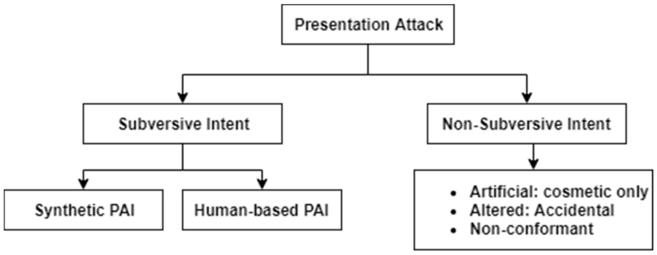

Figure 1 Presentation Attack taxonomy

1) Attacks with non-subversive intent: In this case, the subject performs a biometric presentation that may interfere the final decision of the recognition system. basically, no malicious intent is considered from the subject's standpoint. For example, using artificial products for cosmetic purposes, such as cosmetic contact lenses, may lead to suspicious detection. Furthermore, the genuine biometric trait might be altered because of accidental change like burns or scars. Unlimited to these cases, non-conformant presentations (e.g. non-attentive, poorly trained and careless users) are considered non-subversive; no malicious goal is assumed.

In research studies, although the attacker aims to trick the system by performing different types of attack, the goal is to enhance security by eliminating potential attacks.

2) Attacks with subversive intent: This category assumes that malicious purpose is intended by the attacker. The presented instrument could be synthesized or human-based, and yet it could be created with the cooperation of the genuine user. The proposed taxonomy details subversive attacks into subclasses based on attacks type.

a) Synthetic PAI: Synthesizing a PAI might be simple such as wearing sunglasses, or sophisticated like producing a 3D facial mask. Generally speaking, PAI can be seen from two different perspectives:

First, does PAI contain full or partial biometric information? Depending on attack type we may define the following types:

- Fully synthesized (complete) artefacts are created such that PAIs have identical features as real biometric traits. For instance, 3D masks and artificial eyes provide a 3D presentation which could bypass the system's countermeasures;
- partial samples are those samples that contain partial discriminative features and used later by a claim or evade an identity. For example, textured contact lens attack is a potential attack due to the fact that it has a 3D shape of the eye when it's being used by the attacker, furthermore, the correspondent eye behaves naturally.

Second, can PAI provide the dynamic information of real biometrics? The artefact may have dynamic changes or not, the attacker decides based on the attack type and ToE:

- Static artefact provides information of time instant for a biometric trait. Image attack on face or iris systems is a static attack;
- Dynamic artefact provides dynamic temporal information during the presentation. For instance, a video attack provides dynamic information that may succeed in the attack.

Previous classes result in four generic types of PAIs: (1) static complete instrument, (2) static partial instrument, (3) dynamic partial instrument, and (4) dynamic complete instrument. Examples of these classes are provided in Table 2.

b) Human-based PAI: instead of synthesizing a PAI, attackers may present live, dead, altered or imitated samples. One way to present a live sample occurs when coercing the genuine user to present his biometric sample to the sensor. Similarly, dead body parts (i.e. cadaver or severed parts) could be employed to overcome the biometric system, dead fingers are studied in [12]. Moreover, alterations on the attacker biometric trait are considered as a potential change which brings out different characteristics that result in a suspicious presentation (e.g. damaged on purpose, burns, plastic surgeries).

behavioral biometrics are also attainable, whereas attackers collect as much information as possible about the trait and try to imitate it at the biometric sensor. The dynamic handwritten signature is a significant example where the attacker aims to forge the graphical form of the signature while applying similar features such as speed, pressure, and orientation [13]–[15].

B. Presentation Attack Detection taxonomy

State of the art studies such as [8], [9], [11], classify PAD methods into three main classes based on the necessary tools to detect the attacks: (1) Hardware methods, where extra hardware components are embedded in the biometric sensor. (2) Software methods, where additional processes take place in order to analyze the acquired data, which support the decision process to mitigate presentation attacks. (3) Score level methods, mainly, the process is performed in the matcher to analyze the information that comes from biometric sensors, PAD mechanisms or a combination of both.

PAI source	PAI Type	Examples
Human-based	***Live sample***	Zero-effort attempt, (under coercion, drugged, unconscious) genuine.
	Dead body part	Pulled eye, severed hand or finger, cadaver part.
	Altered	Body part amputation, plastic surgeries, fingerprints switching.
	Behavioral	Forging handwritten signature, mimicking voice, gait imitation.
Synthetic	***static complete***	Printed image, display image, full head casting, artificial eye, static handwritten signature.
	static partial	Glasses, scarf, partial face image.
	dynamic partial	Cosmetic makeup, textured eye lenses, facial hair, dirty fingerprints.
	dynamic complete	Video attack, voice record, wearable 3D masks, forging a dynamic handwritten signature.

Table 2 Presentation Attack Instruments

From a different point of view, the proposed taxonomy analyses the basis of PAD mechanisms, and associates the exploited distinguishing information (see Figure 2). It is interesting to note that previous classifications integrate the proposed taxonomy to determine the used tools in any PAD mechanism.

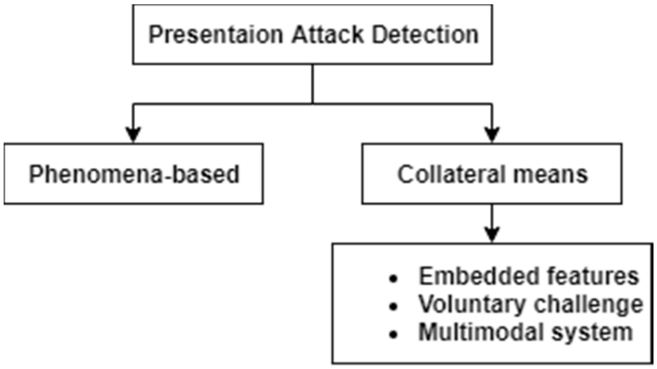

Figure 2 Presentation Attack Detection Taxonomy

As noticed until here, excellent knowledge about genuine biometric traits, biometric systems topology and presentation attack types, leads to establish PAD mechanisms which analyze natural patterns or collateral information from the biometric presentation. The following expose these two fundamentals with examples for each.

1) Within sample phenomena: In addition to the unique discriminative pattern of a natural biometric trait, manifest and latent spatio-temporal information can be extracted. Case in point, the human face has a unique 3D geometry that has specific characteristics and capable of responding to environmental conditions; unconscious responses like eye blinking. This definition of face extends the meaning for face biometric trait.

Furthermore, vein pattern is recognized by blood flow in vein network, in this case, dynamic acquisition might be utilized to prove the trait liveness.

2) Collateral means : This group focuses on the acquired biometric sample to be a source of extra information, which could be exploited to classify bona fide and attack presentations. Collateral information is not necessarily provided in natural presentations, other types of collateral means might be included in voluntary challenge response and multimode composition.

a) Embedded features: implicit means exist on each biometric presentation. Distortion analysis, texture analysis, and quality measures are popular and widely investigated tools in the context of PAD development.

b) Voluntary challenge: humans are capable to respond to voluntary requests like mouth and eye movement [16], where the PAD mechanism analysis the response to eliminate potential attacks.

c) Multimodal biometrics: different combinations of biometric modalities are proposed in the literature, proposing enhancement in the overall security of the biometric system [17]–[19]. The system acquires different traits and combines mechanism results to take a decision that verifies or reject the presentation.

Literature exposes massive researches on software solutions compared to those studies on hardware solutions. Software solutions are proposed on testing datasets of biometric sensors without any need to modify the original design of the sensor, which means no additional cost on the overall system. Moreover, software solutions assist the deployed commercial devices that use biometric recognition systems.

Next two sections explore presentation attacks and correspondent solutions that aim to eliminate or mitigate those attacks.

IV. State of the Art in Presentation Attack

PAIs can be prepared with or without the cooperation of genuine users. Furthermore, attacker's technical expertise and knowledge about the sensor's functionality will influence the strength of different PAI.

Based on the previous discussion this chapter provides a panorama view about the security of six biometric modalities, attack types and analysis.

A. Iris recognition

Iris recognition system may use visible-light [20]–[22] or near-infrared (NIR) illumination to acquire the iris sample. Systems that operate on visible light illumination had shown a major obstacle to localizing the pupil [23], especially, for eyes with high concentration of melanin. This is explained by the significant capability of melanin to absorb light. Currently, because of the high accuracy of NIR systems, all commercial sensors work on NIR illumination [10], [24].

Identifying the IUT technology directs the attacker to choose a PAI that may succeed in the intended PA. Two comprehensive surveys [10], [25] have been proposed to cover potential attacks on iris recognition system. Table 3 summarizes known attacks and connect them with the proposed taxonomy in Figure 1.

PAI type		PAI	REFERENCES
Synthetic	***Static complete***	Printed image	[26]–[28]
		Prosthetic Eye	[25], [29]–[33]
		Display image	[34]–[44]
	Dynamic Complete	Display video	
		Textured contact lens	(imposter)
	Dynamic Partial	Textured contact lens (cosmetic)	[45], [46] (concealer)
Human-based	***Non-Conformant***	Eye movement and rotation	[47]
		Actual eye affected by drugs	[48], [49]
	Cadavers	Cadaver eye	[50]–[52]
	Coercion	Presentation under coercion	-

Table 3 PA on iris recognition systems

Attack analysis:

- First and foremost, the attacker needs to analyze the sensor functionality, is it a visible light/ NIR sensor? Does the sensor apply NIR filtering?

- choosing a PAI comes subsequent to the analysis of previous point. As an illustration, all image and video attacks fall apart when attacking NIR system. An exception is shown in [53] where e-ink technology is used to attack a commercial sensor;

- concealers have demonstrated different methods to evade recognition. Cosmetic texture lenses have shown the capability to defeat the system. Further, excessive dilation of the eye's pupil has proved the feasibility of bypassing iris recognition systems [48];

- research has tended to mention potential attacks such as prosthetic eye and textured contact lens as impersonate attacks. These attacks require high expertise, advanced tools and long time to prepare the PAI.

B. Fingerprint recognition

In the literature, there are many studies have been carried out to prove the feasibility of creating an artificial fingerprint from latent fingermarks [26], [54]–[57]. Recent investigation has demonstrated an imaging technique that revealed fingermarks on difficult substrates, an exceptional level of detail has been obtained after over 26 days of deposition [58].

Biometric society is aware of this threat, and currently, many researchers are conducting presentation attack experiments to estimate the risk of such attacks. Often, those studies are performed with the cooperation of subjects, where a mold of fingermarks is taken directly from the real finger [54]–[57], [59]–[65].

Various reviews of the literature on fingerprint presentation attack have been carried out in [11], [66], [67], to investigate the system's vulnerabilities and classify corresponding threats and countermeasures. Table 4 lists the investigated attack types, and it is followed by key observations.

PAI type		PAI
Synthetic	***Static complete***	Printed image
		Fingerprint reactivation
	Dynamic Complete	Artefacts
		Latent fingerprint
	Dynamic Partial	
Human-based	***Non-Conformant Use***	Side of a finger, presenting different finger (e.g. index instead of thumb)
	Cadavers	dead fingerprint
	Altered	Altered fingerprint
	Coercion	Bona fide presentation under coercion

Table 4 PA on fingerprint

Attack analysis:

- In [67] the authors exposed fingerprint sensing technologies and classified fingerprint acquisition into three categories: (1) swipe, (2) touch and (3) touchless. Under those circumstances, the attacker defines a suitable PAI to exploit the system's vulnerability;

- the combination of sensor's technology and acquisition method needs to be comprehended in order to (1) identify a PAI (2) perform attack presentation. Case in point, a touch capacitive sensor obliges the attacker to use conductive material to create the PAI, and it needs to keep the pattern while applying the pressure during the presentation;

- public information about fingerprint sensors might be limited, such as the fingerprint subsystem in mobile devices. despite fact that those subsystems are seen as black boxes, many evaluations are carried out to evaluate the system against the state of the art attacks [68]–[70];

- in supervised environments, the attacker must consider the visibility of PAI and its resistant to the environmental conditions. Some materials perform differently in different conditions (e.g. temperature, humidity, time, etc.).

C. Face recognition

Face recognition encounters diverse presentation attacks designed to manipulate the biometric system's decision. Similar to previous modalities, attacking face recognition starts with identifying the target sensor, i.e. 2D or 3D acquisition system. In fact, the human face has a unique 3D geometry and capable of performing physical movements and emotional expressions. Moreover, a man has unconscious facial responses for external events such as eye blinking.

Face recognition security occupies high attention since it has been deployed in many areas such as passport check and video surveillance. Surveys [8], [71] and book chapters [66] have been published to update the threats and solutions for face recognition systems. Table 5 classifies potential attacks based on Figure 1.

PAI type		PAI	REFERENCES
Synthetic	***Static partial***	Facial accessories	[72], [73], [74]
	Static complete	full head casting, static mask	
		Printed image	
		Display image	[75]–[78]
	Dynamic Complete	Display video	
		Wearable mask	[79]–[81]
	Dynamic Partial	Artificial and natural facial hair	[74], [82]
Human-based	***Non-Conformant***	facial expressions	[83]
	Altered	Plastic surgery, facial makeup	[84], [85], [86], [87]
	Live	Identical twin	[88], [89]
	Coercion	Presentation under coercion	-

Table 5 PA on face recognition systems

Attack analysis:

- Face recognition systems are either 2D or 3D acquisition-based. 3D acquisition requires a PAI that presents the 3D geometry of the genuine face;

- attack potential varies significantly when considering different systems. For example, cost, time, and required equipment for display attack are considerably affordable compared to those needed to create a 3D wearable mask;

- ongoing investigations are taking place on this domain, therefore, the attacker should consider that the target system has already countermeasures for different known attacks;

- using a PAI that provides the facial dynamics combined with 3D information might increase the attack strength.

D. *Vascular recognition*

In the 9th GBDe Summit, a study about the security of embedded black-box system was demonstrated [90], vein biometric systems were investigated, and the possibility of creating artificial traits was discussed as well. This work pointed out the need for further studies and evaluations to understand the deficiencies of vascular biometric systems.

Investigations have started with cooperative attacks, where researchers started performing PAs with the genuine user's cooperation. That is to test the system vulnerability against PAIs. As far as proposed in literature, the only presentation attack which performed on vascular biometric sensors is photo attack [91]–[93].

Attack analysis:

- Human tissues have a relatively low susceptibility to absorb infrared illumination, while the infrared absorption in blood vessels is high;

- near Infrared (NIR), and Far Infrared (FIR) imaging are used to extract the vein pattern from different parts of the body, as demonstrated on [94], [95];

- human veins network is not directly visible and requires specific devices to be captured;

- experiments like [92], [93], have proved the printed ink capability of absorbing infrared illumination. However, a printed image is a static source of information and it could be detected in PAD subsystem;

- at the present time, the risk of capturing images without the user acceptance or leaving biometric traces is not taken into account for vascular systems. We are not aware of commercial devices capable of capturing the vein network in real life scenarios.

E. *Handwritten signature forgery*

Handwritten signature forgery is a behavioral attack that is performed by a forger (i.e. human based), aiming to produce an identical graphical signature and temporal features like speed and pressure. Forging handwritten signatures is influenced by two main factors: complexity of the signature [96] and proficiency of the imposter [97].

A difficulty index has been proposed in [98] to evaluate a genuine signature vulnerability to imposter's attacks. In fact, the proposed "difficulty index" is completely independent from the quality of the forged sample which is produced by an imposter, and it contributes to measuring the challenge of imitating the genuine signature.

Imposters are classified in literature, depending on their knowledge and ability to forge a signature, to three main types [99]: (a) Random (Simple) forgery: imposter uses the victim name in order to generate a signature without any knowledge about the genuine signature; (b) causal forgery: the forger in this class has observed the genuine signature for a while then an imitation is performed based on the graphical memories of the imposter; (c) skilled forgery: imitating the signature is performed by a professional who has a prior knowledge about the genuine sample, and typically trains many times before performing the attack.

Attack analysis:

- Handwritten signature relies on the psychophysical status of the signer, which means that the signature can be slightly different under various conditions;

- handwritten signature modality is divided into two types: static and dynamic recognition. Static signature lies only on the graphical format, while dynamic signature is acquired by dedicated sensors which acquire extra temporal signals such as pressure, time, orientation, etc.

- dynamic signature [100], [101] provides higher accuracy compared to that obtained from static signature, this is due to exploiting temporal data that enhance the decision process, subsequently, the overall system becomes more robust to presentation attack [102];

- a skilled forger considers all previous comments to identify the target sensor and exploit the vulnerability.

F. *Automatic speaker recognition*

Speech is generally influenced by complex biological, social and regional factors. Aging, stress, colds, etc. are typical causes of voice variation which bring out more challenges for Automatic Speaker Verification (ASV) algorithms [103], [104]. In case of considering those cases as attacks, they would fit under alternated presentations with no malicious intent.

Literature exposes presentation attacks on ASV as shown in Table 6. These attacks are supposed to be performed with malicious intent; i.e. according to Figure 1 they are considered as subversive attacks with dynamic PAIs.

PAI type		PAI	REFERENCES
Synthetic	***Dynamic Complete***	Replay attack	[105]–[110]
		Speech synthesis	[111]–[115]
		Voice conversion	[116]–[123]
Human-Based	***Alternations***	Voice changes	[103], [104]
	Behavioral	Impersonation	[124]–[127]

Table 6 PA on speaker recognition systems

Attack analysis:

- Public sources such as social networks, TV, radio might be potentially used to analyze the victim's voice.

- mimicry artists can generate similar samples to the genuine ones, but not sufficiently comparable to spoof ASV systems [108];

- At the present time, recording devices and advanced audio-recording applications provide high-quality records. That simplifies the process of spying to a person and collect several speech samples;

- Voice conversion and speech synthesis show a threat toward ASV system as can be noticed from the references in Table 6.

V. State of the Art in Presentation Attack Detection

As stated in the previous chapter, the research is being undertaken in order to study presentation attacks and propose detection mechanisms to eliminate or mitigate those attacks. There is a vast amount of literature on presentation attack and presentation attack detection evaluations, which we introduce in this chapter and link those investigations to the proposed taxonomy.

The following subsections present a literature review about the proposed PAD mechanisms, and link them to the proposed taxonomy in Figure 2

A. *Mechanisms based on natural biometric phenomena*

The following table lists the proposed mechanisms that consider natural phenomena as distinguishing basis to address the issue of PA.

Modality	Method	Reference
Iris	Dynamic eye response	[28], [31], [109]–[116]
	3D geometry analysis	[28], [109], [117], [118],
Fingerprint	Perspiration analysis	[119]–[123]
	Pores detection	[122]
	Fingerprint coarseness	[123]
Face	Behavioral analysis	[114]–[119]
	3D geometry analysis	[129]–[131]
Vascular	Blood features	[127] [128]
	Motion magnification	[129]
Handwritten signature	Dynamic analysis	[14], [15], [100], [130], [131]

Table 7 PAD mechanisms based on natural phenomena

B. *Mechanisms based on collateral means*

1) Embadded features: Table 8 shows the different methods which have been investigated in the literature for the different modalities.

2) Voulentary challenge: biometric system's user is capable of performing simple actions while performing a biometric presentation. Eye and mouth movements, face rotation or any other councious response will be classified under this subclass [16], [115], [208], [209].

3) Multimodal systems: Independent biometric modalities might be combined in one biometric system such that different acquisition subsystems are employed to capture the user biometric data [210]. Theoretically, multimodal systems are supposed to provide high level of security[17]–[19], but nevertheless various investigations show that a multimodal system is vulnerable to presentation attack [211]–[213].

VI. Discussion

A serious concern is pointed out, which is the feasibility of stealing our biometric identities. Many factors impact the generation of efficient artefacts that can defeat the recognition system. The general taxonomy of presentation attacks is demonstrated in a way that helps to recognize any potential attack. Firstly, the intention of the user (genuine or attacker) is essential. Subversive intents mean to defeat and end up with a successful imposter or concealer try. On the other hand, non-subversive intents are still considered as suspicious presentations, while users are behaving normally by wearing commercial products for cosmetic purposes, facing accidents which causes problems in engaging with a system, or need more knowledge about the use of these systems.

Considering two major types of modalities: physiological and behavioral modalities, generating artefacts can take different directions. Presentation attacks are performed by creating a spoofing trait that contains static or dynamic information, depending on the recognition system topology, such that the PAI provides an identical pattern to the genuine sample. Additionally, the attacker here focuses on the biometric sensor specifications, the required hardware and software tools, and PAIs creation methodology.

At the same time, behavioral modalities demand the attacker has particular experience for each sample, this involves training on each target sample to get a high-quality spoof. Moreover, the dynamic information should be considered while applying the attack. We deduce that attackers consider and study many factors to defeat a recognition system, and the factors vary according to the biometric system and the genuine sample complexity. An exception appears when considering zero-effort attack, where the attacker invests no efforts to perform the attack.

As presented in sections IV and V, all modalities have been defeated by presentation attacks. Consequently, reliability of Biometrics as recognition systems is lower. Statistically speaking, evaluation measures of biometric systems security are degraded while considering presentation attack. Therefore, countermeasures have been developed and embedded in the system to boost the resistance of the system against spoofing attacks.

Literature exposes massive research on PAD mechanisms which have been reclassified in this paper. A novel PA and PAD taxonomies are proposed in section III to categorize the state of the art anti-spoofing methods. The base criteria we adopted to establish the taxonomy is the type of information used in the PAD mechanism. First class consists of the methods which analyze the natural features of the trait; i.e. features produced because of natural phenomena or any information from within the sample. Second class covers the rest of solutions which detect collateral information adding extra hardware or software to the system.

Hardware based methods requires modifications on the sensor in the biometric system, meaning that cooperation from the manufacturers is expected to deploy this type of solutions. Meanwhile the rest of solutions are proposed following testing of datasets on a biometric sensor without any need to modify the original design of the sensor, which means no additional cost on the overall system. This explains the relatively low quantity of hardware-based solutions compared to software-based solutions.

Acknowledgment

This work was supported by the EU Horizon 2020 Framework for Research and Innovation under Grant Agreement Number 675087 as part of the AMBER (enhAnced Mobile BiomEtRics) Marie Sklodowska-Curie project.

References

[1] "ISO/IEC 30107-3:2017 - Information technology -- Biometric presentation attack detection -- Part 3: Testing and reporting." .

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J., vol. 40, no. 3, pp. 614–634, 2001.

[3] P. M. Mell, K. A. Scarfone, and S. Romanosky, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," FIRST, 2007.

[4] "Common Methodology for Information Technology Security Evaluation," 2012.

[5] T. Dunstone, "Performance Testing and Reporting," in Biometric System and Data Analysis, Boston, MA: Springer US, 2009, pp. 81–97.

[6] "ISO/IEC 30107-1:2016 - Information technology -- Biometric presentation attack detection -- Part 1: Framework." .

[7] "ISO/IEC 30107-2:2017 - Information technology -- Biometric presentation attack detection -- Part 2: Data formats." .

[8] J. Galbally, S. Marcel, and J. Fierrez, "Biometric Antispoofing Methods: A Survey in Face Recognition," IEEE Access, vol. 2, pp. 1530–1552, 2014.

[9] J. Galbally and M. Gomez-Barrero, "A review of iris anti-spoofing," in 2016 4th International Conference on Biometrics and Forensics (IWBF), 2016, pp. 1–6.

[10] A. Czajka and K. W. Bowyer, "Presentation Attack Detection for Iris Recognition," ACM Comput. Surv., vol. 51, no. 4, pp. 1–35, Jul. 2018.

[11] E. Marasco and A. Ross, "A Survey on Antispoofing Schemes for Fingerprint Recognition Systems," ACM Comput. Surv., vol. 47, no. 2, pp. 1–36, Nov. 2014.

[12] P. Sengottuvelan and A. Wahi, "Analysis of Living and Dead Finger Impression Identification for Biometric Application," in International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007), 2007, pp. 466–470.

[13] R. Sanchez-Reillo, H. C. Quiros-Sandoval, J. Liu-Jimenez, and I. Goicoechea-Telleria, "Evaluation of strengths and weaknesses of dynamic handwritten signature recognition against forgeries," in 2015 International Carnahan Conference on Security Technology (ICCST), 2015, pp. 373–378.

[14] R. Sanchez-Reillo, H. C. Quiros-Sandoval, I. Goicoechea-Telleria, and W. Ponce-Hernandez, "Improving Presentation Attack Detection in Dynamic Handwritten Signature Biometrics," IEEE Access, vol. 5, pp. 20463–20469, 2017.

[15] R. Sanchez-Reillo, J. Liu-Jimenez, R. Blanco-Gonzalo, and O. Miguel-Hurtado, "Performance evaluation of handwritten signature recognition in mobile environments," IET Biometrics, vol. 3, no. 3, pp. 139–146, Sep. 2014.

[16] A. K. Singh, P. Joshi, and G. C. Nandi, "Face recognition with liveness detection using eye and mouth movement," in 2014 International Conference on Signal Propagation and Computer Technology (ICSPCT 2014), 2014, pp. 592–597.

[17] R. N. Rodrigues, L. L. Ling, and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks," J. Vis. Lang. Comput., vol. 20, no. 3, pp. 169–179, Jun. 2009.

[18] B. Biggio, Z. Akthar, G. Fumera, G. L. Marcialis, and F. Roli, "Robustness of multi-modal biometric verification systems under realistic spoofing attacks," in 2011 International Joint Conference on Biometrics (IJCB), 2011, pp. 1–6.

[19] Y. Wang, T. Tan, and A. K. Jain, "Combining Face and Iris Biometrics for Identity Verification."

[20] "MobBIO: A Multimodal Database Captured with a Portable Handheld Device," in Proceedings of the 9th International Conference on Computer Vision Theory and Applications, 2014, pp. 133–139.

[21] "SOCIA Lab. - Soft Computing and Image Analysis Group. 2004. Noisy Visible Wavelength Iris Image Databases (UBIRIS). (2004)." [Online]. Available: http://iris.di.ubi.pt/.

[22] M. Trokielewicz and E. Bartuzi, "Cross-spectral Iris Recognition for Mobile Applications using High-quality Color Images."

[23] "Biometric personal identification system based on iris analysis," Jul. 1991.

[24] G. W. Quinn, P. Grother, J. Matey, W. L. Ross, and W. Copan, "NISTIR 8207 IREX IX Part One Performance of Iris Recognition Algorithms NISTIR 8207 IREX IX Part One Performance of Iris Recognition Algorithms Executive Summary," 2018.

[25] J. Galbally and M. Gomez-Barrero, “A review of iris anti-spoofing,” in 2016 4th International Conference on Biometrics and Forensics (IWBF), 2016, pp. 1–6.

[26] L. Thalheim, J. Krissler, and P.-M. Ziegler, “Body Check: Biometric Access Protection Devices and their Programs Put to the Test.”

[27] 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,” Springer, Berlin, Heidelberg, 2008, pp. 181–190.

[28] A. Pacut and A. Czajka, “Aliveness Detection for IRIS Biometrics,” in Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology, 2006, pp. 122–129.

[29] A. Czajka, “Pupil Dynamics for Iris Liveness Detection,” IEEE Trans. Inf. Forensics Secur., vol. 10, no. 4, pp. 726–735, Apr. 2015.

[30] A. Czajka, “Iris Liveness Detection by Modeling Dynamic Pupil Features,” Springer, London, 2016, pp. 439–467.

[31] I. Rigas and O. V. Komogortsev, “Eye movement-driven defense against iris print-attacks,” Pattern Recognit. Lett., vol. 68, pp. 316–326, Dec. 2015.

[32] C.-H. Teng et al., “Liveness Detection: Iris,” in Encyclopedia of Biometrics, Boston, MA: Springer US, 2009, pp. 931–938.

[33] J. Zuo, N. A. Schmid, and X. Chen, “On Generation and Analysis of Synthetic Iris Images,” IEEE Trans. Inf. Forensics Secur., vol. 2, no. 1, pp. 77–90, Mar. 2007.

[34] W. S.-A. Fathy and H. S. Ali, “Entropy with Local Binary Patterns for Efficient Iris Liveness Detection,” Wirel. Pers. Commun., pp. 1–14, Dec. 2017.

[35] L. He, H. Li, F. Liu, N. Liu, Z. Sun, and Z. He, “Multi-patch convolution neural network for iris liveness detection,” in 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2016, pp. 1–7.

[36] J. Connell, N. Ratha, J. Gentile, and R. Bolle, “Fake iris detection using structured light,” in 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, 2013, pp. 8692–8696.

[37] X. He, Y. Lu, and P. Shi, “A New Fake Iris Detection Method,” Springer, Berlin, Heidelberg, 2009, pp. 1132–1139.

[38] X. Huang, C. Ti, Q. Hou, A. Tokuta, and R. Yang, “An experimental study of pupil constriction for liveness detection,” in 2013 IEEE Workshop on Applications of Computer Vision (WACV), 2013, pp. 252–258.

[39] M. Kumar and N. B. Puhan, “Iris liveness detection using texture segmentation,” in 2015 Fifth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG), 2015, pp. 1–4.

[40] M. De Marsico, D. Riccio, and H. Wechsler, “Mobile Iris Challenge Evaluation (MICHE)-I, biometric iris dataset and protocols,” Pattern Recognit. Lett., vol. 57, pp. 17–23, May 2015.

[41] A. F. Sequeira, J. Murari, and J. S. Cardoso, “Iris liveness detection methods in the mobile biometrics scenario,” in 2014 International Joint Conference on Neural Networks (IJCNN), 2014, pp. 3002–3008.

[42] A. F. Sequeira, S. Thavalengal, J. Ferryman, P. Corcoran, and J. S. Cardoso, “A realistic evaluation of iris presentation attack detection,” in 2016 39th International Conference on Telecommunications and Signal Processing (TSP), 2016, pp. 660–664.

[43] Y. N. Singh and S. K. Singh, “Vitality detection from biometrics: State-of-the-art,” in 2011 World Congress on Information and Communication Technologies, 2011, pp. 106–111.

[44] Z. Sun and T. Tan, “Iris Anti-spoofing,” Springer, London, 2014, pp. 103–123.

[45] J. DAUGMAN, “DEMODULATION BY COMPLEX-VALUED WAVELETS FOR STOCHASTIC PATTERN RECOGNITION,” Int. J. Wavelets, Multiresolution Inf. Process., vol. 01, no. 01, pp. 1–17, Mar. 2003.

[46] J. S. Doyle, P. J. Flynn, and K. W. Bowyer, “Automated classification of contact lens type in iris images,” in 2013 International Conference on Biometrics (ICB), 2013, pp. 1–6.

[47] A. Czajka, K. W. Bowyer, M. Krumdick, and R. G. VidalMata, “Recognition of Image-Orientation-Based Iris Spoofing,” IEEE Trans. Inf. Forensics Secur., vol. 12, no. 9, pp. 2184–2196, Sep. 2017.

[48] A. N. Al-Raisi and A. M. Al-Khouri, “Iris recognition and the challenge of homeland and border control security in UAE,” Telemat. Informatics, vol. 25, no. 2, pp. 117–132, May 2008.

[49] I. Tomeo-Reyes, A. Ross, and V. Chandran, “Investigating the impact of drug induced pupil dilation on automated iris recognition,” in 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2016, pp. 1–8.

[50] A. Sansola, “Postmortem iris recognition and its application in human identification,” 2015.

[51] M. Trokielewicz, A. Czajka, and P. Maciejewicz, “Human iris recognition in post-mortem subjects: Study and database,” in 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2016, pp. 1–6.

[52] M. Trokielewicz, A. Czajka, and P. Maciejewicz, “Post-mortem human iris recognition,” in 2016 International Conference on Biometrics (ICB), 2016, pp. 1–6.

[53] A. Czajka and K. W. Bowyer, “Presentation Attack Detection for Iris Recognition: An Assessment of the State of the Art,” Mar. 2018.

[54] T. Matsumoto, “Gummy and Conductive Silicone Rubber Fingers Importance of Vulnerability Analysis,” Springer, Berlin, Heidelberg, 2002, pp. 574–575.

[55] T. Putte and J. Keuning, “Biometrical Fingerprint Recognition: Don’t get your Fingers Burned,” in Smart Card Research and Advanced Applications, Boston, MA: Springer US, 2000, pp. 289–303.

[56] M. Espinoza, C. Champod, and P. Margot, “Vulnerabilities of fingerprint reader to fake fingerprints attacks,” Forensic Sci. Int., vol. 204, no. 1–3, pp. 41–49, Jan. 2011.

[57] T. Chugh, K. Cao, and A. K. Jain, “Fingerprint Spoof Buster: Use of Minutiae-Centered Patches,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 9, pp. 2190–2202, Sep. 2018.

[58] T. D. Thandauthapani, A. J. Reeve, A. S. Long, I. J. Turner, and J. S. Sharp, “Exposing latent fingermarks on problematic metal surfaces using time of flight secondary ion mass spectroscopy,” Sci. Justice, vol. 58, no. 6, pp. 405–414, Nov. 2018.

[59] I. Goicoechea-Telleria, J. Liu-Jimenez, H. Quiros-Sandoval, and R. Sanchez-Reillo, “Analysis of the attack potential in low cost spoofing of fingerprints,” in 2017 International Carnahan Conference on Security Technology (ICCST), 2017, pp. 1–6.

[60] C. Barral and A. Tria, “Fake Fingers in Fingerprint Recognition: Glycerin Supersedes Gelatin,” Springer, Berlin, Heidelberg, 2009, pp. 57–69.

[61] S. A. . Schuckers, “Spoofing and Anti-Spoofing Measures,” Inf. Secur. Tech. Rep., vol. 7, no. 4, pp. 56–62, Dec. 2002.

[62] M. Sandstrom, “Liveness Detection in Fingerprint Recognition Systems,” 2004.

[63] S. J. Elliott, S. K. Modi, L. Maccarone, M. R. Young, C. Jin, and H. Kim, “Image Quality and Minutiae Count Comparison for Genuine and Artificial Fingerprints,” in 2007 41st Annual IEEE International Carnahan Conference on Security Technology, 2007, pp. 30–36.

[64] J. Blommé, “Evaluation of biometric security systems against artificial fingers,” 2003.

[65] J. Spurny, M. Doleel, O. Kanich, M. Drahansky, and K. Shinoda, “New Materials for Spoofing Touch-Based Fingerprint Scanners,” in 2015 International Conference on Computer Application Technologies, 2015, pp. 207–211.

[66] S. Marcel, M. S. Nixon, J. Fierrez, and N. Evans, Handbook of biometric anti-spoofing : presentation attack detection. .

[67] C. Busch and C. Sousedik, “Presentation attack detection methods for fingerprint recognition systems: a survey,” IET Biometrics, vol. 3, no. 4, pp. 219–233, Dec. 2014.

[68] I. Goicoechea-Telleria, J. Liu-Jimenez, R. Sanchez-Reillo, and W. Ponce-Hemandez, “Vulnerabilities of biometric systems integrated in mobile devices: An evaluation,” in 2016 IEEE International Carnahan Conference on Security Technology (ICCST), 2016, pp. 1–8.

[69] I. Goicoechea-Telleria, A. Garcia-Peral, A. Husseis, and R. Sanchez-Reillo, “Presentation Attack Detection Evaluation on Mobile Devices: Simplest Approach for Capturing and Lifting a Latent Fingerprint,” in 2018 International Carnahan Conference on Security Technology (ICCST), 2018, pp. 1–5.

[70] R. B. Gonzalo et al., “Attacking a Smartphone Biometric Fingerprint System: A Novice’s Approach,” in 2018 International Carnahan Conference on Security Technology (ICCST), 2018, pp. 1–5.

[71] R. Ramachandra and C. Busch, “Presentation Attack Detection Methods for Face Recognition Systems,” ACM Comput. Surv., vol. 50, no. 1, pp. 1–37, Mar. 2017.

[72] R. Min, A. Hadid, and J.-L. Dugelay, “Improving the recognition of faces occluded by facial accessories,” in Face and Gesture 2011, 2011, pp. 442–447.

[73] H. Liu, H. Duan, H. Cui, and Y. Yin, “Face recognition using training data with artificial occlusions,” in 2016 Visual Communications and Image Processing (VCIP), 2016, pp. 1–4.

[74] M. Singh, R. Singh, M. Vatsa, N. Ratha, and R. Chellappa, “Recognizing Disguised Faces in the Wild,” Nov. 2018.

[75] J. Maatta, A. Hadid, and M. Pietikainen, “Face spoofing detection from single images using micro-texture analysis,” in 2011 International Joint Conference on Biometrics (IJCB), 2011, pp. 1–7.

[76] R. Raghavendra, K. Raja, S. Venkatesh, and C. Busch, “Face morphing versus face averaging: Vulnerability and detection,” in 2017 IEEE International Joint Conference on Biometrics (IJCB), 2017, pp. 555–563.

[77] R. Tronci et al., “Fusion of multiple clues for photo-attack detection in face recognition systems,” in 2011 International Joint Conference on Biometrics (IJCB), 2011, pp. 1–6.

[78] K. Patel, H. Han, A. K. Jain, and G. Ott, “Live face video vs. spoof face video: Use of moir&amp;#x00E9; patterns to detect replay video attacks,” in 2015 International Conference on Biometrics (ICB), 2015, pp. 98–105.

[79] N. Kose and J.-L. Dugelay, “On the vulnerability of face recognition systems to spoofing mask attacks,” in 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, 2013, pp. 2357–2361.

[80] N. Erdogmus and S. Marcel, “Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect,” in 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, pp. 1–6.

[81] N. Erdogmus and S. Marcel, “Spoofing Face Recognition With 3D Masks,” IEEE Trans. Inf. Forensics Secur., vol. 9, no. 7, pp. 1084–1097, Jul. 2014.

[82] T. I. Dhamecha, R. Singh, M. Vatsa, and A. Kumar, “Recognizing Disguised Faces: Human and Machine Evaluation,” PLoS One, vol. 9, no. 7, p. e99212, Jul. 2014.

[83] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, “Eigenfaces vs. Fisherfaces: recognition using class specific linear projection,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 7, pp. 711–720, Jul. 1997.

[84] R. Singh, M. Vatsa, and A. Noore, “Effect of plastic surgery on face recognition: A preliminary study,” in 2009 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, 2009, pp. 72–77.

[85] A. S. O. Ali, V. Sagayan, A. Malik, and A. Aziz, “Proposed face recognition system after plastic surgery,” IET Comput. Vis., vol. 10, no. 5, pp. 344–350, Aug. 2016.

[86] Z. Zheng and C. Kambhamettu, “Multi-level Feature Learning for Face Recognition under Makeup Changes,” in 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), 2017, pp. 918–923.

[87] Z. Zheng and G. Guo, “A joint optimization scheme to combine different levels of features for face recognition with makeup changes,” in 2016 IEEE International Conference on Image Processing (ICIP), 2016, pp. 3001–3005.

[88] A. Afaneh, F. Noroozi, and Ö. Toygar, “Recognition of identical twins using fusion of various facial feature extractors,” EURASIP J. Image Video Process., vol. 2017, no. 1, p. 81, Dec. 2017.

[89] P. J. Phillips et al., “Distinguishing identical twins by face recognition,” in Face and Gesture 2011, 2011, pp. 185–192.

[90] “gbd-e.org.” [Online]. Available: http://gbd-e.org/?domain=gbd-e.org?reqp=1&qaspoofip=163.117.174.163&reqp=1&reqr=. [Accessed: 14-Jun-2018].

[91] “VERA Palmvein Database.” [Online]. Available: https://www.idiap.ch/dataset/vera-palmvein. [Accessed: 14-Jun-2018].

[92] P. Tome and S. Marcel, “On the Vulnerability of Palm Vein Recognition to Spoofing Attacks.”

[93] P. Tome, M. Vanoni, and S. Marcel, “On the Vulnerability of Finger Vein Recognition to Spoofing.”

[94] J. M. Cross and C. L. Smith, “Thermographic imaging of the subcutaneous vascular network of the back of the hand for biometric identification,” in Proceedings The Institute of Electrical and Electronics Engineers. 29th Annual 1995 International Carnahan Conference on Security Technology, pp. 20–35.

[95] L. Wang and G. Leedham, “Near- and Far- Infrared Imaging for Vein Pattern Biometrics,” in 2006 IEEE International Conference on Video and Signal Based Surveillance, 2006, pp. 52–52.

[96] J.-J. Brault and R. Plamondon, “A complexity measure of handwritten curves: modeling of dynamic signature forgery,” IEEE Trans. Syst. Man. Cybern., vol. 23, no. 2, pp. 400–413, 1993.

[97] L. Ballard, D. Lopresti, and F. Monrose, “Forgery Quality and Its Implications for Behavioral Biometric Security,” IEEE Trans. Syst. Man Cybern. Part B, vol. 37, no. 5, pp. 1107–1118, Oct. 2007.

[98] J.-J. Brault and R. Plamondon, “How to detect problematic signers for automatic signature verification,” in Proceedings. International Carnahan Conference on Security Technology, pp. 127–132.

[99] G. Pirlo, “Algorithms for Signature Verification,” in Fundamentals in Handwriting Recognition, Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 435–454.

[100]M. Vatsa, R. Singh, P. Mitra, and A. Noore, “Signature Verification Using Static and Dynamic Features,” Springer, Berlin, Heidelberg, 2004, pp. 350–355.

[101]M. A. Ferrer, M. Diaz, C. Carmona-Duarte, and A. Morales, “A Behavioral Handwriting Model for Static and Dynamic Signature Synthesis,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 39, no. 6, pp. 1041–1053, Jun. 2017.

[102]R. Sanchez-Reillo, H. C. Quiros-Sandoval, J. Liu-Jimenez, and I. Goicoechea-Telleria, “Evaluation of strengths and weaknesses of dynamic handwritten signature recognition against forgeries,” in 2015 International Carnahan Conference on Security Technology (ICCST), 2015, pp. 373–378.

[103]E. Zetterholm, “Same speaker – different voices A study of one impersonator and some of his different imitations.”

[104]E. Zetterholm, K. P. H. Sullivan, and J. Van Doorn, “THE IMPACT OF SEMANTIC EXPECTATION ON THE ACCEPTANCE OF A VOICE IMITATION.”

[105]B. Gillett and S. King, “Transforming F0 Contours.”

[106]Chung-Hsien Wu, Chi-Chun Hsia, Te-Hsien Liu, and Jhing-Fa Wang, “Voice conversion using duration-embedded bi-HMMs for expressive speech synthesis,” IEEE Trans. Audio, Speech Lang. Process., vol. 14, no. 4, pp. 1109–1116, Jul. 2006.

[107]E. E. Helander and J. Nurminen, “A Novel Method for Prosody Prediction in Voice Conversion,” in 2007 IEEE International Conference on Acoustics, Speech and Signal Processing - ICASSP ’07, 2007, p. IV-509-IV-512.

[108]J. Mariéthoz and S. Bengio, “Can a Professional Imitator Fool a GMM-Based Speaker Verification System?” IDIAP, 2005.

[109]A. Czajka, “Making iris recognition more reliable and spoof resistant,” SPIE Newsroom, 2007.

[110]A. CZAJKA, A. PACUT, and M. CHOCHOWSKI, “METHOD OF EYE ALIVENESS TESTING AND DEVICE FOR EYE ALIVENESS TESTING,” Mar. 2008.

[111]F. M. Villalbos-Castaldi and E. Suaste-Gomez, "In the use of the spontaneous pupillary oscillations as a new biometric trait," in 2nd International Workshop on Biometrics and Forensics, 2014, pp. 1–6.

[112]N. K. Shaydyuk and T. Cleland, "Biometric identification via retina scanning with liveness detection using speckle contrast imaging," in 2016 IEEE International Carnahan Conference on Security Technology (ICCST), 2016, pp. 1–5.

[113]I. Rigas and O. V. Komogortsev, "Gaze estimation as a framework for iris liveness detection," in IEEE International Joint Conference on Biometrics, 2014, pp. 1–8.

[114]K. B. Raja, R. Raghavendra, and C. Busch, "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 10, pp. 2048–2056, Oct. 2015.

[115]O. V. Komogortsev, A. Karpov, and C. D. Holland, "Attack of Mechanical Replicas: Liveness Detection With Eye Movements," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 4, pp. 716–725, Apr. 2015.

[116]O. V. Komogortsev and A. Karpov, "Liveness detection via oculomotor plant characteristics: Attack of mechanical replicas," in 2013 International Conference on Biometrics (ICB), 2013, pp. 1–8.

[117]E. C. Lee and K. R. Park, "Fake iris detection based on 3D structure of iris pattern," Int. J. Imaging Syst. Technol., vol. 20, no. 2, pp. 162–166, May 2010.

[118]E. C. Lee, K. R. Park, and J. Kim, "Fake Iris Detection by Using Purkinje Image," Springer, Berlin, Heidelberg, 2005, pp. 397–403.

[119]Bozhao Tan and S. Schuckers, "Liveness Detection for Fingerprint Scanners Based on the Statistics of Wavelet Signal Processing," in 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), pp. 26–26.

[120]B. DeCann, B. Tan, and S. Schuckers, "A Novel Region Based Liveness Detection Approach for Fingerprint Scanners," Springer, Berlin, Heidelberg, 2009, pp. 627–636.

[121]A. Abhyankar and S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition," Pattern Recognit., vol. 42, no. 3, pp. 452–464, Mar. 2009.

[122]S. Memon, N. Manivannan, and W. Balachandran, "Active pore detection for liveness in fingerprint identification system," in 2011 19thTelecommunications Forum (TELFOR) Proceedings of Papers, 2011, pp. 619–622.

[123]Y. S. Moon, J. S. Chen, K. C. Chan, K. So, and K. C. Woo, "Wavelet based fingerprint liveness detection," Electron. Lett., vol. 41, no. 20, p. 1112, 2005.

[124]G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera," in 2007 IEEE 11th International Conference on Computer Vision, 2007, pp. 1–8.

[125]Wei Bao, Hong Li, Nan Li, and Wei Jiang, "A liveness detection method for face recognition based on optical flow field," in 2009 International Conference on Image Analysis and Signal Processing, 2009, pp. 233–236.

[126]X. Tan, Y. Li, J. Liu, and L. Jiang, "Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model," Springer, Berlin, Heidelberg, 2010, pp. 504–517.

[127]B. Qin, J. Pan, G. Cao, and G. Du, "The Anti-spoofing Study of Vein Identification System," in 2009 International Conference on Computational Intelligence and Security, 2009, pp. 357–360.

[128]J. Lee et al., "A finger-vein imaging and liveness detection for identity authentication using 2-axis MEMS scanner," in 2016 International Conference on Optical MEMS and Nanophotonics (OMN), 2016, pp. 1–2.

[129]R. Raghavendra, M. Avinash, S. Marcel, and C. Busch, "Finger vein liveness detection using motion magnification," in 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2015, pp. 1–7.

[130]S. J. Elliott, "Development of a biometric testing protocol for dynamic signature verification," in 7th International Conference on Control, Automation, Robotics and Vision, 2002. ICARCV 2002., vol. 2, pp. 782–787.

[131]R. Sanchez-Reillo, H. C. Quiros-Sandoval, J. Liu-Jimenez, and I. Goicoechea-Telleria, "Evaluation of strengths and weaknesses of dynamic handwritten signature recognition against forgeries," in 2015 International Carnahan Conference on Security Technology (ICCST), 2015, pp. 373–378.

[132]J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in 2012 5th IAPR International Conference on Biometrics (ICB), 2012, pp. 271–276.

[133]H. Zhang, Z. Sun, T. Tan, and J. Wang, "Learning Hierarchical Visual Codebook for Iris Liveness Detection."

[134]Z. Sun, H. Zhang, T. Tan, and J. Wang, "Iris Image Classification Based on Hierarchical Visual Codebook," IEEE Trans. Pattern Anal. Mach. Intell., vol. 36, no. 6, pp. 1120–1133, Jun. 2014.

[135]Z. Akhtar, C. Michelon, and G. L. Foresti, "Liveness detection for biometric authentication in mobile applications," in 2014 International Carnahan Conference on Security Technology (ICCST), 2014, pp. 1–6.

[136]Z. Akhtar, C. Micheloni, C. Piciarelli, and G. L. Foresti, "MoBio&amp;#x005F;LivDet: Mobile biometric liveness detection," in 2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), 2014, pp. 187–192.

[137]F. Alonso-Fernandez and J. Bigun, "Exploting periocular and RGB information in fake iris detection," in 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014, pp. 1354–1359.

[138]A. Das, U. Pal, M. A. Ferrer, and M. Blumenstein, "A framework for liveness detection for direct attacks in the visible spectrum for multimodal ocular biometrics," Pattern Recognit. Lett., vol. 82, pp. 232–241, Oct. 2016.

[139]D. Gragnaniello, C. Sansone, and L. Verdoliva, "Iris liveness detection for mobile devices based on local descriptors," Pattern Recognit. Lett., vol. 57, pp. 81–87, May 2015.

[140]A. P. S. Bhogal, D. Sollinger, P. Trung, and A. Uhl, "Non-reference image quality assessment for biometric presentation attack detection," in 2017 5th International Workshop on Biometrics and Forensics (IWBF), 2017, pp. 1–6.

[141]C. Chen and A. Ross, "A Multi-task Convolutional Neural Network for Joint Iris Detection and Presentation Attack Detection," in 2018 IEEE Winter Applications of Computer Vision Workshops (WACVW), 2018, pp. 44–51.

[142]A. Czajka, "Database of iris printouts and its application: Development of liveness detection method for iris recognition," in 2013 18th International Conference on Methods & Models in Automation & Robotics (MMAR), 2013, pp. 28–33.

[143]J. S. Doyle and K. W. Bowyer, "Robust Detection of Textured Contact Lenses in Iris Recognition Using BSIF," IEEE Access, vol. 3, pp. 1672–1683, 2015.

[144]J. S. Doyle, K. W. Bowyer, and P. J. Flynn, "Variation in accuracy of textured contact lens detection based on sensor and lens pattern," in 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, pp. 1–7.

[145]D. Yadav, N. Kohli, M. Vatsa, R. Singh, and A. Noore, "Unconstrained visible spectrum iris with textured contact lens variations: Database and benchmarking," in 2017 IEEE International Joint Conference on Biometrics (IJCB), 2017, pp. 574–580.

[146]J. Daugman, Biometrics. Personal Identification in a Networked Society, chapter Recognizing Persons by their Iris Patterns, pp. 103–121, Kluwer Academic Publishers, 1999. .

[147]S. J. Lee, K. R. Park, and J. Kim, "Robust Fake Iris Detection Based on Variation of the Reflectance Ratio Between the IRIS and the Sclera," in 2006 Biometrics Symposium: Special Session on Research at the Biometric Consortium Conference, 2006, pp. 1–6.

[148]J. H. Park and M. G. Kang, "Iris Recognition Against Counterfeit Attack Using Gradient Based Fusion of Multi-spectral Images," Springer, Berlin, Heidelberg, 2005, pp. 150–156.

[149]J. H. Park and M.-G. Kang, "Multispectral iris authentication system against counterfeit attack using gradient-based image fusion," Opt. Eng., vol. 46, no. 11, p. 117003, Nov. 2007.

[150]R. Chen, X. Lin, and T. Ding, “Liveness detection for iris recognition using multispectral images,” Pattern Recognit. Lett., vol. 33, no. 12, pp. 1513–1519, Sep. 2012.

[151]S.-H. Hsieh, Y.-H. Li, W. Wang, and C.-H. Tien, “A Novel Anti-Spoofing Solution for Iris Recognition Toward Cosmetic Contact Lens Attack Using Spectral ICA Analysis,” Sensors, vol. 18, no. 3, p. 795, Mar. 2018.

[152]S. Thavalengal, T. Nedelcu, P. Bigioi, and P. Corcoran, “Iris liveness detection for next generation smartphones,” IEEE Trans. Consum. Electron., vol. 62, no. 2, pp. 95–102, May 2016.

[153]A. Antonelli, R. Cappelli, D. Maio, and D. Maltoni, “Fake Finger Detection by Skin Distortion Analysis,” IEEE Trans. Inf. Forensics Secur., vol. 1, no. 3, pp. 360–373, Sep. 2006.

[154]J. Jia, L. Cai, K. Zhang, and D. Chen, “A New Approach to Fake Finger Detection Based on Skin Elasticity Analysis,” in Advances in Biometrics, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 309–318.

[155]Y. Zhang, J. Tian, X. Chen, X. Yang, and P. Shi, “Fake Finger Detection Based on Thin-Plate Spline Distortion Model,” in Advances in Biometrics, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 742–749.

[156]Eyung Lim, Xudong Jiang, and Weiyun Yau, “Fingerprint quality and validity analysis,” in Proceedings. International Conference on Image Processing, vol. 1, p. I-469-I-472.

[157]Y. Chen, S. C. Dass, and A. K. Jain, “Fingerprint Quality Indices for Predicting Authentication Performance,” Springer, Berlin, Heidelberg, 2005, pp. 160–170.

[158]Tai Pang Chen, Xudong Jiang, and Wei Yun Yau, “Fingerprint image quality analysis,” in 2004 International Conference on Image Processing, 2004. ICIP ’04., vol. 2, pp. 1253–1256.

[159]Lin Hong, Yifei Wan, and A. Jain, “Fingerprint image enhancement: algorithm and performance evaluation,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 20, no. 8, pp. 777–789, 1998.

[160]B. Sankur, B. Sankur, and K. Sayood, “Statistical evaluation of image quality measures,” J. Electron. Imaging, vol. 11, no. 2, p. 206, Apr. 2002.

[161]Q. Huynh-Thu and M. Ghanbari, “Scope of validity of PSNR in image/video quality assessment,” Electron. Lett., vol. 44, no. 13, p. 800, 2008.

[162]Susu Yao, Weisi Lin, EePing Ong, and Zhongkang Lu, “Contrast signal-to-noise ratio for image quality assessment,” in IEEE International Conference on Image Processing 2005, 2005, p. I-397.

[163]A. M. Eskicioglu and P. S. Fisher, “Image quality measures and their performance,” IEEE Trans. Commun., vol. 43, no. 12, pp. 2959–2965, 1995.

[164]M. G. Martini, C. T. E. R. Hewage, and B. Villarini, “Image quality assessment based on edge preservation,” Signal Process. Image Commun., vol. 27, no. 8, pp. 875–882, Sep. 2012.

[165]N. B. Nill and B. Bouzas, “Objective image quality measure derived from digital image power spectra,” Opt. Eng., vol. 31, no. 4, p. 813, 1992.

[166]Anmin Liu, Weisi Lin, and M. Narwaria, “Image Quality Assessment Based on Gradient Similarity,” IEEE Trans. Image Process., vol. 21, no. 4, pp. 1500–1512, Apr. 2012.

[167]R. Soundararajan and A. C. Bovik, “RRED Indices: Reduced Reference Entropic Differencing for Image Quality Assessment.”

[168]X. Zhu and P. Milanfar, “A NO-REFERENCE SHARPNESS METRIC SENSITIVE TO BLUR AND NOISE.”

[169]A. Abhyankar and S. Schuckers, “Fingerprint Liveness Detection Using Local Ridge Frequencies and Multiresolution Texture Analysis Techniques,” in 2006 International Conference on Image Processing, 2006, pp. 321–324.

[170]S. B. Nikam and S. Agarwal, “Curvelet-based fingerprint anti-spoofing,” Signal, Image Video Process., vol. 4, no. 1, pp. 75–87, Mar. 2010.

[171]P. Coli, G. L. Marcialis, and F. Roli, “Power spectrum-based fingerprint vitality detection,” in 2007 IEEE Workshop on Automatic Identification Advanced Technologies, 2007, pp. 169–173.

[172]C. Jin, H. Kim, and S. Elliott, “Liveness Detection of Fingerprint Based on Band-Selective Fourier Spectrum,” in Information Security and Cryptology - ICISC 2007, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 168–179.

[173]V. Ojansivu, E. Rahtu, and J. Heikkila, “Rotation invariant local phase quantization for blur insensitive texture analysis,” in 2008 19th International Conference on Pattern Recognition, 2008, pp. 1–4.

[174]V. Ojansivu and J. Heikkilä, “Blur Insensitive Texture Classification Using Local Phase Quantization,” Springer, Berlin, Heidelberg, 2008, pp. 236–243.

[175]J. G. Martins, L. S. Oliveira, and R. Sabourin, “Combining textural descriptors for forest species recognition,” in IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society, 2012, pp. 1483–1488.

[176]Y. Cheng and K. V. Larin, “Artificial fingerprint recognition by using optical coherence tomography with autocorrelation analysis,” Appl. Opt., vol. 45, no. 36, p. 9238, Dec. 2006.

[177]S. Chang, Y. Cheng, K. V. Larin, Y. Mao, S. Sherif, and C. Flueraru, “Optical coherence tomography used for security and fingerprint-sensing applications,” IET Image Process., vol. 2, no. 1, p. 48, 2008.

[178]A. Z. A. Aziz, H. Wei, and J. Ferryman, “Face anti-spoofing countermeasure: Efficient 2D materials classification using polarization imaging,” in 2017 5th International Workshop on Biometrics and Forensics (IWBF), 2017, pp. 1–6.

[179]L. Li, P. L. Correia, and A. Hadid, “Face recognition under spoofing attacks: countermeasures and research directions,” IET Biometrics, vol. 7, no. 1, pp. 3–14, Jan. 2018.

[180]T. Ahonen, A. Hadid, and M. Pietikainen, “Face Description with Local Binary Patterns: Application to Face Recognition,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 2037–2041, Dec. 2006.

[181]G. B. de Souza, D. F. da Silva Santos, R. G. Pires, A. N. Marana, and J. P. Papa, “Deep Texture Features for Robust Face Spoofing Detection,” IEEE Trans. Circuits Syst. II Express Briefs, vol. 64, no. 12, pp. 1397–1401, Dec. 2017.

[182]E. Fourati, W. Elloumi, and A. Chetouani, “Face anti-spoofing with image quality assessment,” in 2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART), 2017, pp. 1–4.

[183]H. Li, S. Wang, and A. C. Kot, “Face spoofing detection with image quality regression,” in 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA), 2016, pp. 1–6.

[184]C.-H. Yeh and H.-H. Chang, “Face Liveness Detection Based on Perceptual Image Quality Assessment Features with Multi-scale Analysis,” in 2018 IEEE Winter Conference on Applications of Computer Vision (WACV), 2018, pp. 49–56.

[185]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, no. 3–4, pp. 215–225, Aug. 2011.

[186]J. Komulainen, A. Hadid, and M. Pietikainen, “Context based face anti-spoofing,” in 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013, pp. 1–8.

[187]W. R. Schwartz, A. Rocha, and H. Pedrini, “Face spoofing detection through partial least squares and low-level descriptors,” in 2011 International Joint Conference on Biometrics (IJCB), 2011, pp. 1–8.

[188]R. Tronci et al., “Fusion of multiple clues for photo-attack detection in face recognition systems,” in 2011 International Joint Conference on Biometrics (IJCB), 2011, pp. 1–6.

[189]J. Li, Y. Wang, T. Tan, and A. K. Jain, “Live Face Detection Based on the Analysis of Fourier Spectra.”

[190]B. Peixoto, C. Michelassi, and A. Rocha, “Face liveness detection under bad illumination conditions,” in 2011 18th IEEE International Conference on Image Processing, 2011, pp. 3557–3560.

[191]Di Wen, Hu Han, and A. K. Jain, “Face Spoof Detection With Image Distortion Analysis,” IEEE Trans. Inf. Forensics Secur., vol. 10, no. 4, pp. 746–761, Apr. 2015.

[192]R. T. Tan and K. Ikeuchi, “Separating reflection components of textured surfaces using a single image,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 2, pp. 178–193, Feb. 2005.

[193]Z. Boulkenafet, J. Komulainen, and A. Hadid, “Face anti-spoofing based on color texture analysis,” in 2015 IEEE International Conference on Image Processing (ICIP), 2015, pp. 2636–2640.

[194]E. M. Rudd, M. Gunther, and T. E. Boult, “PARAPH: Presentation Attack Rejection by Analyzing Polarization Hypotheses,” in 2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2016, pp. 171–178.

[195]R. Raghavendra and C. Busch, “Presentation Attack Detection Algorithms for Finger Vein Biometrics: A Comprehensive Study,” in 2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), 2015, pp. 628–632.

[196]P. Tome et al., “The 1st Competition on Counter Measures to Finger Vein Spoofing Attacks,” in 2015 International Conference on Biometrics (ICB), 2015, pp. 513–518.

[197]L. Stoll and G. Doddington, “Hunting for Wolves in Speaker Recognition.”

[198]W. Shang and M. Stevenson, “Score normalization in playback attack detection,” in 2010 IEEE International Conference on Acoustics, Speech and Signal Processing, 2010, pp. 1678–1681.

[199]J. Villalba and E. Lleida, “Preventing replay attacks on speaker verification systems,” in 2011 Carnahan Conference on Security Technology, 2011, pp. 1–8.

[200]A. Paul, R. K. Das, R. Sinha, and S. R. M. Prasanna, “Countermeasure to handle replay attacks in practical speaker verification systems,” in 2016 International Conference on Signal Processing and Communications (SPCOM), 2016, pp. 1–5.

[201]C. H. E. E. (ELECO), 2017 10th, and undefined 2017, “Features and classifiers for replay spoofing attack detection,” ieeexplore.ieee.org.

[202]P. L. De Leon, I. Hernaez, I. Saratxaga, M. Pucher, and J. Yamagishi, “Detection of synthetic speech for the problem of imposture,” in 2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2011, pp. 4844–4847.

[203]Z. Wu, E. S. Chng, and H. Li, “Detecting Converted Speech and Natural Speech for anti-Spoofing Attack in Speaker Recognition.”

[204]Z. Wu, X. Xiao, E. S. Chng, and H. Li, “Synthetic speech detection using temporal modulation feature,” in 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, 2013, pp. 7234–7238.

[205]F. Alegre, A. Amehraye, and N. Evans, “Spoofing countermeasures to protect automatic speaker verification from voice conversion,” in 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, 2013, pp. 3068–3072.

[206]M. J. Correia, A. Abad, and I. Trancoso, “Preventing converted speech spoofing attacks in speaker verification,” in 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014, pp. 1320–1325.

[207]Z. Wu et al., “ASVspoof: The Automatic Speaker Verification Spoofing and Countermeasures Challenge,” IEEE J. Sel. Top. Signal Process., vol. 11, no. 4, pp. 588–604, Jun. 2017.

[208]W.-Y. Yau, H.-L. Tran, and E.-K. Teoh, “Fake finger detection using an electrotactile display system,” in 2008 10th International Conference on Control, Automation, Robotics and Vision, 2008, pp. 962–966.

[209]I. Rigas and O. V. Komogortsev, “Eye movement-driven defense against iris print-attacks,” Pattern Recognit. Lett., vol. 68, pp. 316–326, Dec. 2015.

[210]A. A. (Arun A. Ross, A. K. Jain, and K. Nandakumar, Handbook of Multibiometrics. .

[211]R. N. Rodrigues, L. L. Ling, and V. Govindaraju, “Robustness of multimodal biometric fusion methods against spoof attacks.”

[212]P. A. Johnson, B. Tan, and S. Schuckers, “Multimodal fusion vulnerability to non-zero effort (spoof) imposters,” in 2010 IEEE International Workshop on Information Forensics and Security, 2010, pp. 1–5.

[213]R. N. Rodrigues, N. Kamat, and V. Govindaraju, “Evaluation of biometric spoofing in a multimodal system,” in 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2010, pp. 1–5.