Chapter 5
Introduction to Presentation Attack Detection in Iris Biometrics and Recent Advances

Aythami Morales, Julian Fierrez, Javier Galbally, and Marta Gomez-Barrero

Abstract Iris recognition technology has attracted an increasing interest in the last decades in which we have witnessed a migration from research laboratories to real-world applications. The deployment of this technology raises questions about the main vulnerabilities and security threats related to these systems. Among these threats, presentation attacks stand out as some of the most relevant and studied. Presentation attacks can be defined as the presentation of human characteristics or artifacts directly to the capture device of a biometric system trying to interfere with its normal operation. In the case of the iris, these attacks include the use of real irises as well as artifacts with different levels of sophistication such as photographs or videos. This chapter introduces iris Presentation Attack Detection (PAD) methods that have been developed to reduce the risk posed by presentation attacks. First, we summarize the most popular types of attacks including the main challenges to address. Second, we present a taxonomy of PAD methods as a brief introduction to this very active research area. Finally, we discuss the integration of these methods into iris recognition systems according to the most important scenarios of practical application.

A. Morales (✉) · J. Fierrez (✉)
School of Engineering, Universidad Autonoma de Madrid, Madrid, Spain
e-mail: aythami.morales@uam.es

J. Fierrez
e-mail: julian.fierrez@uam.es

J. Galbally (✉)
eu-LISA / European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, Tallinn, Estonia
e-mail: javier.galbally@eulisa.europa.eu

M. Gomez-Barrero (✉)
Hochschule Ansbach, Ansbach, Germany
e-mail: marta.gomez-barrero@hs-ansbach.de

S. Marcel et al. (eds.), *Handbook of Biometric Anti-Spoofing*, Advances in Computer Vision and Pattern Recognition, https://doi.org/10.1007/978-981-19-5288-3_5

5.1 Introduction

The iris is one of the most popular biometric characteristics within biometric recognition technologies. Since the earliest Daugman publications proposing the iris as a reliable method to identify individuals [1] to most recent approaches based on latest machine learning and computer vision techniques [2–4], iris recognition has evolved improving performance, ease of use, and security. Such advances have attracted the interest of researchers and companies boosting the number of products, publications, and applications. The first iris recognition capture devices were developed to work as stand-alone systems [5]. However, today iris recognition technology is included as an authentication service in some of the most important operating systems (e.g., Android and Microsoft Windows) and devices (e.g., laptop or desktop computers and smartphones). One-seventh of the world population (1.14 billion people) has been enrolled in the Aadhaar India national biometric ID program [6] and iris is one of the three biometric characteristics (in addition to fingerprint and face) employed for authentication in that program. The main advantages of iris as a means for personal authentication can be summarized as follows:

- The iris is generated during prenatal gestation and presents highly random patterns. Such patterns are composed of complex and interrelated shapes and colors. The highly discriminant characteristics of the iris make it possible that recognition algorithms reach performances comparable to the most accurate biometric characteristics [3].
- The genetic prevalence of iris is limited and therefore irises from people with shared genes are different. Both irises of a person are considered as different instances, which do not match each other.
- The iris is an internal organ of the eye that is externally visible. It can be acquired at a distance and the advances in capture devices allow to easily integrate iris recognition into portable devices [7, 8].

The fast deployment of iris recognition technologies in real applications has increased the concerns about its security. The applications of iris biometrics include a variety of different scenarios and security levels (e.g., banking, smartphone user authentication, and governmental ID programs). Among all threats associated to biometric systems, the resilience against presentation attacks (PAs) emerges as one of the most active research areas in the recent iris biometrics literature. The security of commercial iris systems has been questioned and put to test by users and researchers. For instance, in 2017, the Chaos Computer Club reported their successful attack to the Samsung Galaxy S8 iris scanner using a simple photograph and a contact lens [9]. In the context of biometric systems, PAs are defined as the presentation of human characteristics or artifacts directly to the capture device of a biometric system trying to interfere its normal operation [10, 11]. This definition includes spoofing attacks, evasion attacks, and the so-called zero-effort attacks. Most of the literature on iris PAD methods is focused on the detection of spoofing attacks. The term liveness detection is also employed in the literature to propose systems capable of classifying

between bona fide samples and presentation attack instruments (PAIs) or artifacts used to attack biometric systems. Depending on the motivations of the attacker, we can distinguish two types of attacks:

- Impostor: the attacker tries to impersonate the identity of other subjects by using his own iris (e.g., zero-effort attacks) or a PAI mimicking the iris of the spoofed identity (e.g., photo, video, or synthetic iris). This type of attack requires a certain level of knowledge about the iris of the impersonated subject and the characteristics of the iris sensor in order to increase the success of the attack (see Sect. 5.2).
- Identity concealer: the attacker tries to evade recognition. Examples, in this case, include the enrollment of subjects with fake irises (e.g., synthetically generated) or modified irises (e.g., textured contact lens). These examples represent a way to masquerade real identities.

The first PAD approaches proposed in the literature were just theoretical exercises based on potential vulnerabilities [12]. In recent years, the number of publications focused on this topic has increased exponentially. Some of the PAD methods discussed in the recent literature have been inspired by methods proposed for other biometric characteristics such as face [13–15]. However, the iris has various particularities which can be exploited for PAD, such as the dynamic, fast, and involuntary responses of the pupil and the heterogeneous characteristics of the eye's tissue. The eye reacts according to the amount and nature of the light received. Another large group of PAD methods exploits these dynamic responses and involuntary signals produced by the eye.

The performance of iris PAD approaches can be measured according to different metrics. During the last years, the metrics proposed by the ISO/IEC 30107-3:2017 [10] have been adopted by the most important competitions [16]:

- Attack Presentation Classification Error Rate (APCER): measured as the percentage of attacks (usually from the same PAI) incorrectly classified as bonafide samples.[1]
- Bona fide Presentation Classification Error Rate (BPCER): defined as the percentage of bona fide samples classified as attacks.

In case of multiple PAIs or generation methods, the ISO/IEC 30107-3:2017 recommends to add the maximum value of APCER during the evaluation of different PAD approaches.

This chapter starts by presenting a description of the most important types of attacks from zero-effort attacks to the most sophisticated synthetic eyes. We then introduce iris PAD methods and their main challenges. The PAD methods are organized according to the nature of the features employed dividing them into three main groups: hardware-based, software-based, and challenge–response approaches.

[1] A bona fide presentation is defined in ISO/IEC 30107-3:2017 [10] as the interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system.

The rest of the chapter is organized as follows: Sect. 5.2 presents the main vulnerabilities of iris recognition systems with special attention to different types of PAs. Section 5.3 summarizes the PADmethods, while Sect. 5.4 presents the integration of PAD approaches with Iris Recognition Systems (IRSs). Finally, conclusions are presented in Sect. 5.5.

5.2 Vulnerabilities in Iris Biometrics

As already mentioned in the introduction, like any other biometric recognition technology, iris recognition is vulnerable to attacks. Figure 5.1 includes a typical block diagram of an IRS and its vulnerable points. The vulnerabilities depend on the characteristics of each module and cover communication protocols, data storage, or resilience against artifact presentations, among others. Several subsystems and not just one will define the security of an IRS:

- Sensor (V1): CCD/CMOS are the most popular sensors including visible and near-infrared images. The iris pattern is usually captured in the form of an image or video. The most important vulnerability is related to the presentation of PAIs (e.g., photos, videos, and synthetic eyes) that mimic the characteristics of real irises.
- Feature Extraction and Comparison modules (V2–V3): these software modules comprise the algorithms in charge of pre-processing, segmentation, generation of templates, and comparison. Attacks to these modules include the alteration of algorithms to carry out illegitimate operations (e.g., modified templates and altered comparison scores).
- Database (V5): the database is composed of structured data associated to the subject information, devices, and iris templates. Any alteration of this information can

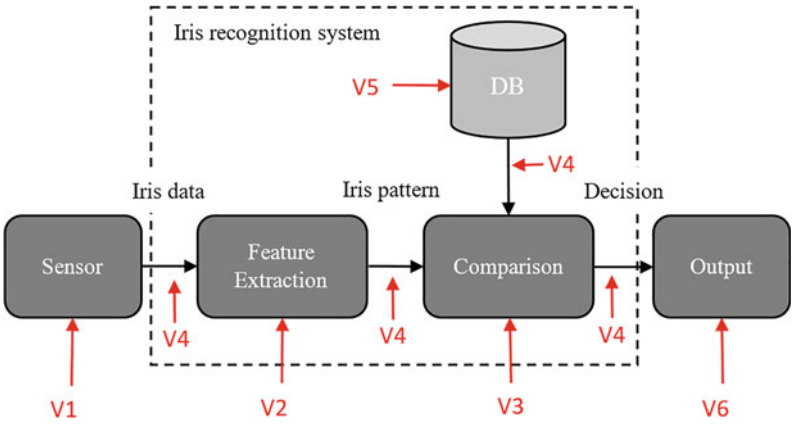

Fig. 5.1 Block diagram of a typical Iris Recognition System (IRS) and main vulnerabilities [17]

affect the final response of the system. The security level of the database storage differs depending on the applications. The use of encrypted templates is crucial to ensure the unlinkability between systems and attacks based on weak links.
- Communication channel and actuators (V4 and V6): include internal (e.g., communication between software modules) and external communications (e.g., communication with mechanical actuators or cloud services). The most important vulnerabilities rely on alterations of the information sent and received by the different modules of the IRS.

In this work, we will focus on PAs to the sensor (V1 vulnerabilities). Key properties of these attacks are their high attack success ratio (if the system is not properly protected) and the low amount of information about the system needed to perform the attack. Other vulnerabilities not covered by this work include attacks to the database (V5), to the software modules (V2–V3), the communication channels (V4), or actuators at the output (V6). This second group of vulnerabilities requires access to the system and countermeasures to these attacks are more related to general system security protocols. These attacks are beyond the scope of this chapter but should not be underestimated.

Regarding the nature of the PAI employed to spoof the system, the most popular PAs can be divided into the following categories:

- Zero-effort attacks: the attack is performed using the iris of the attacker that tries to take advantage of the False Match Rate (FMR) of the system.
- Photo and video attacks: the attack is performed displaying a printed photo, digital image, or video from the bona fide iris directly to the sensor of the IRS.
- Contact lens attacks: the attack is performed using iris patterns printed on contact lenses.
- Prosthetic eye attacks: the attack is performed using synthetic eyes generated to mimic the characteristics of real ones.
- Cadaver eye attacks: the attack is performed using eyes from postmortem subjects.

In the next subsections, each of these categories of attacks is discussed in more detail, paying special attention to three important features that define the risk posed by each of the threats: (1) information needed to perform the attack, (2) difficulty to generate the Presentation Attack Instrument (PAI), and (3) expected impact of the attack.

5.2.1 Zero-effort Attacks

In this attack, the impostor does not use any artifact or information about the identity under attack. The iris pattern from the impostor does not match the legitimate pattern and the success of the attack is exclusively related to the False Match Rate (FMR) of the system [18, 19]. Systems with high FMR will be more vulnerable to this type of attack. Note that the FMR is inversely related to the False Non-Match Rate (FNMR)

and both are defined by the operational point of the system. An operation point setup to obtain a low FMR can produce an increment of the FNMR and therefore a higher number of false negatives (legitimate subjects are rejected).

- Information needed to perform the attack: no information needed.
- Generation of the PAIs: no need to generate a fake iris. The system is attacked using the real iris of the attacker.
- Expected impact of the attack: Most iris recognition systems present very low False Match Rates. The success rate of these attacks can be considered low.

5.2.2 Photo and Video Attacks

Photo attacks are probably the PAs against IRS most studied in the literature [14, 20–24]. They simply consist of presenting to the sensor an image of the attacked iris, either printed on a sheet of paper or displayed on a digital screen. These attacks are among the most popular ones due to three main factors.

First, with the advent of digital photography and social image sharing (e.g., Flickr, Facebook, Picasaweb, and others), headshots of attacked clients from which the iris can be extracted are becoming increasingly easy to obtain. Even though the face or the voice are characteristics more exposed to this new threat, iris patterns can also be obtained from high-resolution face images (e.g., 200 dpi resolution).

Second, it is relatively easy to print high-quality iris photographs using commercial cameras (up to 12 Megapixel sensors in most of the nowadays smartphones) and ink printers (1200 dpi in most of the commercial ink printers). Alternatively, most mobile devices (smartphones and tablets) are equipped with high-resolution screens capable of reproducing very natural images and videos in the visible spectrum (see Fig. 5.2).

Third, the latest advances in machine learning methods to generate synthetic images open new ways to attack IRS. Recent works demonstrated that it is possible to mimic the pattern of real images using Generative Adversarial Networks [25, 26]. The synthetic iris can be used to conduct PAs or to train PAD methods.

As a more sophisticated version of photo attacks, the literature has also largely analyzed the so-called "video attacks", that consist of replaying on a digital screen a video of the attacked iris [27–30]. These attacks are able to mimic not only the static patterns of the iris but also the dynamic information of the eye that could potentially be exploited to detect static photo attacks (e.g., blinking, dilation/contraction of the pupil). As a limitation compared to the simpler photo attacks, it is more difficult to obtain a video than an image of a given iris.

- Information needed to perform the attack: Image or video of the iris of the subject to be impersonated.
- Generation of the PAIs: It is relatively easy to obtain high-resolution face photographs from social media and internet profiles. Other options include capturing

Fig. 5.2 Examples of Presentation Attack Instruments (PAIs): printed photo (top-left), screen photo (top-right) and prosthetic eye (bottom) adapted from Soper Brothers and Associates [http://www.soperbrothers.com]

it using a concealed camera. Once a photo is obtained, if it is of sufficient quality, the iris region can be printed and then presented to the iris acquisition sensor. A screen could also be used for presenting the photograph to the sensor. Another way to obtain the iris would be to steal the raw iris image acquired by an existing iris recognition system in which the subject being spoofed was already enrolled. In the case of video attacks, the availability of high-resolution videos of the iris is rather low in comparison with photographs. Nonetheless, it is relatively easy to capture a video in public spaces and the usage of long-range sensors open allows video capturing at a distance with high-resolution qualities.

- Expected impact of the attack: The literature offers a large number of approaches with good detection rates of printed photo attacks [14, 20–23, 31]. However, most of these methods exploit the lack of realism/quality of printed images in comparison with bona fide samples. The superior quality of new screens capable of reproducing digital images and video attacks with high definition represents a difficult challenge for PAD approaches based on visible spectrum imaging. To overcome this potential threat, new commercial scanners based on near-infrared cameras or even on 3D sensors have recently been proposed.

5.2.3 Contact Lens Attacks

This type of attack uses contact lenses created to mimic the pattern of a different individual (impostor attack) or contact lenses created to masquerade the identity (identity concealer attack). The case of a potential identity concealer attack is particularly worrying because nowadays more and more people wear contact lenses (approximately 125 million people worldwide wear contact lenses). We can differentiate between transparent contact lenses (used in general to correct some sight handicaps like myopia) and textured contact lenses (also known as printed). Textured contact lenses change the original iris information by the superposition of synthetic patterns. Although these contact lenses are mostly related to cosmetic applications, the same technology can be potentially used to print iris patterns from real subjects in order to carry out impostor attacks. If an individual is enrolled in the IRS without taking off the textured contact lenses, the IRS can be compromised at a later stage. Note that asking to remove transparent/corrective contact lenses before enrolment or recognition is a non-desirable solution as it clearly decreases the user comfort and usability.

- Information needed to perform the attack: Image of the iris of the client to be attacked for impostor attacks. No information is needed for identity concealer attacks.
- Generation of the PAIs: In comparison with photo or video attacks, the generation of textured contact lenses requires a more sophisticated method based on optometrist devices and protocols.The characteristics of the devices employed to manufacture the contact lenses are critical to define the performance of PAD methods. For example, the results reported in [16] suggested that the proposed methods presented a lower performance against unknown contact lens brands.
- Expected impact of the attack: These types of attacks represent a great challenge for either automatic PAD systems or visual inspection by humans. It has been reported by several researchers that it is actually possible to spoof iris recognition systems with well-made contact lenses [27, 30, 32–35].

5.2.4 Synthetic Eye Attacks

This type of attack is the most sophisticated. Prosthetic eyes have been used since the beginning of twentieth century to reduce the esthetic impact related to the absence of eyes (e.g., blindness, amputations, etc.). Current technologies for prosthetic manufacturing allow mimicking the most important attributes of the eye with very realistic results. The similarity goes beyond the visual appearance including manufacturing materials with similar physical properties (e.g., elasticity and density). The number of studies including attacks to iris biometric systems using synthetic eyes is still low [36].

- Information needed to perform the attack: Image of the eye of the client to be attacked.
- Generation of the PAIs: this is probably the most sophisticated attack method as it involves the generation of both 2D images and 3D structures. Manually made in the past, 3D printers and their application to the prosthetic field have revolutionized the generation of synthetic body parts.
- Expected impact of the attack: Although the number of studies is low, the detection of prosthetic eyes represents a big challenge. The detection of these attacks by techniques based on image features is difficult. On the other hand, PAD methods based on dynamic features can be useful to detect the unnatural dynamics of synthetic eyes.

5.2.5 Cadaver Eye Attacks

Postmortem biometric analysis is very common in forensic sciences. However, during the last years, this field of study attracted the interest of other research communities. As a result of this increasing interest, researchers have evaluated the potential of attacks based on eyes from postmortem subjects [37, 38]. This type of attack has been included in recent iris PAD competitions demonstrating its challenge [16].

- Information needed to perform the attack: no information needed.
- Generation of the PAIs: this type of attack is particularly difficult to perform as the attacker needs to have access to the cadaver of the person to be impersonated.
- Expected impact of the attack: Although the number of studies is low, the detection accuracy of this attack increases with respect to the time gap to the postmortem time horizon. As a living tissue, the pattern on the iris degrades over time once the subject is dead.

Table 5.1 summarizes the literature on iris PAs including the most popular public databases available for research purposes.

5.3 Presentation Attack Detection Approaches

These methods are also known in the literature as liveness detection, anti-spoofing, or artifact detection among others. The term PAD was adopted in the ISO/IEC 30107-1:2016 [10] and it is now largely accepted by the research community.

The different PAD methods can be categorized according to several characteristics. Some authors propose a taxonomy of PAD methods based on the nature of both methods and attacks: passive or active methods employed to detect static or dynamic attacks [40]. Passive methods include those capable of extracting features from samples obtained by traditional iris recognition systems (e.g., image from the iris sensor).

Table 5.1 Literature on presentation attack detection methods. Summary of the literature concerning iris Presentation Attack Detection (PAD) methods depending on the Presentation Attack Instrument (PAI)

Ref.	PAI	PAD	Database
[13]	Photo	Quality measures	Public
[39]	Photo	Wavelet measures	Proprietary
[14]	Photo	Deep features	Public
[40]	Video	Pupil dynamics	Proprietary
[41]	Video	Oculomotor Plant Char.	Proprietary
[42]	Video	Pupillary reflex	Proprietary
[43]	Contact Lens	Photometric features	Public
[44]	Contact Lens	2D & 3D features	Public
[35]	Contact lens	LBP features	Proprietary
[45]	Various	Hyperspectral features	Proprietary
[46]	Various	Pupillary reflex	Proprietary
[47]	Various	Various	Public
[48]	Various	Deep features	Public
[49]	Various	Deep features	Public
[26]	Various	Deep features	Public
[50]	Various	Deep features	Public

Active methods modify the recognition system in order to obtain features for the PAD method (e.g., dynamic illumination and challenge–response). Static attacks refer to those based on individual samples (e.g., image), while dynamic attacks include PAIs capable of changing with time (e.g., video or lens attacks).

In this chapter, we introduce the most popular PAD methods according to the nature of the features used to detect the forged iris: hardware-based, software-based, and challenge–response. The challenge–response and most of the hardware methods can be considered active approaches, as they need additional sensors or collaboration from the subject. On the other hand, most of the software methods employ passive approaches in which PAD features are directly obtained from the biometric sample acquired by the iris sensor. Fig. 5.3 presents a taxonomy of the iris PAD methods introduced in this chapter.

5.3.1 Hardware-Based Approaches

Also known as sensor-based approaches in the literature. These methods employ specific sensors (in addition to the standard iris sensor) to measure the biological and physical characteristics of the eye. These characteristics include physical properties

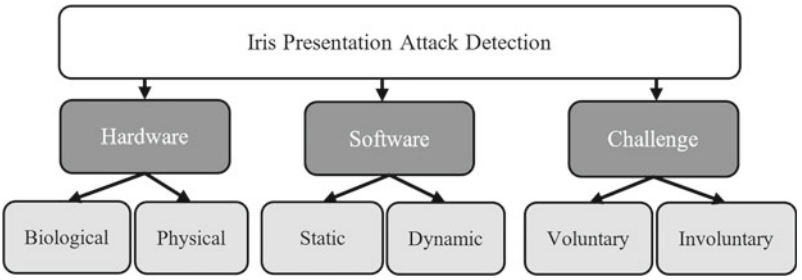

Fig. 5.3 Taxonomy of iris Presentation Attack Detection methods

of the eye (e.g., light absorption of the different eye layers or electrical conductivity), and biological properties (e.g., density of the eye tissues, melanin, or blood vessel structures in the eye). The most popular hardware-based PAD approaches that can be found in the literature belong to one of three groups:

- Multispectral imaging [51–54]: The eye includes complex anatomical structures enclosed in three layers. These layers are made of organic tissue with different spectrographic properties. The idea underlying these methods is to use the spectroscopic print of the eye tissues for PAD. Non-living tissue (e.g., paper, crystal from the screens, or synthetic materials including contact lenses) will present reflectance characteristics different from those obtained from a real eye. These approaches exploit the use of illumination with different wavelengths that vary according to the method proposed and the physical or biological characteristic being measured (e.g., hemoglobin presents an absorption peak in near-infrared bands).
- 3D imaging [22, 55]: The curvature and 3D nature of the eye has been exploited by researchers to develop PAD methods. The 3D profile of the iris is captured in [55] by using two near-infrared light sources and a simple 2D sensor. The idea underlying the method is to detect the shadows on real irises produced by non-uniform illumination provided from two different directions. Light-Field Cameras (LFCs) are used in [22] to acquire multiple depth images and detect the lack of volumetric profiles of photo attacks.
- Electrooculography [56]: The electric standing potential between the cornea and retina can be measured and the resulting signal is known as electrooculogram. This potential can be used as a liveness indicator but the acquisition of these signals is invasive and includes the placement of at least two electrodes in the eye region. Advances in non-intrusive new methods to acquire the electrooculogram can boost the interest in these approaches.

5.3.2 Software-Based Approaches

Software-based PAD methods use features directly extracted from the samples obtained by the standard iris sensor. These methods exploit pattern recognition techniques in order to detect fake samples. Techniques can be divided into static or dynamic depending on the nature of the information used. While static approaches search for patterns obtained from a single sample, dynamic approaches exploit time sequences or multiple samples (typically a video sequence).

Some authors propose methods to detect the clues or imperfections introduced by printing devices used during the manufacturing of PAIs (e.g., printing process for photo attacks). These imperfections can be detected by Fourier image decomposition [20, 21, 39], Wavelet analysis [27], or Laplacian transform [28]. All these methods employ features obtained from the frequency domain in order to detect artificial patterns in fake PAIs. Other authors have explored iris quality measures for PAD. The quality of biometric samples has a direct impact on the performance of biometric systems. The literature includes several approaches to measure the quality of image-based biometric samples. The application of quality measures as PAD features for iris biometrics has been studied in [13, 57]. These techniques exploit iris and image quality in order to detect photo attacks from real irises.

Advances in image processing techniques have also allowed to develop new PAD methods based on the analysis of features obtained at pixel level. These approaches include features obtained from gray level values [58], edges [34], or color [59]. The idea underlying these methods is that the texture of manufacturing materials shows different patterns due to the non-living properties of materials (e.g., density and viscosity). In this line, the method proposed in [59] analyzes image features obtained from near-infrared and visible spectrums. Local descriptors have been also used for iris PAD: Local Binary Patterns—LBP [35, 60–62], Binary Statistical Image Features—BSIF [15, 60], Scale-Invariant Feature Transform—SIFT [30, 60, 63], fusion of 2D and 3D features [44], and Local Phase Quantization—LPQ [60].

Finally, in [14], researchers evaluated for the first time the performance of deep learning techniques for iris photo attack detection with encouraging results. Then the same group of researchers studied how to use those networks to detect more challenging attacks in [64]. Since those initial works were based on deep learning, over the past few years, many works have continued to work in that direction, proposing novel PAD methods based on deep architectures including attention learning [48, 65], adversarial learning [26, 49], and several approaches based on popular convolutional features [66].

5.3.3 Challenge–Response Approaches

These methods analyze voluntary and involuntary responses of the human eye. The involuntary responses are part of the processes associated to the neuromotor activities

of the eye, while the voluntary behavior are responses to specific challenges. Both voluntary and involuntary responses can be driven by external stimuli produced by the PAD system (e.g., changes in the intensity of the light, blink instructions, gaze tracking during dedicated challenges, etc.). The eye reacts to such external stimuli and these reactions can be used as a proof of life to detect attacks based on photos or videos. In addition, there are eye reactions inherent to a living body that can be measured in terms of signals (e.g., permanent oscillation of the eye pupil called hippus, involuntary eye movements called microsaccades, etc.). These reactions can be considered as involuntary responses non-controlled by the subject. The occurrence of these signals is used as a proof of life.

The pupil reactions in the presence of uniform light or lighting events were early proposed in [32] for PAD applications and more deeply studied in [40]. As mentioned above, the hippus are permanent oscillations of the pupil that are visible even with uniform illumination. These oscillations range from 0.3 to 0.7Hz and decline with age. The PAD methods based on hippus have been explored to detect photo attacks and prosthetic eye attacks [21, 67]. However, the difficulties to perform a reliable detection reduce the performance of these methods. Based on similar principles related to eye dynamics, the use of oculomotor plant models to serve as PAD methods was evaluated in [41].

The reflection of the light in the lens and cornea produces a well-known involuntary effect named Purkinje reflections. This effect is a reflection of the eye to external illumination. At least four Purkinje reflections are usually visible. The reflections change depending on the light source and these changes can be used for liveness detection [46, 52]. Simple photo and video attacks can be detected by these PAD methods by simply varying the illumination conditions. However, their performance against contact lens or synthetic eye attacks is not clear due to the natural reflections on real pupils (contact lens or photo attacks with pupil holes) or sophisticated fabrication methods (synthetic eyes).

5.4 Integration with Iris Recognition Systems

PAD approaches should be integrated into the iris recognition systems granting a correct and normal workflow. There are two basic integration schemes [68]:

- Parallel integration: the outputs of the IRS and PAD systems are combined before the decision module. The combination method depends on the nature of the output to be combined (e.g., score-level or decision-level fusion) [69].
- Serial integration: the sample is first analyzed by the PAD system. In case of a legitimate subject, the IRS processes the sample. Otherwise, the detection of an attack will avoid unnecessary recognition and the sample will be directly discarded.

The software-based PAD methods are usually included as modules (serial or parallel) in the feature extraction algorithms. A potential problem associated to the

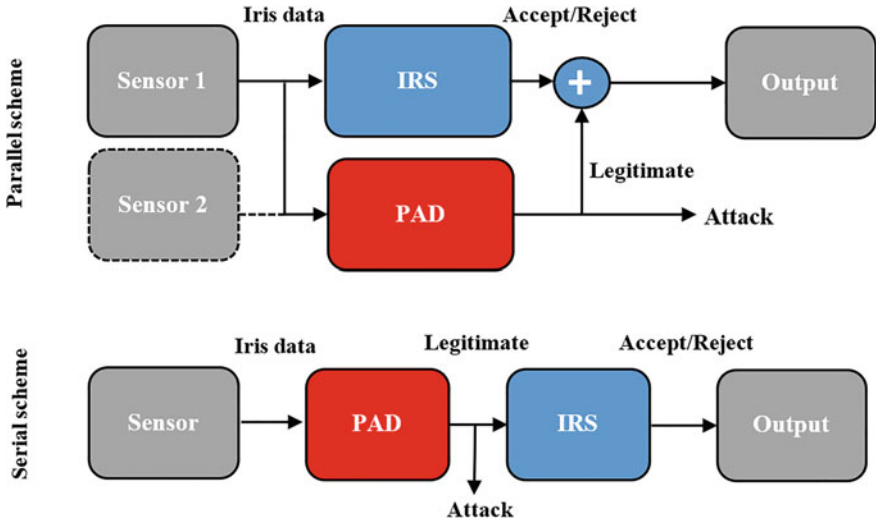

Fig. 5.4 Integration of Presentation Attack Detection (PAD) with Iris Recognition Systems (IRS) in parallel (top) and serial (bottom) schemes

inclusion of PAD software is a delay in the recognition time. However, most PAD approaches based on software methods report a low computational complexity that mitigates this concern. The automatic detection of contact lenses plays an important role in software-based approaches. The effects of wearing contact lenses can be critical in case of textured lenses. In [70], the authors reported that textured lenses can cause the FNMR to exceed 90%. The detection of contact lenses represents the first step in IRS and specific algorithms have been developed and integrated as a preprocessing module [14, 70, 71]. The final goal of these algorithms is to detect and filter the images to remove the synthetic pattern.

Hardware-based PAD approaches are usually integrated before the iris sensor (serial) or as an independent parallel module (see Fig. 5.4). In addition to the execution time concerns, hardware-based approaches increase the complexity of the system and the authentication process. Therefore, the main aspects to be analyzed during the integration of those approaches come from the necessity of dedicated sensors and its specific restrictions related to size, time, and cost. These are barriers that difficult the integration of hardware-based approaches into mobile devices (e.g., smartphones).

The main drawback of challenge-response approaches is the increased level of collaboration needed from the subject (either for serial or parallel schemes). This collaboration usually introduces delays in the recognition process and some subjects can perceive it as an unfriendly process.

5.5 Conclusions

Iris recognition systems have been improved over the last decade achieving better performance [16], more convenient acquisition at a distance [8], and full integration with mobile devices [7]. However, the robustness against attacks is still a challenge for the research community and industrial applications [18]. Researchers have shown the vulnerability of iris recognition systems and there is a consensus about the necessity of finding new methods to improve the security of iris biometrics. Among the different types of attacks, presentation attacks represent a key concern because of their simplicity and high attack success rates. The acquisition at a distance achieved by recent advances on new sensors and the public exposure of face, and therefore iris, make it relatively easy to obtain iris patterns and use them for malicious purposes. The literature on PAD methods is large including a broad variety of methods, databases, and protocols. Over the next years, it will be desirable to unify the research community into common benchmarks and protocols. Even if the current technology shows high detection rates for the simplest attacks (e.g., zero-effort and photo attacks), there are still challenges associated to the most sophisticated attacks such as those using textured contact lenses and synthetic eyes.

Future work in this area of iris PAD may exploit: (1) related research being conducted to recognize the periocular region [72], (2) other information from the face when the iris image or the biometric system as a whole includes a partial or a full face [73], and (3) related research in characterizing natural vs artificially generated faces (DeepFakes) using recent deep learning methods [74]. All these complementary fields of research can provide valuable information for improved PAD when the iris images or videos are accompanied by additional information from the face surrounding the iris.

Acknowledgements This work was mostly done (2nd Edition of the book) in the context of the TABULA RASA and BEAT projects funded under the 7th Framework Programme of EU. The 3rd Edition update has been made in the context of EU H2020 projects PRIMA and TRESPASS-ETN. This work was also partially supported by the Spanish project BIBECA (RTI2018-101248-B-I00 MINECO/FEDER) and by the DFG-ANR RESPECT Project (406880674).

References

1. Daugman J (1993) High confidence visual recognition of persons by a test of statistical independence. IEEE Trans Pattern Anal Mach Intell 15:1148–1161
2. Alonso-Fernandez F, Farrugia RA, Bigun J, Fierrez J, Gonzalez-Sosa E (2019) A survey of super-resolution in iris biometrics with evaluation of dictionary-learning. IEEE Access 7(1):6519–6544. https://doi.org/10.1109/ACCESS.2018.2889395
3. Burge MJ, Bowyer KW (eds) (2013) Handbook of iris recognition. Springer
4. Galbally J, Gomez-Barrero M (2017) Iris and periocular biometric recognition. In: Rathgeb C, Busch C (eds) Presentation attack detection in iris recognition. IET Digital Library, pp 235–263

5. Flom L, Safir A (1987) Iris recognition system. US Patent US4641349 A
6. Abraham R, Bennett ES, Sen N, Shah NB (2017) State of AADHAAR report 2016–17. Technical report, IDinsight
7. Alonso-Fernandez F, Farrugia RA, Fierrez J, Bigun J (2019) Super-resolution for selfie biometrics: introduction and application to face and iris. Springer, pp 105–128. https://doi.org/10.1007/978-3-030-26972-2_5
8. Nguyen K, Fookes C, Jillela R, Sridharan S, Ross A (2017) Long range iris recognition: a survey. Pattern Recognit 72:123–143
9. Chaos Computer Club Berlin (2017) Chaos computer clubs breaks iris recognition system of the Samsung Galaxy S8. https://www.ccc.de/en/updates/2017/iriden
10. ISO/IEC CD 30107-1 (2016) information technology - biometrics - presentation attack detection - part 1: framework
11. Galbally J, Fierrez J, Ortega-Garcia J (2007) Vulnerabilities in biometric systems: attacks and recent advances in liveness detection. In: Proceedings of Spanish workshop on biometrics, (SWB)
12. Daugman J (1999) Biometrics. Personal identification in a networked society, Recognizing persons by their iris patterns. Kluwer Academic Publishers, pp 103–121
13. Galbally J, Marcel S, Fierrez J (2014) Image quality assessment for fake biometric detection: application to iris, fingerprint and face recognition. IEEE Trans Image Process 23:710–724
14. Menotti D, Chiachia G, Pinto A, Schwartz WR, Pedrini H, Falcao AX, Rocha A (2015) Deep representations for iris, face, and fingerprint spoofing detection. IEEE Trans Inf Forensics Secur 10:864–878
15. Raghavendra R, Busch C (2014) Presentation attack detection algorithm for face and iris biometrics. In: Proceedings of IEEE European signal processing conference (EUSIPCO), pp 1387–1391
16. Das P, Mcfiratht J, Fang Z, Boyd A, Jang G, Mohammadi A, Purnapatra S, Yambay D, Marcel S, Trokielewicz M, et al (2020) Iris liveness detection competition (LivDet-Iris)-the 2020 edition. In: 2020 IEEE international joint conference on biometrics (IJCB), pp 1–9
17. Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634
18. Hadid A, Evans N, Marcel S, Fierrez J (2015) Biometrics systems under spoofing attack. IEEE Signal Process Mag 32:20–30
19. Johnson P, Lazarick R, Marasco E, Newton E, Ross A, Schuckers S (2012) Biometric liveness detection: framework and metrics. In: Proceedings of NIST international biometric performance conference (IBPC)
20. Czajka A (2013) Database of iris printouts and its application: development of liveness detection method for iris recognition. In: Proceedings of international conference on methods and models in automation and robotics (MMAR), pp 28–33
21. Pacut A, Czajka A (2006) Aliveness detection for iris biometrics. In: Proceedings of IEEE international carnahan conference on security technology (ICCST), pp 122–129
22. Raghavendra R, Busch C (2014) Presentation attack detection on visible spectrum iris recognition by exploring inherent characteristics of light field camera. In: Proceedings of IEEE international joint conference on biometrics (IJCB)
23. Ruiz-Albacete V, Tome-Gonzalez P, Alonso-Fernandez F, Galbally J, Fierrez J, Ortega-Garcia J (2008) Direct attacks using fake images in iris verification. In: Proceedings of COST 2101 workshop on biometrics and identity management (BioID), LNCS-5372. Springer, pp 181–190
24. Thalheim L, Krissler J (2002) Body check: biometric access protection devices and their programs put to the test. ct magazine pp 114–121
25. Galbally J, Ross A, Gomez-Barrero M, Fierrez J, Ortega-Garcia J (2013) Iris image reconstruction from binary templates: an efficient probabilistic approach based on genetic algorithms. Comput Vis Image Underst 117(10):1512–1525. https://doi.org/10.1016/j.cviu.2013.06.003
26. Yadav S, Chen C, Ross A (2019) Synthesizing iris images using RaSGAN with application in presentation attack detection. In: Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops

27. He X, Lu Y, Shi P (2009) A new fake iris detection method. In: Proceedings of IAPR/IEEE international conference on biometrics (ICB), LNCS-5558. Springer, pp 1132–1139
28. Raja KB, Raghavendra R, Busch C (2015) Presentation attack detection using laplacian decomposed frequency response for visible spectrum and near-infra-red iris systems. In: Proceedings of IEEE international conference on biometrics: theory and applications (BTAS)
29. Raja KB, Raghavendra R, Busch C (2015) Video presentation attack detection in visible spectrum iris recognition using magnified phase information. IEEE Trans Inf Forensics Secur 10:2048–2056
30. Zhang H, Sun Z, Tan T, Wang J (2011) Learning hierarchical visual codebook for iris liveness detection. In: Proceedings of IEEE international joint conference on biometrics (IJCB)
31. Yambay D, Doyle JS, Boyer KW, Czajka A, Schuckers S (2014) Livdet-iris 2013 - iris liveness detection competition 2013. In: Proceedings of IEEE international joint conference on biometrics (IJCB)
32. Daugman J (2004) Iris recognition and anti-spoofing countermeasures. In: Proceedings of international biometrics conference (IBC)
33. von Seelen UC (2005) Countermeasures against iris spoofing with contact lenses. In: Proceedings biometrics consortium conference (BCC)
34. Wei Z, Qiu X, Sun Z, Tan T (2008) Counterfeit iris detection based on texture analysis. In: Proceedings of IAPR international conference on pattern recognition (ICPR)
35. Zhang H, Sun Z, Tan T (2010) Contact lense detection based on weighted LBP. In: Proceedings of IEEE international conference on pattern recognition (ICPR), pp 4279–4282
36. Lefohn A, Budge B, Shirley P, Caruso R, Reinhard E (2003) An ocularist's approach to human iris synthesis. IEEE Trans Comput Graph Appl 23:70–75
37. Trokielewicz M, Czajka A, Maciejewicz P (2018) Presentation attack detection for cadaver iris. In: 2018 IEEE 9th international conference on biometrics theory, applications and systems (BTAS), pp 1–10
38. Trokielewicz M, Czajka A, Maciejewicz P (2020) Post-mortem iris recognition with deep-learning-based image segmentation. Image Vis Comput 94:103,866
39. He X, Lu Y, Shi P (2008) A fake iris detection method based on FFT and quality assessment. In: Proceedings of IEEE Chinese conference on pattern recognition (CCPR)
40. Czajka A (2015) Pupil dynamics for iris liveness detection. IEEE Trans Inf Forensics Secur 10:726–735
41. Komogortsev O, Karpov A (2013) Liveness detection via oculomotor plant characteristics: attack of mechanical replicas. In: Proceedings of international conference of biometrics (ICB)
42. Kanematsu M, Takano H, Nakamura K (2007) Highly reliable liveness detection method for iris recognition. In: Proceedings of SICE annual conference, international conference on instrumentation, control and information technology (ICICIT), pp 361–364
43. Czajka A, Fang Z, Bowyer K (2019) Iris presentation attack detection based on photometric stereo features. In: 2019 IEEE winter conference on applications of computer vision (WACV), pp 877–885
44. Fang Z, Czajka A, Bowyer KW (2020) Robust iris presentation attack detection fusing 2d and 3d information. IEEE Trans Inf Forensics Secur 16:510–520
45. Chen R, Lin X, Ding T (2012) Liveness detection for iris recognition using multispectral images. Pattern Recogn Lett 33:1513–1519
46. Lee EC, Yo YJ, Park KR (2008) Fake iris detection method using Purkinje images based on gaze position. Opt Eng 47:067,204
47. Yambay D, Becker B, Kohli N, Yadav D, Czajka A, Bowyer KW, Schuckers S, Singh R, Vatsa M, Noore A, Gragnaniello D, Sansone C, Verdoliva L, He L, Ru Y, Li H, Liu N, Sun Z, Tan T (2017) Livdet iris 2017 – iris liveness detection competition 2017. In: Proceedings of IEEE international joint conference on biometrics (IJCB), pp 1–6
48. Fang M, Damer N, Boutros F, Kirchbuchner F, Kuijper A (2021) Iris presentation attack detection by attention-based and deep pixel-wise binary supervision network. In: 2021 IEEE international joint conference on biometrics (IJCB), pp 1–8

49. Yadav S, Ross A (2021) Cit-gan: cyclic image translation generative adversarial network with application in iris presentation attack detection. In: Proceedings of the IEEE/CVF winter conference on applications of computer vision, pp 2412–2421
50. Sharma R, Ross A (2020) D-netpad: An explainable and interpretable iris presentation attack detector. In: 2020 IEEE international joint conference on biometrics (IJCB), pp 1–10
51. He Y, Hou Y, Li Y, Wang Y (2010) Liveness iris detection method based on the eye's optical features. In: Proceedings of SPIE optics and photonics for counterterrorism and crime fighting VI, p 78380R
52. Lee EC, Park KR, Kim J (2006) Fake iris detection by using Purkinje image. In: Proceedings of IAPR international conference on biometrics (ICB), pp 397–403
53. Lee SJ, Park KR, Lee YJ, Bae K, Kim J (2007) Multifeature-based fake iris detection method. Opt Eng 46:127,204
54. Park JH, Kang MG (2005) Iris recognition against counterfeit attack using gradient based fusion of multi-spectral images. In: Proceedings of international workshop on biometric recognition systems (IWBRS), LNCS-3781. Springer, pp 150–156
55. Lee EC, Park KR (2010) Fake iris detection based on 3D structure of the iris pattern. Int J Imaging Syst Technol 20:162–166
56. Krupiński R, Mazurek P (2012) Estimation of electrooculography and blinking signals based on filter banks. In: Proceedings of the 2012 international conference on computer vision and graphics, pp 156–163
57. Galbally J, Ortiz-Lopez J, Fierrez J, Ortega-Garcia J (2012) Iris liveness detection based on quality related features. In: Proceedings of IAPR international conference on biometrics (ICB), pp 271–276
58. He X, An S, Shi P (2007) Statistical texture analysis-based approach for fake iris detection using support vector machines. In: Proceedings of IAPR international conference on biometrics (ICB), LNCS-4642. Springer, pp 540–546
59. Alonso-Fernandez F, Bigun J (2014) Fake iris detection: a comparison between near-infrared and visible images. In: Proceedings IEEE International conference on signal-image technology and internet-based systems (SITIS), pp 546–553
60. Gragnaniello, D., Poggi, G., Sansone, C., Verdoliva, L.: An investigation of local descriptors for biometric spoofing detection. IEEE Trans. on Information Forensics and Security **10**, 849–863 (2015)
61. Gupta P, Behera S, Singh MVV (2014) On iris spoofing using print attack. In: IEEE international conference on pattern recognition (ICPR)
62. He Z, Sun Z, Tan T, Wei Z (2009) Efficient iris spoof detection via boosted local binary patterns. In: Proceedings IEEE international conference on biometrics (ICB)
63. Sun Z, Zhang H, Tan T, Wang J (2014) Iris image classification based on hierarchical visual codebook. IEEE Trans Pattern Anal Mach Intell 36:1120–1133
64. Silva P, Luz E, Baeta R, Pedrini H, Falcao AX, Menotti D (2015) An approach to iris contact lens detection based on deep image representations. In: Proceedings of conference on graphics, patterns and images (SIBGRAPI)
65. Chen C, Ross A (2021) An explainable attention-guided iris presentation attack detector. In: WACV (Workshops), pp 97–106
66. El-Din YS, Moustafa MN, Mahdi H (2020) Deep convolutional neural networks for face and iris presentation attack detection: survey and case study. IET Biometrics 9(5):179–193
67. Park KR (2006) Robust fake iris detection. In: Proceedings of articulated motion and deformable objects (AMDO), LNCS-4069. Springer, pp 10–18
68. Fierrez J, Morales A, Vera-Rodriguez R, Camacho D (2018) Multiple classifiers in biometrics. part 1: fundamentals and review. Inf Fusion 44:57–64
69. Biggio B, Fumera G, Marcialis G, Roli F (2017) Statistical meta-analysis of presentation attacks for secure multibiometric systems. IEEE Trans Pattern Anal Mach Intell 39(3):561–575
70. Bowyer KW, Doyle JS (2014) Cosmetic contact lenses and iris recognition spoofing. IEEE Comput 47:96–98

71. Yadav D, Kohli N, Doyle JS, Singh R, Vatsa M, Bowyer KW (2014) Unraveling the effect of textured contact lenses on iris recognition. IEEE Trans Inf Forensics Secur 9:851–862
72. Alonso-Fernandez F, Raja KB, Raghavendra R, Busch C, Bigun J, Vera-Rodriguez R, Fierrez J (2019) Cross-sensor periocular biometrics for partial face recognition in a global pandemic: comparative benchmark and novel multialgorithmic approach. arXiv:1902.08123
73. Gonzalez-Sosa E, Fierrez J, Vera-Rodriguez R, Alonso-Fernandez F (2018) Facial soft biometrics for recognition in the wild: recent works, annotation and COTS evaluation. IEEE Trans Inf Forensics Secur 13(8):2001–2014
74. Tolosana R, Vera-Rodriguez R, Fierrez J, Morales A, Ortega-Garcia J (2020) Deepfakes and beyond: a survey of face manipulation and fake detection. Inf Fusion 64:131–148. https://doi.org/10.1016/j.inffus.2020.06.014