Chapter 6
Introduction to Iris Presentation Attack Detection

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

Abstract Iris recognition technology has attracted an increasing interest since more than two decades in which we have witnessed a migration from laboratories to real-world applications. The deployment of this technology in real applications raises questions about the main vulnerabilities and security threats related to these systems. Presentation attacks can be defined as presentation of human characteristics or artifacts directly to the input of a biometric system trying to interfere with its normal operation. These attacks include the use of real irises as well as artifacts with different levels of sophistication. This chapter introduces iris presentation attack detection methods and its main challenges. First, we summarize the most popular types of attacks including the main challenges to address. Second, we present a taxonomy of presentation attack detection methods to serve as a brief introduction on 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 (✉)
School of Engineering, Universidad Autonoma de Madrid, Madrid, Spain
e-mail: aythami.morales@uam.es

J. Fierrez
Universidad Autonoma de Madrid, Madrid, Spain
e-mail: julian.fierrez@uam.es

J. Galbally
European Commission - DG Joint Research Centre, Ispra, Italy
e-mail: javier.galbally@ec.europa.eu

M. Gomez-Barrero
da/sec - Biometrics and Internet Security Research Group, Hochschule Darmstadt, Darmstadt, Germany
e-mail: marta.gomez-barrero@h-da.de

S. Marcel et al. (eds.), *Handbook of Biometric Anti-Spoofing*,
Advances in Computer Vision and Pattern Recognition,
https://doi.org/10.1007/978-3-319-92627-8_6

6.1 Introduction

The iris is one of the most popular biometric modes inside the biometric person recognition technologies. Since the earliest Daugman publications proposing the iris as a biometric characteristic [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 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, Microsoft Windows) and devices (e.g., laptop or desktop computers, 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 on three biometric modes (in addition to fingerprint and face) employed for authentication in this program. The main advantages of iris can be summarized as follows:

- The iris is generated during the 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 possible that recognition algorithms obtain performances comparable to the most accurate biometric modes [2].
- The genetic prevalence on 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. The iris can be acquired at a distance and the advances on acquisition sensors allow to easily integrate iris recognition into portable devices [7].

The fast deployment of iris recognition technology 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 attacks emerges as one of the most active research areas in the recent iris biometrics literature. The security of commercial iris systems is questioned by users. 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 [8]. In the context of biometric systems, presentation attacks are defined as presentation of human characteristics or artifacts directly to the input of a biometric system trying to interfere with its normal operation [9]. This definition includes spoofing attacks, evasion attacks, and the so-called zero-effort attacks. Most of the literature on iris Presentation Attack Detection (PAD) is focused on spoofing attacks detection. The term liveness detection is also employed in the literature to propose systems capable of classifying between bona fide samples and 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 an artifact mimicking the iris of the spoofed identity (e.g., photo, video or synthetic iris). This type of attack requires certain level of knowledge about the iris of the impersonated user and the characteristics of the iris sensor in order to increase the success of the attack (see Sect. 6.2).
- Identity concealer: The attacker tries to evade the iris recognition. Examples in this case include the enrollment of users with fake irises (e.g., synthetically generated) or modified irises (e.g., textured contact lens). These examples represent a way to masquerade the real identities.

The first PAD approaches proposed in the literature were just theoretical exercises based on potential vulnerabilities [10]. In recent years, the number of publications focused on this topic has increased significantly. Some of the PAD methods discussed in the recent literature have been inspired by methods proposed for other biometric modes such as face [11–13]. 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 eyes 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.

This chapter presents a description of the most important types of attacks from zero-effort attacks to the most sophisticated synthetic eyes. We introduce iris Presentation Attacks Detection methods and its main challenges. The PAD methods are organized according to the nature of features employed with a taxonomy divided into three main groups: hardware-based, software-based, and challenge–response approaches. Please note that the material presented in this chapter tries to be up to date, but keeping an introductory nature. A more comprehensive survey of iris PAD can be found in [4].

The rest of the chapter is organized as follows: Sect. 6.2 presents the main vulnerabilities of iris recognition systems with special attention to different types of presentation attacks. Section 6.3 summarizes the presentation attacks detection methods while Sect. 6.4 presents the integration with iris recognition systems. Finally, conclusions are presented in Sect. 6.5.

6.2 Vulnerabilities in Iris Biometrics

Traditional block diagrams of Iris Recognition Systems (IRS) are similar to block diagrams of other biometric modes. As any other biometric recognition technology, iris recognition is vulnerable to attacks. Figure 6.1 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 to artifact presentations, among others. Several subsystems and not just one will define the security of an IRS [14]:

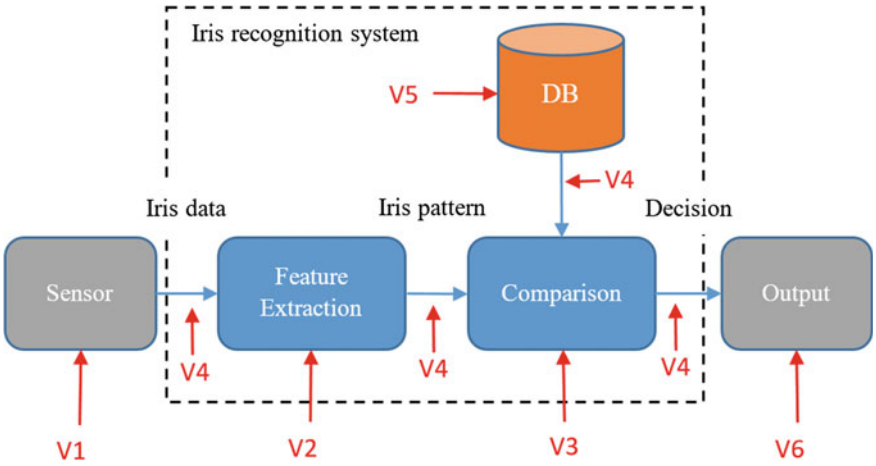

Fig. 6.1 Block diagram of traditional iris recognition systems and main vulnerabilities [14]

- Sensor (V1): CCD/CMOS are the most popular sensors including visible and near-infrared imaging. The iris pattern is usually captured in form of image or video. The most important vulnerability is related to the presentation of artifacts (e.g., photos, videos, synthetic eyes) that mimic the characteristics of real irises.
- Feature extraction and matcher modules (V2-V3): These software modules are composed of the algorithms in charge of preprocessing, segmentation, generation of templates, and comparison. Attacks to these modules include the alteration of algorithms to carry out not legitimate operations (e.g., modified templates, altered comparison).
- Database (V5): The database is composed of structured data associated to the subject information, devices, and iris templates. Any alteration on this information can 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 [15].
- Communication channel and actuators (V4 and V6): Including 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 presentation attacks on the sensor (V1 vulnerabilities). Key properties of these attacks are the high attack success ratio of spoofed irises (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 Presentation Attack Instrument (PAI) employed to spoof the system, the most popular presentation attacks can be divided into the following categories:

- Zero-effort attacks,
- photo and video attacks,
- contact lens attacks, and
- synthetic eye attacks.

6.2.1 Zero-Effort Attacks

The attack is performed using the iris from the attacker. 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 [16, 17]. Systems with high FMR will be more vulnerable to this type of attack. Note that the FMR is related to the False Non-Match Rate (FNMR) and both are related to the operational point of the system. An operational setup to obtain a low FMR can produce an increment of the FNMR and therefore a higher number of false negatives (legitime users are rejected).

- Information needed to perform the attack: No information needed.
- Generation and acquisition of the PAIs: No need to generate a fake iris. The system is attacked using real irises of the attacker.
- Expected impact of the attack: Most iris recognition systems present very low false acceptance rates. The success rate of these attacks can be considered low.

6.2.2 Photo and Video Attacks

The attack is performed displaying a printed photo, digital image or video from the spoofed iris directly to the sensor of the IRS. Photo attacks are the ones most studied in the literature [12, 18–22] because of two main aspects.

First, with the advent of digital photography and social image sharing (e.g., Flickr, Facebook, Picasa Web, and others), headshots of attacked clients from which the iris can be extracted are becoming increasingly easy to obtain. The face or the voice are biometric modes more exposed than iris. However, iris patterns can 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 Megapixels sensors in most of the nowadays smartphones) and ink printers (1200 dpi in most of the commercial ink printers). Alternatively, most of the mobile devices (smartphones and tablets) are equipped with high-resolution

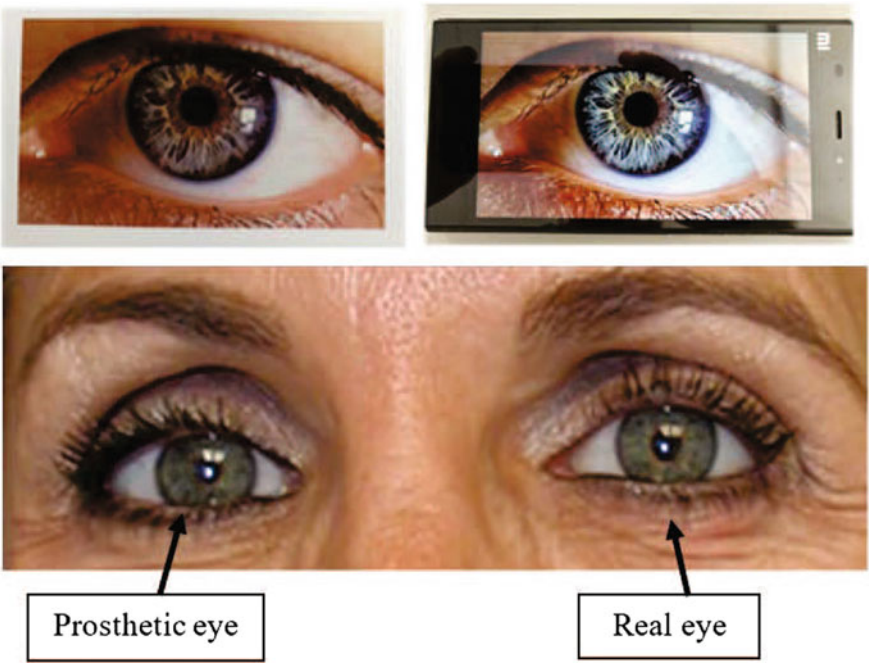

Fig. 6.2 Examples of spoofing artifacts: printed photo (top-left), screen photo (top-right), and prosthetic eye (down). Adapted from Soper Brothers and Associates [http://www.soperbrothers.com]

screens capable of reproducing very natural images and videos in the visible spectrum (see Fig. 6.2).

Video attacks are a sophistication of photo attacks that allows to mimic both the static patterns and the dynamic information of the eye [23–26].

- Information needed to perform the attack: Image or video of the iris of the subject to be impersonated.
- Generation and acquisition of the PAIs: It is relatively easy to obtain high-resolution face photographs from social media and Internet profiles. Other options include the capture using a concealed/hidden camera. Once a photo is obtained, if it is of sufficient quality, one can print the iris region and then present it in front of the iris camera. A screen could also be used for presenting the photograph to the camera. 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.
- Expected impact of the attack: The literature offers a large number of approaches with good detection rates of printed photo attacks [12, 18–21, 27]. 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 a high quality represents a

difficult challenge for PAD approaches based on visible spectrum imaging but not for Near-infrared sensors of commercial systems.

6.2.3 Contact Lens Attacks

This type of attack uses contact lenses created to mimic the pattern of other users (impostor attack) or contact lenses created to masquerade the identity (identity concealer attack). Although the impression of a real iris pattern into contact lenses is theoretically possible, it implies practical difficulties that mitigate the likelihood of this attack. The second scenario is particularly worrying because nowadays, more and more people wear contact lenses (e.g., approximately 125 million people worldwide wear contact lens). We can differentiate between transparent contact lenses and textured contact lenses (also known as printed). Textured contact lenses change the original iris information by the superposition of synthetic patterns (e.g., cosmetic lens to change the color). Although these contact lenses are mostly intended for cosmetics, the same technology can be potentially used to print iris patterns from real users. Once users have been enrolled into the IRS without taking off the textured contact lenses, the IRS can be fooled. Note that asking to remove the contact lenses before the 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 needed for masquerade attacks.
- Generation and acquisition of the fakes: In comparison with photo or video attacks, the generation of textured contact lenses requires a more sophisticated method based on optometrist devices and protocols.
- 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 lens [23, 26, 28–31].

6.2.4 Synthetic Eye Attacks

This type of attack is the most sophisticated. The attack uses synthetic eyes generated to mimic the characteristics of real ones. 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, density).

Table 6.1 Literature on presentation attack detection methods. Summary of key literature about iris PAD methods depending on the type of attack

Type of attack	References	Public databases	Detection errors %
Photo and Video	[11, 12, 33–40]	[20, 21, 24, 27, 35, 41, 42]	0–6
Contact lens	[30, 31, 33, 39, 40]	[27, 43]	0.2–10
Synthetic	[33, 39]	none	0.2–0.3

The number of studies including attacks to iris biometric systems using synthetic eyes is still low [32].

- Information needed to perform the attack: Image of the eye of the client to be attacked.
- Generation and acquisition 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.

Table 6.1 lists key literature on iris PAD including the most popular public databases available for research purposes.

6.3 Presentation Attack Detection Approaches

These methods are also known in the literature as liveness detection, anti-spoofing, or artifact detection among others. The term Presentation Attack Detection (PAD) was adopted in the ISO/IEC 30107-1:2016 [9], 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 [34]. Passive methods include those capable of extracting features from samples obtained by traditional iris recognition systems (e.g., image from the iris sensor). Active methods modify the recognition system in order to obtain features for the PAD method (e.g., dynamic illumination, challenge–response). Static attacks refer to those based on individual samples (e.g., image) while dynamic attacks include artifacts capable to change 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,

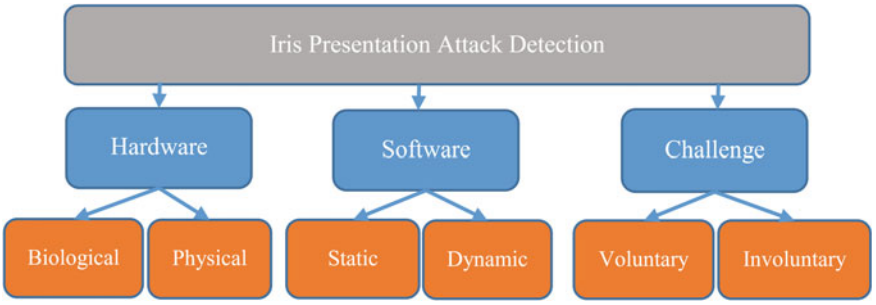

Fig. 6.3 Taxonomy of iris presentation attack detection methods

and challenge–response. The challenge-response approach 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. Figure 6.3 presents a taxonomy of the iris PAD methods introduced in this chapter.

6.3.1 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 biological and physical characteristics of the eye. These characteristics include optical properties related with the reflectance (e.g., light absorption of the different eye layers), color or composition (e.g., melanin or blood vessel structures in the eye), electrical properties (e.g., electrooculography), or physical properties (e.g., density of the eye tissues). These methods include:

- Multispectral imaging [44–47]: 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. Nonliving tissue (e.g., paper, crystal from the screens or synthetic materials including contact lenses) will present reflectance characteristics different to those obtained from a real eye. These approaches exploit illuminations with different wavelengths that vary according to the method proposed and the characteristic involved (e.g., hemoglobin presents an absorption peak in near-infrared bands).
- 3D imaging [21, 48]: The curvature and 3D nature of the eye have been exploited by researchers to develop PAD methods. The 3D profile of the iris is captured in [48] 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 nonuni-

form illumination provided from two different directions. Light Field Cameras (LFC) are used in [21] to acquire multiple depth images and detect the lack of volumetric profiles of photo attacks.

- Electrooculography [49]: The 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 on nonintrusive new methods to acquire the electrooculogram can boost the interest on these approaches.

6.3.2 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 (e.g., one image), dynamic approaches exploit time sequences or multiple samples (e.g., a video sequence).

Some authors propose methods to detect the clues or imperfections introduced by printing devices used during manufacturing of PAIs (e.g., printing process for photo attacks). These imperfections can be detected by Fourier image decomposition [18, 19, 36], wavelet analysis [23], or Laplacian transform [24]. 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 [11, 50]. These techniques exploit iris and image quality in order to detect photo attacks.

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 [51], edges [30], or color [52]. The idea underlying these methods is that the texture of manufacturing materials shows different patterns due to the nonliving properties of materials (e.g., density, viscosity). In this line, the method proposed in [52] analyzes image features obtained from near-infrared and visible spectrums. Local descriptors have been also used for iris PAD: local binary patterns [31, 35, 53, 54], binary statistical image features [13, 53], scale invariant feature transform [26, 53, 55], and local phase quantization [53].

Finally, in [12], researchers evaluate the performance of deep learning techniques for iris photo attack detection with encouraging results. How to use these networks in more challenging attacks requires a deeper study and novel approaches [12].

6.3.3 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 is response 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, microsaccades, etc.). These reactions can be considered as involuntary challenges noncontrolled by the subject. The occurrence of these signals can be also considered as a proof of life. As a main drawback, these methods increase the level of collaboration demanded from the subjects.

The pupil reactions in presence of uniform light or lighting events were early proposed in [28] for PAD applications and more deeply studied in [34]. 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 0.7 Hz and decline with age. The PAD methods based on hippus have been explored to detect photo attacks and prosthetic eye attacks [19, 56]. 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 biomechanical models to serve as PAD methods was evaluated in [57].

The eye is a complex organ that includes different types of surfaces. The reflection of the light in the lens and cornea produces a well-known effect named Purkinje reflections. This effect is an involuntary 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 [39, 45]. Simple photo and video attacks can be detected by these PAD methods. 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).

6.4 Integration with Iris Recognition Systems

PAD approaches should be integrated into iris recognition systems granting a correct and normal workflow. Software-based PAD methods are usually included as modules in the feature extraction algorithms. A potential problem associated to the 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 [58], authors reported that textured lenses can cause the FNMR to exceed 90%. The detection of contact lenses represents a first step in IRS, and specific algorithms have been developed and integrated as a preprocessing module [12, 43, 58]. The final goal of these algorithms is to detect and to filter the images to remove the image patterns generated by contact lenses.

Hardware-based PAD approaches are usually integrated before the iris sensor or as an independent parallel module (see Fig. 6.4). 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 user. This collaboration usually introduces delays in the recognition process and some users can perceive it as an unfriendly process.

There are two basic integration schemes:

- 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) [3, 59].
- Series integration: The sample is first analyzed by the PAD system. In case of a legitimate user, the IRS processes the sample. Otherwise, the detection of an attack will avoid unnecessary recognition and the sample will be directly discarded.

6.5 Conclusions

Iris recognition systems have been improved during the last decade achieving better performance, more convenient acquisition at a distance, and full integration with mobile devices. However, the robustness against attacks is still a challenge for the research community and industrial applications. 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 its simplicity and high attack success rates. The acquisition at a distance achieved by recent advances on new sensors and the public exposure of the face, and therefore the iris, make 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. In 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

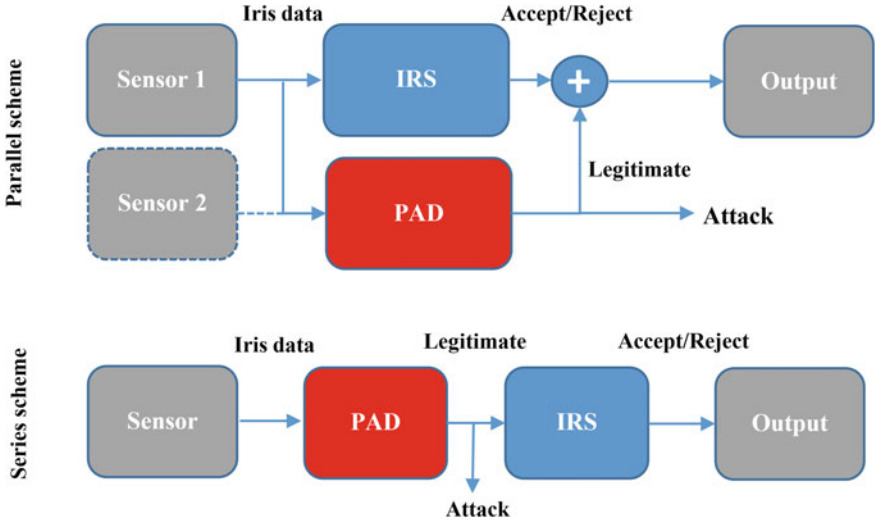

Fig. 6.4 Integration of Presentation Attack Detection (PAD) with Iris Recognition Systems (IRS) in parallel (top) and serial (down) schemes

still challenges associated to most sophisticated attacks such as those using textured contact lenses and synthetic eyes.

Acknowledgements This work was done in the context of the TABULA RASA and BEAT projects funded under the 7th Framework Programme of EU. This work was supported in part by the CogniMetrics Project under Grant TEC2015-70627-R from MINECO/FEDER.

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. Burge MJ, Bowyer KW (eds) (2013) Handbook of iris recognition. Springer, Berlin
3. Fierrez J, Morales A, Vera-Rodriguez R, Camacho D (2018) Multiple classifiers in biometrics. part 1: fundamentals and review. Inf Fusion 44:57–64
4. Galbally J, Gomez-Barrero M (2017) chapter. In: Rathgeb C, Busch C (eds) Iris and periocular biometric recognition. 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. Tech Rep, IDinsight
7. Nguyen K, Fookes C, Jillela R, Sridharan S, Ross A (2017) Long range iris recognition: a survey. Pattern Recognit 72:123–143
8. Chaos Computer Club Berlin: chaos computer clubs breaks iris recognition system of the samsung galaxy s8 (2017). https://www.ccc.de/en/updates/2017/iriden
9. ISO/IEC CD 30107-1. Information technology - biometrics - presentation attack detection - Part 1: framework (2016)

10. Daugman J (1999) Biometrics. Personal identification in a networked society. In: Chapter, Recognizing persons by their iris patterns. Kluwer Academic Publishers, Dordrecht, pp 103–121
11. 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
12. 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
13. Raghavendra R, Busch C (2014) Presentation attack detection algorithm for face and iris biometrics. In: Proceedings of the IEEE European signal processing conference (EUSIPCO), pp 1387–1391
14. Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. IBM Syst J 40(3):614–634
15. Gomez-Barrero M, Maiorana E, Galbally J, Campisi P, Fierrez J (2017) Multi-biometric template protection based on homomorphic encryption. Pattern Recogn 67:149–163
16. Hadid A, Evans N, Marcel S, Fierrez J (2015) Biometrics systems under spoofing attack. IEEE Signal Process Mag 32:20–30
17. Johnson P, Lazarick R, Marasco E, Newton E, Ross A, Schuckers S (2012) Biometric liveness detection: framework and metrics. In: Proceedings of the NIST international biometric performance conference (IBPC)
18. Czajka A (2013) Database of iris printouts and its application: development of liveness detection method for iris recognition. In: Proceedings of the international conference on methods and models in automation and robotics (MMAR), pp 28–33
19. Pacut A, Czajka A (2006) Aliveness detection for iris biometrics. In: Proceedings of the IEEE international Carnahan conference on security technology (ICCST), pp 122–129
20. 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 the COST 2101 workshop on biometrics and identity management (BioID). LNCS, vol 5372. Springer, Berlin, pp 181–190
21. Raghavendra R, Busch C (2014) Presentation attack detection on visible spectrum iris recognition by exploring inherent characteristics of light field camera. In: Proceedings of the IEEE international joint conference on biometrics (IJCB) (2014)
22. Thalheim L, Krissler J (2002) Body check: biometric access protection devices and their programs put to the test. ct magazine, pp 114–121
23. He X, Lu Y, Shi P (2009) A new fake iris detection method. In: Proceedings of the IAPR/IEEE international conference on biometrics (ICB). LNCS, vol 5558. Springer, Berlin, pp 1132–1139
24. 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 the of IEEE international conference on biometrics: theory and applications (BTAS)
25. 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
26. Zhang H, Sun Z, Tan T, Wang J (2011) Learning hierarchical visual codebook for iris liveness detection. In: Proceedings of the IEEE international joint conference on biometrics (IJCB)
27. Yambay D, Doyle JS, Boyer KW, Czajka A, Schuckers S (2014) Livdet-iris 2013 - iris liveness detection competition 2013. In: Proceedings of the IEEE international joint conference on biometrics (IJCB)
28. Daugman J (2004) Iris recognition and anti-spoofing countermeasures. In: Proceedings of the international biometrics conference (IBC)
29. von Seelen UC (2005) Countermeasures against iris spoofing with contact lenses. In: Proceedings of the biometrics consortium conference (BCC)
30. Wei Z, Qiu X, Sun Z, Tan T (2008) Counterfeit iris detection based on texture analysis. In: Proceedings of the IAPR international conference on pattern recognition (ICPR)

31. Zhang H, Sun Z, Tan T (2010) Contact lense detection based on weighted LBP. In: Proceedings of the IEEE international conference on pattern recognition (ICPR), pp 4279–4282
32. 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
33. Chen R, Lin X, Ding T (2012) Liveness detection for iris recognition using multispectral images. Pattern Recogn Lett 33:1513–1519
34. Czajka A (2015) Pupil dynamics for iris liveness detection. IEEE Trans Inf Forensics Secur 10:726–735
35. Gupta P, Behera S, Singh MVV (2014) On iris spoofing using print attack. In: IEEE international conference on pattern recognition (ICPR)
36. He X, Lu Y, Shi P (2008) A fake iris detection method based on FFT and quality assessment. In: Proceedings of the IEEE Chinese conference on pattern recognition (CCPR)
37. Huang X, Ti C, zhen Hou Q, Tokuta A, Yang R (2013) An experimental study of pupil constriction for liveness detection. In: Proceedings of the IEEE workshop on applications of computer vision (WACV), pp 252–258
38. Kanematsu M, Takano H, Nakamura K (2007) Highly reliable liveness detection method for iris recognition. In: Proceedings of the SICE annual conference, international conference on instrumentation, control and information technology (ICICIT), pp 361–364
39. Lee EC, Yo YJ, Park KR (2008) Fake iris detection method using Purkinje images based on gaze position. Opt Eng 47(067):204
40. 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 the IEEE international joint conference on biometrics (IJCB), pp 1–6
41. Raghavendra R, Busch C (2015) Robust scheme for iris presentation attack detection using multiscale binarized statistical image features. IEEE Trans Inf Forensics Secur 10:703–715
42. Sequeira AF, Oliveira HP, Monteiro JC, Monteiro JP, Cardoso JS (2014) MobILive 2014 - mobile iris liveness detection competition. In: Proceedings of the IEEE international joint conference on biometrics (IJCB)
43. 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
44. He Y, Hou Y, Li Y, Wang Y (2010) Liveness iris detection method based on the eye's optical features. In: Proceedings of the SPIE optics and photonics for counterterrorism and crime fighting VI, p 78380R
45. Lee EC, Park KR, Kim J (2006) Fake iris detection by using Purkinje image. In: Proceedings of the IAPR international conference on biometrics (ICB), pp 397–403
46. Lee SJ, Park KR, Lee YJ, Bae K, Kim J (2007) Multifeature-based fake iris detection method. Opt Eng 46(127):204
47. Park JH, Kang MG (2005) Iris recognition against counterfeit attack using gradient based fusion of multi-spectral images. In: Proceedings of the of international workshop on biometric recognition systems (IWBRS). LNCS, vol 3781. Springer, Berlin, pp 150–156
48. Lee EC, Park KR (2010) Fake iris detection based on 3D structure of the iris pattern. Int J Imaging Syst Technol 20:162–166
49. Krupiski R, Mazurek P (2012) Estimation of electrooculography and blinking signals based on filter banks. In: Proceedings of the of the 2012 international conference on computer vision and graphics, pp 156–163
50. Galbally J, Ortiz-Lopez J, Fierrez J, Ortega-Garcia J (2012) Iris liveness detection based on quality related features. In: Proceedings of the IAPR international conference on biometrics (ICB), pp 271–276
51. He X, An S, Shi P (2007) Statistical texture analysis-based approach for fake iris detection using support vector machines. In: Proceedings of the IAPR international conference on biometrics (ICB), LNCS, vol 4642. Springer, Berlin, pp 540–546
52. Alonso-Fernandez F, Bigun J (2014) Fake iris detection: a comparison between near-infrared and visible images. In: Proceedings of the IEEE international conference on signal-image technology and internet-based systems (SITIS), pp 546–553

53. Gragnaniello D, Poggi G, Sansone C, Verdoliva L (2015) An investigation of local descriptors for biometric spoofing detection. IEEE Trans Inf Forensics Secur 10:849–863
54. He Z, Sun Z, Tan T, Wei Z (2009) Efficient iris spoof detection via boosted local binary patterns. In: Proceedings of the IEEE international conference on biometrics (ICB)
55. 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
56. Park KR (2006) Robust fake iris detection. In: Proceedings of the of articulated motion and deformable objects (AMDO). LNCS, vol 4069. Springer, Berlin, pp 10–18
57. Komogortsev O, Karpov A (2013) Liveness detection via oculomotor plant characteristics: attack of mechanical replicas. In: Proceedings of the international conference of biometrics (ICB) (2013)
58. Bowyer KW, Doyle JS (2014) Cosmetic contact lenses and iris recognition spoofing. IEEE Comput 47:96–98
59. 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