A REVIEW OF IRIS ANTI-SPOOFING

Javier Galbally

European Commission - Joint Research Centre
Inst. for the Protection and Security of the Citizen

Marta Gomez-Barrero

Universidad Autonma de Madrid
Biometric Recognition Group - ATVS

ABSTRACT

To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured physical synthetic sample, is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. The whole biometric community, including researchers, developers, standardizing bodies and vendors, has thrown itself into the very challenging task of proposing and developing efficient protection methods against this threat, known as *spoofing*. The goal of this paper is to provide a comprehensive and structured overview on the work that has been carried out over the last decade in the field of iris anti-spoofing. In brief, the paper has been thought as a tool to provide biometric researchers an overall picture of the current panorama in the mentioned area following a systematic approach.

Index Terms— Iris recognition, anti-spoofing, vulnerabilities

1. INTRODUCTION

In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous and very diverse initiatives focused on this major field of research. Among the different threats analyzed, the so-called *direct* or *spoofing* attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris, the fingerprint [1], or the face [2]. In these attacks, the intruder uses some type of synthetically produced artifact (e.g., printed iris image, gummy finger or face mask), or tries to mimic the behaviour of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. As this type of attacks are performed in the analog domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective.

The aforementioned works and other analogue studies have clearly shown the necessity to propose and develop specific protection methods against this threat. This way, researchers have focused on the design of specific countermeasures that enable biometric systems to detect fake samples and reject them, thus improving the robustness and security level of the systems. This has initiated a new research area known as "biometric anti-spoofing" [3].

An *anti-spoofing* method is usually accepted to be any technique that is able to automatically distinguish between real biometric traits presented to the sensor and synthetically produced artefacts imitating the genuine trait. Although it is a very extended one, this nomenclature is not carved in stone and, very often, anti-spoofing approaches are also referred in the literature as *liveness detection*, *vitality detection* or the standardized term *presentation attack detection* techniques.

From a general perspective, iris anti-spoofing techniques may be classified into one of two groups depending on the part of the biometric system where they are integrated: sensor-level and feature-level techniques.

Sensor-level techniques. Usually referred to in the literature as *hardware-based* techniques. These methods add some specific device to the sensor in order to detect particular properties of a living trait (e.g., specific reflection properties of the eye or pupil dynamics). In general, sensor-level approaches measure one of three characteristics, namely: (i) intrinsic properties of a living body; (ii) involuntary signals of a living body; (iii) responses to external stimuli, also known as *challenge-response* methods, which require the user cooperation as they are based on detecting voluntary (behavioural) or involuntary (reflex reactions) responses to an external signal.

Feature-level techniques. Usually referred to in the literature as *software-based* techniques. In this case the fake trait is detected once the sample has been acquired with a standard sensor, that is, features used to distinguish between real and fake traits are extracted from the biometric sample, and not the human body itself. These methods are installed after the sensor, usually operating as part of the feature extractor module. They can be further classified into *static* and *dynamic* anti-spoofing methods, depending on whether they operate with only one instance of the biometric trait, or with a sequence of samples captured over time.

A graphical diagram of the categorization proposed above is given in Fig. 1. Although the present article will follow this three-group taxonomy, this is not a closed classification and some techniques may fall into one or more of these groups. Nonetheless, we believe that this taxonomy can help to visualize the current biometric anti-spoofing scene. Additionally,

978-1-4799-8105-2/15/$31.00

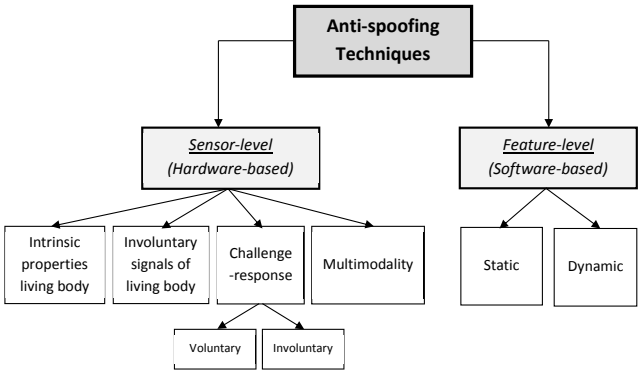

Fig. 1. General taxonomy of anti-spoofing methods considered in the present article with two main groups: sensor-level and feature-level techniques.

the reader should be aware that, even though this is a quite extended and accepted classification, others are also possible.

Similarly to what has been recently done for fingerprint [1] or face [2], in Sect. 3, we present a comprehensive review of the most successful and popular anti-spoofing methods which have been proposed in the literature for iris. Before this review, a brief summary of the most common spoofing techniques is presented in Sect. 2. This initial short overview on iris spoofing can be useful to understand the rationale behind the design of some anti-spoofing techniques later presented This way, the reader can also gain a more general perspective of the current panorama in the field of iris spoofing.

2. IRIS SPOOFING

Whilst iris recognition is one of the most accurate biometric technologies, it is also a younger research field compared for instance to fingerprint or face, with pioneer research studies dating to the early 90's [17]. As a consequence, iris spoofing has also a somewhat shorter tradition than that of other long studied modalities. Almost all iris spoofing attacks reported in the literature follow one of three trends: photo attacks, contact-lens attacks or artificial-eye attacks.

Photo Attacks. From a chronological point of view, these were the first attacks to be reported in the literature and they still remain popular, probably due to their great simplicity and, in many cases, high success rate. They are carried out presenting a photograph of the genuine iris [12, 6]. In the vast majority of cases this image is printed on paper (i.e., print-attacks), although it can also be displayed on the screen of a digital device such as a mobile phone or a tablet (i.e., digital-photo attacks). A more sophisticated variation of photo-attacks are *video-attacks*, which consist of the presentation to the scanner of an eye video replayed on a multimedia device such as a smart phone or a laptop. This way, cues related to the dynamics of the eye are not any more effective to detect such spoofing attempts [18]. Finally, it is also worth noting that recent works on iris image reconstruction have shown that a compromised iris template can be reversed engineered to produce an image with a very similar iriscode to the original sample [19]. These algorithms could also potentially lead to photo attacks using the reconstructed samples, although the vulnerability to such spoofing threat has not yet been rigorously assessed.

Contact-Lens Attacks. These appeared as a further evolution of the classic photo-attacks. In this case, the pattern of a genuine iris is printed on a contact lens that the attacker wears during the fraudulent access attempt . Such attacks are very difficult to be recognized even by human operators, and represent a real challenge for automatic protection methods as all the contextual and ancillary information of the iris corresponds to that of a living eye [20, 21, 10, 22].

Artificial-Eye Attacks. These are far less common than the previous two types and have just started to be systematically studied [22, 5]. Although some works may be found where very sophisticated spoofing artefacts are presented, in most cases these attacks are carried out with artificial eyes made of plastic or glass. Anti-spoofing methods based on the analysis of depth properties of the eye are more prone to be deceived by such 3D reproductions.

3. IRIS ANTI-SPOOFING

In order to give an overall perspective of the different methods studied so far in the iris anti-spoofing related literature, Table 1 presents a summary with relevant features of the most representative works cited in this section. The table should be understood as a tool for quick reference and in no case as a strict comparative study, as most of the results shown in the last column have been obtained using proprietary databases designed to evaluate a specific method (see column "Database"). Moreover, in general, these databases are too small to obtain statistically meaningful results and are in most cases presented in their respective works only as a proof of concept.

3.1. Sensor-Level Approaches

Daugman, regarded as the father of automatic iris recognition due to his pioneering and very successful early works in the field [17], presented some of the first ideas concerning sensor-level anti-spoofing countermeasures for iris biometrics. In some of his initial works Daugman explored different aspects related to iris recognition, proposing some eye specific features that could be potentially used as hardware-based countermeasures against direct attacks [23, 24]. Some of the characteristics mentioned in these early studies are the spectrographic properties of different parts of the eye (tissue, fat, blood, melanin pigment) and the four Purkinje reflections caused by the four optical surfaces comprised inside the eye.

Iris anti-spoofing techniques: General overview					
Sensor-Level techniques					
Reference	**Subtype**	**Features and methodology**	**Attack**	**Database**	**Error**
2013, Huang et al. [4]	Challenge-response	Pupil contraction after a lighting event	Photo	Proprietary, 12 identities, 322 samples	0.2%
2012, Chen et al. [5]	Intrinsic property	Conjunctival vessels detection using multispectral imaging	Photo, contact-lens, artificial	Proprietary, 100 identities, 2000 samples	0.2%
2014, Raghav. and Busch [6]	Intrinsic property	Depth variation Light Field Camera	Photo	Public, GUC-LF-VIAr DB [6] 104 identities, 4847 samples	1.1%
2008, Lee et al. [7]	Invol. body signal	Four Purkinje reflections using NIR illumination	Photo, contact-lens, artificial	Proprietary, 30 identities, 500 samples	0.3%
2015, Czajka [8]	Invol. body signal	Pupil dynamics	Photo	Proprietary, 52 identities, 204 videos	0%
Feature-Level techniques					
Reference	**Subtype**	**Features and methodology**	**Attack**	**Database**	**Error**
2008, He et al. [9]	Static	Iris texture spectrum analysis using the FFT	Photo	Proprietary, 50 identities, 1,500 samples	1%
2010, Zhang et al. [10]	Static	Iris texture analysis using Weighted LBP	Contact-lens	Proprietary, 72 identities, 1,400 samples	0.5%
2014, Galbally et al. [11]	Static	Iris texture analysis using image quality measures	Photo	Public, ATVS-FIr DB [12], 50 identities, 1,600 samples	0.3%
2015, Menotti et al. [13]	Static	Iris texture analysis using deep learning	Photo	Public, ATVS-FIr DB [12] + LivDet-Iris DB [14] + MobBIOfake DB [15]	0.9%
2015, Raghav. and Busch [16]	Dynamic	Iris texture analysis using multiscale binary statistical image features	Photo	Public, VSIA DB [16], 110 identities, 1,100 samples	0%

Table 1. Summary of the most relevant iris anti-spoofing techniques presented in Sect. 3. The column "subtype" corresponds to the algorithm subtype within each of the two main categories considered in the work (sensor-level and feature-level) as shown in the taxonomy in Fig. 1. The column "attack" refers to the type of iris spoofing attacks considered in the work as defined in Sect. 2: photo, contact-lens or artificial-eye attacks.

A second group of possible anti-spoofing mechanisms highlighted in [24] are those based on behavioural eye features like the eye hippus (i.e., permanent oscillation that the eye pupil presents even under uniform lighting conditions) or the pupil response to a sudden lighting event.

Although the works above do not contain any experimental validation of the presented measures and, in the best cases, he just gave individual examples as valid proofs of concept, his proposals set the basis for many of the sensor-based iris anti-spoofing schemes that have been later developed in the literature and that are reviewed here.

As suggested in [23], the spectrographic properties of the eye tissue (e.g., fat or blood) can be used as a liveness cue in iris recognition. If the iris presented to the system is a glass eye, a photograph or dead tissue, spectrographic analyses could help to detect the spoofing attack. Following this approach, an anti-spoofing technique has been proposed using multispectral illumination to estimate the difference in the reflectance properties between the iris an the sclera at different wavelengths [25]. In a subsequent work, these measures were complemented also with the thickness of the corneoscleral limbus [26], and a comparison is established on a database of print, contact-lens and artificial-eye attacks. Based on this same multispectral principle, in [27], a novel sensor-level anti-spoofing method is proposed using NIR illumination at different wavebands and positions in order to detect the reflection properties of the different parts of the eye. Following a similar scheme to the spectrographic and reflectance signatures used in the previous works, in [5] an anti-spoofing technique was presented based on the specific characteristics of conjunctival vessels and iris textures that may be extracted from multispectral images. Also as part of this multispectral imaging research line, in two successive works [28, 29] the authors present a novel iris recognition method using the grey scale sample resulting from the fusion of several images acquired at different wavelengths, and show that such a authentication approach is robust to attacks carried out with photos, contact lenses and artificial irises.

The four Purkinje reflections have also been exploited in the literature to develop iris liveness detection methods.

These reflections are caused in a natural eye by the four optical surfaces that reflect light: the front and back surfaces of the cornea as well as the front and back surfaces of the lens. The position of the reflected light determines the position of the reflections. Therefore, a change in the location of the light source should even detect photographs displaying these reflections [7]. Varying positions of near-infrared light diodes used during image acquisition could also be used to analyse this property of the living eye as first suggested in [30]. However, as it was the case with the previous features, the use of such a characteristic against attack attempts where a real pupil is displayed is at least unclear.

Another intrinsic property of the human body that can be exploited for iris anti-spoofing purposes is the 3D nature of the eye. Based on this characteristic, a novel iris liveness detection method was proposed in [31] using a specific acquisition sensor with two NIR light sources attached to the sides of the camera. This way, the authors are able to acquire images where the 3D structure of the real irises is clearly visible thanks to the change of shadows.

Following a similar hypothesis to the previous work, that is, that it should be possible to detect the 3D structure of the eye with respect to 2D surfaces used in photos attacks, the authors in [6] have developed a presentation attack detection method based on a Light Field Camera (LFC). The method, tested on a database comprising printed and digital-photo attacks from 104 unique iris patterns, measures the variation of focus between multiple depth images rendered by the LFC.

As mentioned above, involuntary signals of the body to measure liveness detection in iris recognition schemes. One of these interesting involuntary signals is the hippus, which is a pupillary diameter oscillation at about 0.5 Hz, occurring even under constant illumination. The coefficient of variation is at least 3%, although it declines with age. Several works have shown that this liveness cue can effectively be used to detect prosthetic eyes, high-resolution photographs or dead tissue [32, 33]. However, as in the previous cases, its performance against video-based attacks or contact-lens attacks has not been tested yet.

Based on an analogous principle to the previous methods, the analysis of the pupil dynamics has also been studied as part of challenge-response approaches. In iris recognition, an involuntary reflex of the body that can be easily triggered by changing the illumination level is the variation of the pupil size. This size fluctuation in response to controlled external changes of light intensity has successfully been used for iris spoofing detection in the literature [32, 34, 4, 8]. The pupillary light reflex does not only cause a change in the pupil size but also on the iris texture brightness, which was exploited in [35] to develop a liveness detection algorithm against print attacks. The two types of changes, pupil size and iris texture, were combined in [36] and tested against contact-lens attacks. In a more recent work [37], the pupil-dynamics metrics were combined with some of the previously proposed feature-level techniques based on the study of the iris texture, such as the multispectral reflectance analysis and the frequency spectrum analysis, and evaluated on a database of photo prints, contact lenses and artificial eyes showing very good results. Another interesting effect which can be observed when the pupil size changes, and which could potentially be used for liveness detection, is the non-elastic distortion of the iris tissue known as iridal pattern deformation [38].

Although all the above mentioned dynamic-based schemes may be efficient even against print-attacks where the pupil has been removed or against contact-lens attacks, it entails a high level of discomfort for the user due to the sudden lighting changes. Therefore, following this trend on the analysis of eye movement cues, other anti-spoofing techniques could be conceived based on voluntary responses of the users such as blinking or gazing at one specific point, so that the degree of unpleasantness is reduced. A preliminary study has been recently presented considering this line of research based on eye movement cues [39].

Following a similar dynamic-based perspective, a presentation attack detection method based on the Eulerian Video Magnification (EVM) was presented in [18] for video-based iris recognition systems. Since this approach requires an iris video, it is included within the sensor-level methods as usual iris scanners only acquire single iris images. The method has shown a remarkable performance even against video attacks.

3.2. Feature-Level Approaches

Regarding feature-level approaches, it was also Daugman who first proposed, mostly as a theoretical framework, some of the feature-level methods that have been later exploited in the field of presentation attack detection for iris biometrics [23, 24].

One of the characteristics pointed out in [24] as a potential cue to detect fake and real irides were the retinal light reflections commonly known as the "red-eye effect". Essentially, light entering the eye is reflected back to the light source from the retina; this effect can be captured by a regular sensor, with no need for any additional hardware device, as long as the angle between light source, eye and camera is smaller than 2.5 degrees. Although such anti-spoofing methods would be very efficient against regular print attacks or even artificial-eye attacks, its performance would be at least under question when dealing with contact lenses.

Daugman also indicated in his initial works that the printing process can leave detectable traces on spoofing artefacts, and that a simple 2D Fourier analysis of the acquired image can expose that unnatural behaviour. Pacut and Czajka [32], Czajka [40], and He *et al.* [9], have developed automated feature-level methods to analyse artificial frequencies in printed iris images. Following the same line, the Wavelet Transform has also been used, combined with a Support Vector Machine (SVM) classifier, as a way to extract discrimi-

native features from the iris frequency spectrum in the task of detecting photo-attacks [21]. Another frequency-based approach was presented in [41], where the iris images are decomposed into Laplacian pyramids of various scales in order to analyze the frequency responses in different orientations. This constitutes the first iris anti-spoofing work that considers video attacks.

From those early works based on the spectral analysis of iris images, different image processing methods have been applied as an alternative to extract features that allow telling apart real and fake irides. For instance, in [42] four features based on the grey level values of the outer region of fake contact lenses are proposed for software-based spoofing detection. Similarly, in a subsequent work, grey level values of the iris texture are studied in order to characterize the visual primitives of the iris complementing them with measures related to the iris edge sharpness [20].

One of the most active trends for presentation attack detection in iris systems is the use of local descriptors for the analysis of the iris texture. In [22, 43], for example, iris texture primitives of real and fake images were modeled using a hierarchical visual codebook to represent the extracted Scale-Invariant Feature Transform (SIFT) features and tested against attacks carried out with printed photos, contact lenses and even plastic eyes. Also the very popular Local Binary Patterns (LBPs) have been considered for the texture representation of the iris image. This approach has been successfully applied to iris anti-spoofing in several works [44, 10, 45], where the efficiency of different configurations of LBPs has been evaluated against a number of known attacks (e.g., contact lenses, photo-attacks, artificial irises, etc.) Other texture-based features that have been studied include the use of Binary Statistical Image Features (BSIF) that was tested on different databases including a new large dataset comprising five types of presentation attacks including print and digital attacks [16]. Finally, a comprehensive study regarding local image descriptors for anti-spoofing purposes was presented in [46]. The work includes an analysis of the combination of multiple local features for the representation of iris texture including LBP, BSIF, SIFT or Local Phase Quantization (LPQ), tested on iris, face and fingerprint spoofing databases with very good results. Also, a good comparative experimental study of several of the above mentioned methods can be found in the article reporting the results of the first Liveness Detection-Iris Competition (LivDet-Iris) held in 2013 [14].

Currently, one of the most promising trends in the wide field of image analysis and understanding is the use of deep neural networks for image classification. A pioneering work in this area has recently analyzed the accuracy of two deep learning approaches applied to the problem of iris, face and fingerprint anti-spoofing reporting very good results against iris print-attacks [13]. However, the accuracy of these approaches against other type of presentation attacks still requires further attention.

The use of image quality assessment metrics has also been studied for iris liveness detection motivated by the assumption that a fake image captured in an attack attempt is expected to have different quality than a real sample acquired in the normal operation scenario for which the sensor was designed. Following this "quality-difference" hypothesis several iris-specific quality metrics [47] and general image quality metrics [11] have been studied to distinguish between real iris images and those acquired in photo-attacks.

Many of the approaches mentioned above, are starting to be also studied in the context of mobile iris applications where sensor-level methods are more difficult to integrate due to the inherent hardware restrictions of this scenarios [48, 15].

4. CONCLUSION

The current biometric security context related to spoofing, has promoted in the last 10 years a massive amount of research which has flooded journals, conferences and media with new information, methods, algorithms and techniques regarding anti-spoofing approaches that intend to make this technology safer. This has been the case specially for some of the most deployed, popular and mature modalities such as the iris, which has also been shown to be one of the most exposed to spoofing. The current article is an attempt to contribute to the difficult review task of the numerous contributions and initiatives that are currently being made in the area of anti-spoofing.

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

5. REFERENCES

[1] E. Marasco and A. Ross, "A survey on anti-spoofing schemes for fingerprints," *ACM Comp. Surveys*, vol. 47, pp. 1–36, 2014.

[2] J. Galbally, S. Marcel, and J. Fierrez, "Biometric anti-spoofing methods: A survey in face recognition," *IEEE Access*, vol. 2, pp. 1530–1552, 2014.

[3] Sebastien Marcel, Mark Nixon, and Stan Z. Li, Eds., *Hanbook of biometric Anti-Spoofing*, Springer, 2014.

[4] X. Huang, C. Ti, et al., "An experimental study of pupil constriction for liveness detection," in *Proc. WACV*, 2013, pp. 252–258.

[5] R. Chen, X. Lin, and T. Ding, "Liveness detection for iris recognition using multispectral images," *PRL*, vol. 33, pp. 1513–1519, 2012.

[6] R. Raghavendra and C. Busch, "Presentation attack detection on visible spectrum iris recognition by exploring inherent characteristics of light field camera," in *Proc. IEEE IJCB*, 2014.

[7] E. C. Lee et al., "Fake iris detection method using purkinje images based on gaze position," *Optical Engineering*, vol. 47, pp. 067204, 2008.

[8] A. Czajka, "Pupil dynamics for iris liveness detection," *IEEE TIFS*, vol. 10, pp. 726–735, 2015.

[9] X. He, Y. Lu, and P. Shi, "A fake iris detection method based on FFT and quality assessment," in *Proc. CCPR*, 2008.

[10] H. Zhang, Z. Sun, and T. Tan, "Contact lense detection based on weighted LBP," in *Proc. ICPR*, 2010, pp. 4279–4282.

[11] J. Galbally et al., "Image quality assessment for fake biometric detection: Application to iris, fingerprint and face recognition," *IEEE TIP*, vol. 23, pp. 710–724, 2014.

[12] V. Ruiz-Albacete et al., "Direct attacks using fake images in iris verification," in *Proc. COST 2101 BioID*, 2008, Springer LNCS-5372, pp. 181–190.

[13] D. Menotti et al., "Deep representations for iris, face, and fingerprint spoofing detection," *IEEE TIFS*, vol. 10, pp. 864–878, 2015.

[14] D. Yambay, J. S. Doyle, et al., "Livdet-iris 2013 - iris liveness detection competition 2013," in *Proc. IJCB*, 2014.

[15] A. F. Sequeira et al., "MobILive 2014 - Mobile Iris Liveness Detection Competition," in *Proc. IEEE IJCB*, 2014.

[16] R. Raghavendra and C. Busch, "Robust scheme for iris presentation attack detection using multiscale binarized statistical image features," *IEEE TIFS*, vol. 10, pp. 703–715, 2015.

[17] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE TPAMI*, vol. 15, pp. 1148–1161, 1993.

[18] K. B. Raja et al., "Video presentation attack detection in visible spectrum iris recognition using magnified phase information," *IEEE TIFS*, vol. 10, pp. 2048–2056, 2015.

[19] J. Galbally, A. Ross, et al., "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms," *CVIU*, vol. 117, pp. 1512–1525, 2013.

[20] Z. Wei, X. Qiu, et al., "Counterfeit iris detection based on texture analysis," in *Proc. ICPR*, 2008.

[21] X. He, Y. Lu, and P. Shi, "A new fake iris detection method," in *Proc. ICB*. 2009, pp. 1132–1139, Springer LNCS-5558.

[22] H. Zhang, Z. Sun, et al., "Learning hierarchical visual codebook for iris liveness detection," in *Proc. IJCB*, 2011.

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

[24] J. Daugman, "Iris recognition and anti-spoofing countermeasures," in *Proc. IBC*, 2004.

[25] S. J. Lee et al., "Robust fake iris detection based on variation of the reflectance ratio between the iris and the sclera," in *Proc. BSym*, 2006, pp. 66–71.

[26] S. J. Lee et al., "Multifeature-based fake iris detection method," *Optical Engineering*, vol. 46, pp. 127204, 2007.

[27] Y. He et al., "Liveness iris detection method based on the eye's optical features," in *Proc. SPIE OPCCF*, 2010.

[28] J. H. Park and M. G. Kang, "Iris recognition against counterfeit attack using gradient based fusion of multi-spectral images," in *Proc. IWBRS*, 2005, Springer LNCS-3781, pp. 150–156.

[29] J. H. Park and M. G. Kang, "Multispectral iris authentication system against counterfeit attack using gradient-based image fusion," *Optical Eng.*, vol. 46, pp. 117003, 2007.

[30] E. C. Lee et al., "Fake iris detection by using purkinje image," in *Proc. ICB*, 2006, pp. 397–403.

[31] E. C. Lee and K. R. Park, "Fake iris detection based on 3D structure of the iris pattern," *Int. Journal of IST*, vol. 20, pp. 162–166, 2010.

[32] A. Pacut and A. Czajka, "Aliveness detection for iris biometrics," in *Proc. ICCST*, 2006, pp. 122–129.

[33] K. R. Park, "Robust fake iris detection," in *Proc. AMDO*, 2006, Springer LNCS-4069, pp. 10–18.

[34] R. Bodade and S. Talbar, "Dynamic iris localisation: A novel approach suitable for fake iris detection," *Int. Journal of CISIMA*, vol. 2, pp. 163–173, 2010.

[35] M. Kanematsu et al., "Highly reliable liveness detection method for iris recognition," in *Proc. ICIT*, 2007, pp. 361–364.

[36] N. B. Puhan et al., "A new iris liveness detection method against contact lens spoofing," in *Proc. ISCE*, 2011.

[37] R. Bodade and S. Talbar, "Fake iris detection: A holistic approach," *Int. Journal of CA*, vol. 19, 2011.

[38] V. F. Pamplona et al., "Photorealistic models for pupil light reflex and iridal pattern deformation," *ACM Trans. on Graphics*, vol. 28, pp. 106:1–106:12, 2009.

[39] O. Komogortsev and A. Karpov, "Liveness detection via oculomotor plant characteristics: Attack of mechanical replicas," in *Proc. ICB*, 2013.

[40] A. Czajka, "Database of iris printouts and its application: Development of liveness detection method for iris recognition," in *Proc. MMAR*, 2013, pp. 28–33.

[41] K. B. Raja et al., "Presentation attack detection using laplacian decomposed frequency response for visible spectrum and near-infra-red iris systems," in *Proc. IEEE BTAS*, 2015.

[42] X. He et al., "Statistical texture analysis-based approach for fake iris detection using support vector machines," in *Proc. ICB*, 2007, pp. 540–546.

[43] Z. Sun, H. Zhang, et al., "Iris image classification based on hierarchical visual codebook," *IEEE TPAMI*, vol. 36, pp. 1120–1133, 2014.

[44] Z. He, Z. Sun, et al., "Efficient iris spoof detection via boosted local binary patterns," in *Proc. ICB*, 2009.

[45] P. Gupta, S. Behera, et al., "On iris spoofing using print attack," in *Proc. ICPR*, 2014.

[46] D. Gragnaniello et al., "An investigation of local descriptors for biometric spoofing detection," *IEEE TIFS*, vol. 10, pp. 849–863, 2015.

[47] J. Galbally et al., "Iris liveness detection based on quality related features," in *Proc. ICB*, 2012, pp. 271–276.

[48] A. F. Sequeira et al., "Iris liveness detection methods in mobile applications," in *Proc. IEEE VISAPP*, 2014, pp. 22–33.