ISSN: 0976-3376

Available Online at http://www.journalajst.com

ASIAN JOURNAL OF SCIENCE AND TECHNOLOGY

Asian Journal of Science and Technology
Vol. 14, Issue, 08, pp. 12613-12617, August, 2023

RESEARCH ARTICLE

LIVENESS DETECTION TECHNIQUES IN USER AUTHENTICATION ON IOT DEVICES

***Joshua Teddy Ibibo**

Blockpass ID Lab, School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK

ARTICLE INFO

Article History:
Received 11th May, 2023
Received in revised form
27th June, 2023
Accepted 20th July, 2023
Published online 24th August, 2023

Keywords:

Biometrics, Spoofing Attacks, Liveness Detection, Mobile Devices, Face Recognition, Fingerprint Recognition, Iris Recognition.

ABSTRACT

Biometric authentication is now widely utilised as an alterna-tive to passwords on IoT devices such as smartphones. However, present biometric systems are subject to spoofing attacks. Several liveness detec-tion techniques have been presented to determine whether a live person or an artificial duplicate is in front of the biometric sensor. However, the challenge remains unsolved due to the difficulty in identifying discrimina-tive and computationally affordable traits for spoofing attacks. Further-more, previous liveness detection techniques are not particularly oriented towards mobile biometrics, making them mostly unsuitable for portable devices. As a solution, we created a software-based multi-biometric pro-totype that detects face, iris, and fingerprint spoofing attacks on mo-bile devices. We present Mobile Biometric Liveness Detection techniques (MBLDT). Apart from the fact that conventional mobile devices perform badly for floating point applications, MBLDT is computed in linear time with respect to the amount of pixels and does not require floating point computation. As a result, our technique is solely simple, quick, and ef-ficient, making it ideal for mobile devices. Furthermore, unlike previous approaches, our method effectively detects liveness using the same lone image descriptor technique for three biometric features, namely face, iris, and fingerprint. Furthermore, our system detects liveness using only one image, which can also be used for recognition. Experiments with real spoofing attacks on widely available face, iris, and fingerprint data sets have yielded encouraging results.

Citation: ***Joshua Teddy Ibibo.*** **2023.** "Liveness detection techniques in user authentication on iot devices", *Asian Journal of Science and Technology*, 14, (08), 12613-12617.

INTRODUCTION

Mobile devices with built-in sensors such as cameras have grown widespread in recent years, and they are now widely used worldwide not just for basic communications but also as a tool to access and manage personal information and data via biometrics. Biometrics is a natural alternative to standard access control methods such as passwords that uses the user's biological or behavioural features. The iPhone 13, Samsung, Huawei and LG, for example, have a touch sensor that recognises the user's fingerprint and unlocks the phone automatically. Additionally, the Android 12 mobile operating system, as well as Hp, Dell, and Sony laptops, include embedded biometric systems that verify users based on individual features [1]. While considerable attempts are already being conducted to boost the ef-fectiveness of biometrics on mobile devices, the issue of their vulnerability to spoofing attacks is often disregarded [2]. A spoofing attack happens when an impostor attempts to masquerade as a genuine user by mimicking the genuine user's biometrics and so acquiring illegitimate access and advantages [3]. For-malized paraphrase For example, In 2021, a Russian hacker uses free or low-cost means to spoof iProov, a UK-based worldwide technology provider, and other IT organisations such as BioID, Shufti Pro, and SumSub [4]. The German hacker group Chaos Computer Club demonstrated in 2013 that the fingerprint scanner in Apple's iPhone 5s can be fooled by an artificial fingerprint, while at the Black Hat 2009 conference, a research team from the University of Hanoi (Vietnam) demonstrated how easily they can spoof facial images of legitimate users and bypass Lenovo, Asus, and Toshiba laptops' Face Recognition, providing admin rights to personal computers.

Fig. 1. Images of a real face, iris, and fingerprint (top row) and spoofing attacks (bot-tom row): Photo attacks on the face, the iris, and the fingerprint (from left to right) [1]

Although spoofing attacks do not require sophisticated technical capabilities, they have a wide number of potential attackers. The success of these attacks is based on the inability of biometric sensors to distinguish between 'fake/spoofed' and 'real' biometric traits. Furthermore, it is common knowledge that as the use of biometric systems grows, so does the number of attempts to deceive them. As a result, addressing biometric spoofing attacks on mobile devices is

critical in order to improve system security and robustness, allowing biometric applications to become more widely used. Liveness detection technique [5–7] has been proposed as a conventional countermeasure against spoofing attacks, with the goal of determining if the provided biometric feature is live or artificial by watching physiological indications of life such as eye blinking, precipitation, and so on. The identification of liveness is carried out by either a software module based on signal processing or a hardware module incorporated in the input device itself. Because they do not need any additional and potentially invasive measurements such as blood pressure, etc., software-based solutions are the most interesting and demanding. As a result, this work focuses on software-based systems as well. So far, different countermeasures have been offered in the research, but none of them have demonstrated the ability to achieve very low error rates. Further-more, existing approaches are primarily trait dependent, hence feature descrip-tors established for face spoofing may not be effective when utilised for iris or fingerprint spoofing, and vice versa. Similarly, because they utilise complicated features and/or have a large processing cost, most of the approaches are not suitable for real-time or mobile applications. To the best of our knowledge, no liveness detection work has been specifically addressed for mobile applications. As a result, technique recommendations to protect biometric applications on mobile devices are needed and welcome. From the abovementioned considerations, we present a novel software-based liveness detection technique, the Mobile Biometric Liveness Detection techniques (MBLDT) that can be employed in a variety of biometric systems on mobile de-vices. MBLDT is a revolutionary technique to real-time picture feature descrip-tion that is simple, fast, and based on linear temporal permutation achieved by sorting the RGB values of image patches. MBLDT does not necessitate the use of floating point computing, which is an advantageous feature for mobile CPUs. Because MBLDT is immune to monotonic photometric alterations and noise, we believe it could be beneficial in distinguishing between a live and a fake characteristic due to information loss during the spoofing attack development. For face, iris, and fingerprint spoof detection, we propose using image de-scriptor classification techniques Locally Uniform Comparison Image Descriptor (LUCID) [8], Census Transform Histogram (CENTRIST) [9], and Patterns of Oriented Edge Magnitudes (POEM) [10].

Contribution

The presented techniques leverages MBLDT to analyse local features in face, fingerprint, and iris images and encodes local patterns into an augmented feature vector. The data are then sent into a Support Vector Machine classifier, which identifies whether or not the input biometric feature is from a living person. Experiments with publicly available data sets containing a variety of actual and artificial faces, irises, and fingerprints yield encouraging results.The following is a breakdown of the paper's structure.

- The study on face, fingerprint, and iris spoofing and anti-spoofing is sum-marised in Section II
- Section III explains the proposed technique.
- Section IV provides the data sets, experimental technique, and results.
- In Section V, preliminary conclusions are drawn.

Background and Related Work: For a long time, biometric systems have been shown to be vulnerable to spoofing attacks [3, 9, 10]. In this detailed outline, we provide an overview of face, iris, and fingerprint spoofing, as well as liveness detection techniques. Iris Spoofing The most accurate technique is generally agreed to be iris recog-nition. An iris photo/video/printed contact lens of a legitimate user, on the other hand, may fool iris identification systems. Until date, liveness detection techniques based on physiological activities or optical features of live eyes, such as those presented in [11], have been proposed. The forgeries can be detected by detecting pupil and eye movement due to involuntary reactions to changes in il-lumination [12]. A comparison of state-of-the-art iris liveness detection methods in [11] reveals that none of them achieves an acceptable error rate and process-ing cost. Frequency spectrum model, reflectance model, dynamics model, and texture model are the four basic categories of iris liveness detection techniques.

Frequency spectrum model: The liveness detection techniques make use of frequency spectrum infordatmation, assuming the presence of artefacts in spoofing attack photos. Daugman et al. [13] and Ma et al. [14] proposed using spectrographic analysis based on Fast Fourier Transform to detect the printed iris. However, due to Shanon's theory, these methods have some major limitations. For example, they fail if the resolution of the printing in-strument used for counterfeit manufacture is greater than double that of the biometric picture acquisition camera. Furthermore, if the supplied counter-feit iris image is purposefully defocused and unfocused, the spoofed iris may be recognised as a real one. He et al. [15] developed a method for analysing statistical features of 2-D Fourier spectra as well as assessing iris image qual-ity.

Reflectance model: This technique entails lighting the eye with diverse wavelengths of light and evaluating the relative reaction in the sclera and iris regions. Lee et al. [16] proposed utilising the theoretical reflectance model to detect live and fake irises based on reflectance characteristics.

Dynamics model: To check for a change in pupil dilation, dynamics model techniques acquire many photos while adjusting the lighting thresholds. Pa-cut et al. [17] developed a composite iris liveness recognition approach that takes into account transient eye properties such pupil dynamics, image fre-quency spectrum, and controlled light reflection from the cornea.

Texture model: In order to discover iris spoofing attacks, texture model techniques evaluate and classify image texture characteristics. Based on the human eye model, Lee et al. [18] suggested a new approach for detecting fake iris by estimating the theoretical locations and distances between the Purkinje images (using collimated IR-LED). Wei et al. [19] proposed a system to detect false iris using IrisTextons (i.e. texture representation). Tan et al. [20] used Adaboost and multi-scale local binary pattern texture features to learn efficient spoof detection. This method, however, necessitates the detection of samples of contact lens patterns as part of its training data. He et al. [21] demonstrated how to detect spoof contact lenses using a grey level co-occurrence matrix and statistical texture analysis. This technique fails for contact lenses and necessitates the use of supplementary technology, a series of iris photographs, and the user's full cooperation.

Fingerprint Spoofing The practise of spoofing fingerprints is extremely an-cient [22]. A 2-D and 3-D imitation finger of a genuine user, manufactured with or without the participation of the person, can trick a fingerprint recognition system. By studying perspiration and pores patterns with wavelet, Abhyankar et al. [22] devised a time-consuming approach for detecting false fingerprints. The Thin-plate Spline model was used by Zhang et al. [23] to construct a skin elasticity-based approach for capturing finger distortion. The biggest disadvan-tage of this method is that it requires special training for users. According on the above research investigation, the majority of existing live-ness detection techniques for face, iris, and fingerprints are either quite sophis-ticated or use non-traditional imaging methods of mobile devices. Furthermore, existing systems often work well just against the attacks of the unique trait for which they were intended, but not against attacks of additional traits. For example, an image descriptor designed for iris spoofing may or may not work for face or fingerprint spoofing, and vice versa. As a result, we offer three al-gorithms for face, iris, and fingerprint liveness detection in this study, each of which is relatively simple, computationally fast, and employs standard photos while requiring no user cooperation. Face Spoofing Face spoofing remains a critical challenge to existing face recog-nition systems, despite significant advances. A photo/video/3D face model of a real user could be used to fake them. Liveness detection

techniques is a common countermeasure against face spoofing that seeks to identify physiological indica-tors such as eye blinking. Pan et al. [24], for example, provided an undirected conditional random field framework for liveness identification based on ocular blinks. For higher-quality video spoof samples, the procedure is likely to fail. The majority of known liveness detection techniques are either extremely sophisti-cated or rely on non-traditional photographic mechanisms. Premised on the cues exploited for spoofing detection techniques, conventional countermeasures, such as face liveness detection, can be crudely categorised into several subsets: motion study and texture study.

Motion study: When two-dimensional generics, such as images or movies, are provided to the system, methods attempt to discover spontaneous move-ment hints. Pan et al. [24], for example, took use of the fact that human eyes blink once every 2-4 seconds and suggested a photo-spoofing technique based on an undirected conditional random field framework to represent eye-blinking.

Texture study: The premise is that the surface properties of real faces and prints, such as colors, are distinct, hence liveness detection algorithms look at skin properties like texture and reflectivity. Printing failures or blurring are examples of observable texture patterns caused by artefacts. By leverag-ing discrepancies in the 2-D Fourier spectra of live and spoof photos, Li et al. [25] presented a method for print-attack face spoofing. Only downsam-pled photos of the attacked identity function effectively with the procedure; higher-quality samples are likely to fail.

Related Work

We present a summary of face, iris, and fingerprint spoofing, with their liveness detection methods, in this brief survey.

- Galbally et. al [26] proposed anti-spoofing approach is evaluated on a database of over 1,600 actual and fake (high quality printed photographs) iris samples, demonstrating that it has a great potential for use as a direct attack protection mechanism.
- Galbally et. al [27] use of an unique fingerprint parameterization based on quality related characteristics is offered as a new software-based liveness detec-tion technique.
- Using multi-scale local phase quantity (LPQ) and principal component anal-ysis (PCA), a new software-based liveness detection technique is proposed in [28]
- When attackers utilise printed lenses, however, these techniques fail. As a marker of liveness, Daugman recommended looking at corneal, retinal, and purk-inje reflections [29]. These techniques, unfortunately, failed when an impostor examines a printed iris image with a cutoff hole in the pupil area [4].
- Park et al. [12] used fused multispectral iris pictures to identify liveness. This method, however, necessitates the use of forged irises throughout the enrolling process.
- Galbally et al. [30] combined picture quality qualities generated by either iris or sensor motion with motion features.
- A comparison of state-of-the-art iris liveness detection methods in [17] reveals that none of the methods achieves an acceptable error rate and processing cost. As a result, new iris liveness detecting algorithms must be developed.
- For liveness identification, Ghiani et al. [31] took advantage of local phase quantization properties. Galbally et al. [32] provided an approach that included ten separate quality criteria, including ridge strength, ridge regularity, and ridge visibility.
- For texture-based liveness identification, Marcel et al. [33] used a local binary pattern descriptor. To distinguish between faked and live faces, the techniques in [34] and [35] used Lambertian and Retinex reflectance models, respectively.
- Kollreider et al. [36] created a liveness detection method based on a brief sequence of photos and a binary detector that captures and tracks the modest movements of various facial components using a simplified optical flow analysis and a dynamic predictor.
- Tan et al. [37] used a Lambertian reflectance model with difference-of-Gaussians (DoG) to determine the variations in motion deformation patterns between 2-D face photographs and 3-D live faces throughout spoofing attacks.

METHODOLOGY

However photographs obtained from spoof attacks may appear to be extremely similar to images captured from live people (see Fig. 1), a closer examination reveals that spoof attack images contain some specific artefacts. Consequently, inspired by image quality assessment and artefact characterisation, we offer a unique software-based multi-biometric technique that may be applied in mobile and real-time applications. In specifically, we construct a face, iris, and finger-print representation capable of capturing distinguishing aspects of actual and false face, iris, and fingerprint images. Using the MBLDT, our system learns the subtle distinctions between photos of actual and fake faces, irises, and fin-gerprints [8]. MBLDT is a revolutionary technique to feature description based on order permutations that can be computed in linear time with respect to the amount of pixels and does not require floating point computing, despite the fact that conventional mobile devices perform badly for floating point ap-plications. Furthermore, MBLDT is a remarkably simple and efficient feature creation method that implicitly encapsulates all possible intensity comparisons in an image's local area.

Experiment

We present an experimental analysis of the hypothesized liveness detection tech-nique for face, iris, and fingerprint biometrics in this part. Data sets We used existing datasets because there are no publicly available spoofing attack datasets obtained using mobile devices.

Iris Spoofing: DB ATVS-FIr [38]. This is also a widely published informa-tion data set including 50 people x 2 eyes x 4 pictures x 2 sessions = 800 fraudulent iris images and genuine data obtained with the Samsung galaxy tab. Both eyes of the same individual are considered as independent individ-uals in the tests (i.e., 50 x 2 = 100 users).

Fingerprint Spoofing: ATVS-FFp DB [39] is a database that contains information about ATVS-FFp. The pointer and ring finger of both palms of 17 individuals (17 x 4 = 68 different fingers) are included in this database, which is also open to the general populace. Two spoofs were created using silicon for each real finger using two different processes (with and without the user's involvement). In one acquisition session, three sensors recorded four samples of each fingerprint. As a result, for each method, the database contains 68 fingerprints x 4 specimens x 3 sensors = 816 true picture samples and the same number of faked photos.

Face Spoofing: We used five datasets that were freely published online. Replay Attack It is made up of 1300 video clips of photo and video at-tacks on 50 clients in various lighting circumstances. We extracted 'live' and 'spoofed' face photos from the relevant films of the Print Attack and Replay Attack databases since we need to operate on images. We retrieved 20 'live' and 20'spoofed' face photos from each video clip for each client [40]. Personal Photo Attack We took 'actual' face photos of 40 clients in two encounters, each with a distinct representation on their face. We next used the 'photo attack' method outlined in [41] to construct the faked facial pho-tos. It entails projecting a snapshot of the targeted client onto a laptop screen, which is then placed in front of the camera. We used personal images of the clients in the live face data set that we found on the Internet, such as social networks. We collected 5 photographs on aggregate from each user.

Print Attack: The dataset comprises of 200 video recordings of printed-photo attack attempts made on 50 people using separate illumination situ-ations, as well as 200 real-access attempted made on the same individuals [40].

Table 1. Comparison of productivity (Half Total Error Rate (HTER)-percent) be-tween the proposed technique and other existing iris [13], face [29], and fingerprint [26] approaches for differentiating live from false face, iris, and fingerprint images

Data Set	Proposed Technique	Older Technique
Iris (ATVS)	1.03±0.34	4.66±1.15
Face (Print Attack)	2.88±0.88	4.54±1.35
Face (NUAA)	1.54±0.16	0.54±0.10
Face (Yale Recaptured)	1.90±0.20	0.80±0.11
Face (Replay Attack)	5.46±0.55	7.30±3.61
Fingerprint (ATVS)	7.17±1.97	14.22±4.10

RESULTS AND DISCUSSIONS

The performance of the proposed liveness detection technique, as well as known approaches for face, iris, and fingerprint biometrics, is reported in Table I. Ta-ble I shows that the suggested method has a lot of promise as a simple, rapid, and new way for detecting spoofing attacks with good classification accuracy for various biometric features. In addition, for all data sets except Yale and NUAA, the new technique outperformed existing schemes. While it may be feasible to identify face, iris, and fingerprint spoofing attacks from a digital object, but it also appears to deliver encouraging liveness detection performance for all three methods, namely face, iris, and fingerprint, in contrast to the state-of-the-art, presented individual image feature descriptor. Similarly, the average time re-quired for feature extraction in the suggested strategy is significantly smaller than that in previous methods. Across all data sets, the MBLDT descriptor scored best on average for iris liveness detection. On the Notre Dame database, for example, the HTER is 0.07 percent, even though the phoney samples used are high-quality faked contact lenses. The approach in [30], on the other hand, produced 1.64 percent HTER by combining two focus (IQF15 and IQF16), two occlusion (IQF3 and IQF19), and one pupil dilation (IQF22) characteristics. The HTERs of suggested method and reflectance analysis based methodology in [35] for face spoof detection on NUAA data set are 1.54. A notable distinction among both a real and spoofed face in the actual world is that spoofs can contain glossy rays due to lighting. Spoof artefacts can also be plainly seen locally, such as on a homogeneous surface such as the cheek. Because the order permutation is invariant to monotonic intensity modifications, LUCID performs better for the face and iris than a phoney fingerprints. To summarise, the findings show that the feature descriptor utilised is ex-tremely simple, quick, and effective, making it ideal for real-time or mobile de-vices. The computational load is reduced since the approach does not use any trait-specific properties. Furthermore, unlike previous techniques, we propose to use only one image descriptor to achieve high accuracy for three biometric traits: face, iris, and fingerprint, as well as liveness detection. Furthermore, our system detects liveness using only one image, which can potentially been exploited in biometric identification.

Conclusion and Future Work

We recommended a technology liveness detection technique that may be applied to a variety of biometric devices. We developed a method for detecting face, iris, and fingerprint spoofing attacks in mobile apps using a novel real-time feature description based on order permutations called the MBLDT. The feature descrip-tion is designed to be simple, quick, and effective, making it ideal for real-time and mobile applications. Apart from the fact that conventional mobile devices perform badly for floating point applications, MBLDT may be computed in lin-ear time with respect to the amount of pixels. Furthermore, contrary existing methods, our method uses a single picture descriptor to effectively detect live-ness in three modalities: face, iris, and fingerprint. The findings of experiments using widely available data sets and real spoofing assaults were impressive. We intuitively believe that the inherent characteristics of spoofing attack im-ages captured by biometric sensors may be analogues for image-based biometric authentication, so there is a need for a generic image feature-based liveness de-tection system that can detect all traits' spoofing attacks, regardless of which biometric trait images they are trained on. A countermeasure designed for face spoofing, for example, should also work for iris or fingerprint spoofing, and vice versa. The work reported in this paper is a first step toward achieving this goal.

REFERENCES

1. Z. Akhtar, C. Michelon, and G. L. Foresti, "Liveness detection for biometric au-thentication in mobile applications," in 2014 International Carnahan Conference on Security Technology (ICCST). IEEE, 2014, pp. 1–6.
2. J. Komulainen, A. Hadid, and M. Pietik¨ainen, "Face spoofing detection using dy-namic texture," in Asian Conference on Computer Vision. Springer, 2012, pp. 146–157.
3. Z. Akhtar, "Security of multimodal biometric systems against spoof attacks," De-partment of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, vol. 6, 2012.
4. "Liveness.com," https://liveness.com/#free, 2021, 16th January 2022.
5. J. Galbally and M. Gomez-Barrero, "A review of iris anti-spoofing," in 2016 4th international conference on biometrics and forensics (IWBF). IEEE, 2016, pp. 1–6.
6. A. Rattani and A. Ross, "Minimizing the impact of spoof fabrication material on fingerprint liveness detector," in 2014 IEEE International Conference on Image Processing (ICIP). IEEE, 2014, pp. 4992–4996.
7. Z. Akhtar, C. Micheloni, C. Piciarelli, and G. L. Foresti, "Mobio livdet: Mobile biometric liveness detection," in 2014 11th IEEE International Conference on Ad-vanced Video and Signal Based Surveillance (AVSS). IEEE, 2014, pp. 187–192.
8. A. Ziegler, E. Christiansen, D. Kriegman, and S. Belongie, "Locally uniform com-parison image descriptor," Advances in Neural Information Processing Systems, vol. 25, pp. 1–9, 2012.
9. J. Daugman, "Demodulation by complex-valued wavelets for stochastic pattern recognition," International Journal of Wavelets, Multiresolution and Information Processing, vol. 1, no. 01, pp. 1–17, 2003.
10. S. T. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. Schuckers, "Time-series detection of perspiration as a liveness test in fingerprint devices," IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Re-views), vol. 35, no. 3, pp. 335–343, 2005.
11. J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in 2012 5th IAPR International Conference on Biometrics (ICB). IEEE, 2012, pp. 271–276.
12. J. H. Park and M.-G. Kang, "Multispectral iris authentication system against counterfeit attack using gradient-based image fusion," Optical Engineering, vol. 46, no. 11, p. 117003, 2007.
13. J. Daugman, "Demodulation by complex-valued wavelets for stochastic pattern recognition," International Journal of Wavelets, Multiresolution and Information Processing, vol. 1, no. 01, pp. 1–17, 2003.
14. L. Ma, T. Tan, Y. Wang, and D. Zhang, "Personal identification based on iris texture analysis," IEEE transactions on pattern analysis and machine intelligence, vol. 25, no. 12, pp. 1519–1533, 2003.

pp. X. He, Y. Lu, and P. Shi, "A fake iris detection method based on fft and quality assessment," in 2008 Chinese Conference on Pattern Recognition. IEEE, 2008, 1–4.

qq. S. Lee, K. R. Park, and J. Kim, "A study on fake iris detection based on the reflectance of the iris to the sclera for iris recognition," in ITC-CSCC: International Technical Conference on Circuits Systems, Computers and Communications, 2005, 1555–1556.

17. A. Pacut and A. Czajka, "Aliveness detection for iris biometrics," in Proceedings 40th annual 2006 international carnahan conference on security technology. IEEE, 2006, pp. 122–129.
18. E. C. Lee, K. R. Park, and J. Kim, "Fake iris detection by using purkinje image," in International Conference on Biometrics. Springer, 2006, pp. 397–403.
19. M. Li, Z. Zhang, K. Huang, and T. Tan, "Estimating the number of people in crowded scenes by mid based foreground segmentation and head-shoulder detec-tion," in 2008 19th international conference on pattern recognition. IEEE, 2008, pp. 1–4.
20. Z. He, Z. Sun, T. Tan, and Z. Wei, "Efficient iris spoof detection via boosted local binary patterns," in International conference on biometrics. Springer, 2009, pp. 1080–1090.
21. X. He, S. An, and P. Shi, "Statistical texture analysis-based approach for fake iris detection using support vector machines," in International conference on biomet-rics. Springer, 2007, pp. 540–546.
22. A. Abhyankar and S. Schuckers, "Integrating a wavelet based perspiration liveness check with fingerprint recognition," Pattern Recognition, vol. 42, no. 3, pp. 452– 464, 2009.
23. Y. Zhang, J. Tian, X. Chen, X. Yang, and P. Shi, "Fake finger detection based on thin-plate spline distortion model," in International Conference on Biometrics. Springer, 2007, pp. 742–749.
24. G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recog-nition from a generic webcamera," in 2007 IEEE 11th international conference on computer vision. IEEE, 2007, pp. 1–8.
25. J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of fourier spectra," in Biometric technology for human identification, vol. 5404. International Society for Optics and Photonics, 2004, pp. 296–303.
26. J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in 2012 5th IAPR International Conference on Biometrics (ICB), 2012, pp. 271–276.
27. J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega- Garcia, "A high performance fingerprint liveness detection method based on quality related features," Future Generation Computer Sys-tems, vol. 28, no. 1, pp. 311–321, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X1000244X
28. C. Yuan, X. Sun, and R. Lv, "Fingerprint liveness detection based on multi-scale lpq and pca," China Communications, vol. 13, no. 7, pp. 60–65, 2016.
29. J. Daugman, "Recognizing persons by their iris patterns, ak jain, r. bolle, s. pankanti (eds.): Biometrics: Personal identification in networked society," 1999.
30. J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in 2012 5th IAPR International Conference on Biometrics (ICB). IEEE, 2012, pp. 271–276.
31. L. Ghiani, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection by local phase quantization," in Proceedings of the 21st international conference on pattern recognition (ICPR2012). IEEE, 2012, pp. 537–540.
32. J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high per-formance fingerprint liveness detection method based on quality related features," Future Generation Computer Systems, vol. 28, no. 1, pp. 311–321, 2012.
33. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary pat-terns in face anti-spoofing," in 2012 BIOSIG-proceedings of the international con-ference of biometrics special interest group (BIOSIG). IEEE, 2012, pp. 1–7.
34. X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in European Conference on Computer Vision. Springer, 2010, pp. 504–517.
35. N. Kose and J.-L. Dugelay, "Reflectance analysis based countermeasure technique to detect face mask attacks," in 2013 18th International Conference on Digital Signal Processing (DSP). IEEE, 2013, pp. 1–6.
36. K. Kollreider, H. Fronthaler, and J. Bigun, "Non-intrusive liveness detection by face images," Image and Vision Computing, vol. 27, no. 3, pp. 233–244, 2009.
37. X. Tan, Y. Li, J. Liu, and L. Jiang, "Face liveness detection from a single image with sparse low rank bilinear discriminative model," in European Conference on Computer Vision. Springer, 2010, pp. 504–517.
38. G. Pan, L. Sun, Z. Wu, and Y. Wang, "Monocular camera-based face liveness detection by combining eyeblink and scene context," Telecommunication Systems, vol. 47, no. 3, pp. 215–225, 2011.
39. J. Bai, T.-T. Ng, X. Gao, and Y.-Q. Shi, "Is physics-based liveness detection truly possible with a single image?" in Proceedings of 2010 IEEE International Sympo-sium on Circuits and Systems. IEEE, 2010, pp. 3425–3428.
40. I. Chingovska, A. Anjos, and S. Marcel, "On the effectiveness of local binary pat-terns in face anti-spoofing," in 2012 BIOSIG-proceedings of the international con-ference of biometrics special interest group (BIOSIG). IEEE, 2012, pp. 1–7.
41. B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad il-lumination conditions," in 2011 18th IEEE International Conference on Image Processing. IEEE, 2011, pp. 3557–3560.

****