SN Computer Science (2021) 2:49
https://doi.org/10.1007/s42979-020-00425-3

SURVEY ARTICLE

A Contemporary Survey of Multimodal Presentation Attack Detection Techniques: Challenges and Opportunities

Kavita[1] · Gurjit Singh Walia[2] · Rajesh Rohilla[1]

Received: 22 November 2020 / Accepted: 10 December 2020 / Published online: 20 January 2021

Abstract
Biometric recognition is a broad and dynamic field of research but the main problem of this field is spoofing attack or presentation attack "use of fake biometric in place of the real biometric sample from original user". Liveness detection is the prime countermeasure to spoofing attacks, which is based on the principle that some additional information can be obtained to verify that the produced data is genuine or not by a standard verification system. It utilized anatomical signs of life, such as facial expression, blinking of eyes, movement of the head, etc. This paper presents a comprehensive review of various liveness detection techniques based on a multimodal biometric system, in which physiological and behavioral properties are used to differentiate between genuine and fake biometric traits. Multimodal systems utilize two or more biometric traits which makes them more secure as compared to unimodal systems. These systems overcome the limitations of the unimodal system such as spoof attack, noisy data, non-universality, distinctiveness, and intra-class variations, etc. Hence to make the biometric systems more secure and robust, multimodal techniques are used. In this paper, we categorized and discuss the various multimodal biometric techniques proposed by various researchers in the last decade, and a new classification is also developed for the same. This paper covers theories, methodology, evaluation datasets, and aims at future work in this field of research.

Keywords Spoofing-attacks · Liveness detection · Unimodal biometric · Multimodal biometric

Introduction

Biometrics is taken from the Greek word in which "bio" refers to the "life" and "metric" refers to the "measure", which tries to identify or to verify individuals based on physiological characteristics (e.g., face, fingerprint, iris) or behavioral characteristics (e.g., signature, voice, gait). Presently, the biometric recognition system is widely used in many security systems but presentation attack or spoofing attack "use of fake biometric in place of the real biometric sample from original user" is still the main issue for these systems. However various methods exist to find out that the person available in front of the biometric sensor is an artifact or live but the problem of spoofing attacks is remained [1]. There are mainly two types of attacks that take place in a biometric recognition system, one is, direct attack and another indirect attack. Direct attacks take place at the biometric sensor level (Fig. 1, Point1) and these attacks are made on the biometric system by representing the human characteristics or an artifact in front of the biometric capture subsystem. The attacks, which are performed inside the system by invaders, are known as indirect attacks. These attacks are made by escaping the feature extractor (Fig. 1, point 3) or matcher (Fig. 1, point 5), in the database by manipulating templates (Fig. 1, point 6), and in the communication channels by exploiting possible weak points (Fig. 1, points 2, 4, 7, and 8) [2]. The figure shows the possible attack point's in the general biometric system.

This article is part of the topical collection "Advances in Computational Approaches for Artificial Intelligence, Image Processing, IoT and Cloud Applications" guest edited by Bhanu Prakash K N and M. Shivakumar.

✉ Kavita
kavbit.207@gmail.com

Gurjit Singh Walia
gurjit.walia@gmail.com

Rajesh Rohilla
rajesh@dce.ac.in

[1] Delhi Technological University, Delhi, India

[2] SAG, DRDO, New Delhi, India

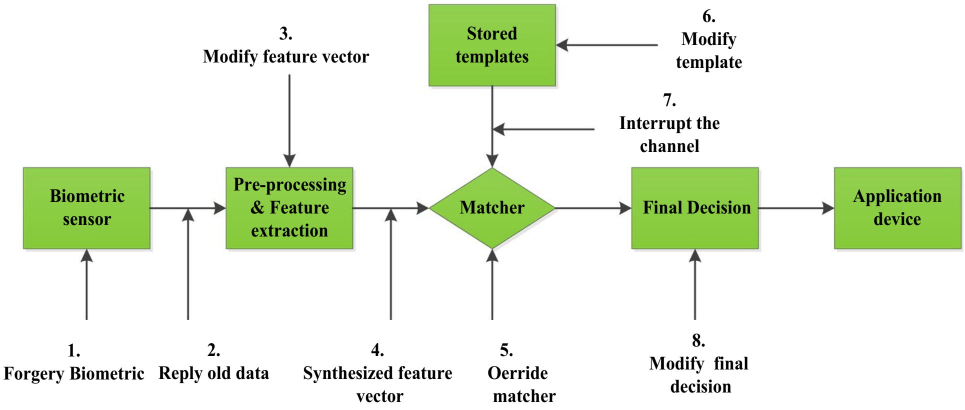

Fig. 1 Attack points in the general biometric system [2]

Liveness detection is also known as Presentation attack detection, is the prime countermeasure to spoofing attacks, which is based on the principle that some additional information can be obtained to verify that the produced data is genuine or not by a standard verification system. Some examples of liveness detection are facial expressions, blinking of eyes, movement of the head, blood pressure, and electrical heart signals (ECG), brain wave (EEG), etc. [3]. In this review, we discuss the various liveness detection techniques based on a multimodal biometric system. In a unimodal system, only a single trait (e.g. face, iris, etc.) is used which can be spoofed easily and therefore it has the following limitations: distinctiveness, spoof attack, noisy data, intra-class variations, non-universality, etc. The multimodal system utilized two or more biometric traits (such as face and iris, face and fingerprint, face, fingerprint, and iris, of a person) which make it more secure and robust as compared to the unimodal system against the spoofing attack. Also, these systems overcome the limitations of the unimodal system.

In this survey paper, various liveness detection techniques based on the multimodal biometric system are discussed, for user authentication. This survey is organized as follows: "Introduction" gives the formal introduction to liveness detection techniques followed by the proposed classification in "Proposed classification of presentation attack detection techniques based on multimodal biometric system", the different methods proposed are presented as: multiple traits in "Multiple traits", multiple sensors in "Multiple sensors", multiple representations in "Multiple representations", behavioral techniques in "Behavioral techniques", and image quality based techniques in "Image quality based techniques". Lastly, concluding remarks are mentioned in "Conclusion".

Proposed Classification of Presentation Attack Detection Techniques Based on Multimodal Biometric System

Nowadays to increase the performance of biometric systems and to make them more secure against spoofing or presentation attacks, multimodal systems are considered better than the unimodal biometric system (Fig. 2).

The main limitations of the unimodal system are spoof attacks, noisy data, distinctiveness, intra-class variations, and non-universality which can be overcome by a multimodal system. Also, apart from the liveness detection, these systems provide better security against spoof attacks as compared to the unimodal system. In [4] a prototype design was proposed for a multimodal biometrics system in which ring fingerprints and left/right index, left/right near-infra-red dorsal hand vein patterns, etc. were taken. The main advantage of adding these modalities was in liveness detection. In [5] two novel approaches were proposed, in which one was the extension of likelihood ratio-based fusion and the second was the use of fuzzy logic against spoofing attacks. In this work impact of spoofing attacks was analyzed on the multimodal biometric systems and it was observed that this scheme was more robust against the spoofing attacks as compared to the likelihood ratio and weighted sum. Jiang et al. [6] have been proposed a video-based multimodal biometric approach that utilized face and speech fusion in the Laplacian subspace for speaker recognition. Fusion using the presented approach achieved better accuracy as compared to the single face or audio modality. Barrero et al. [7] presented the software-based

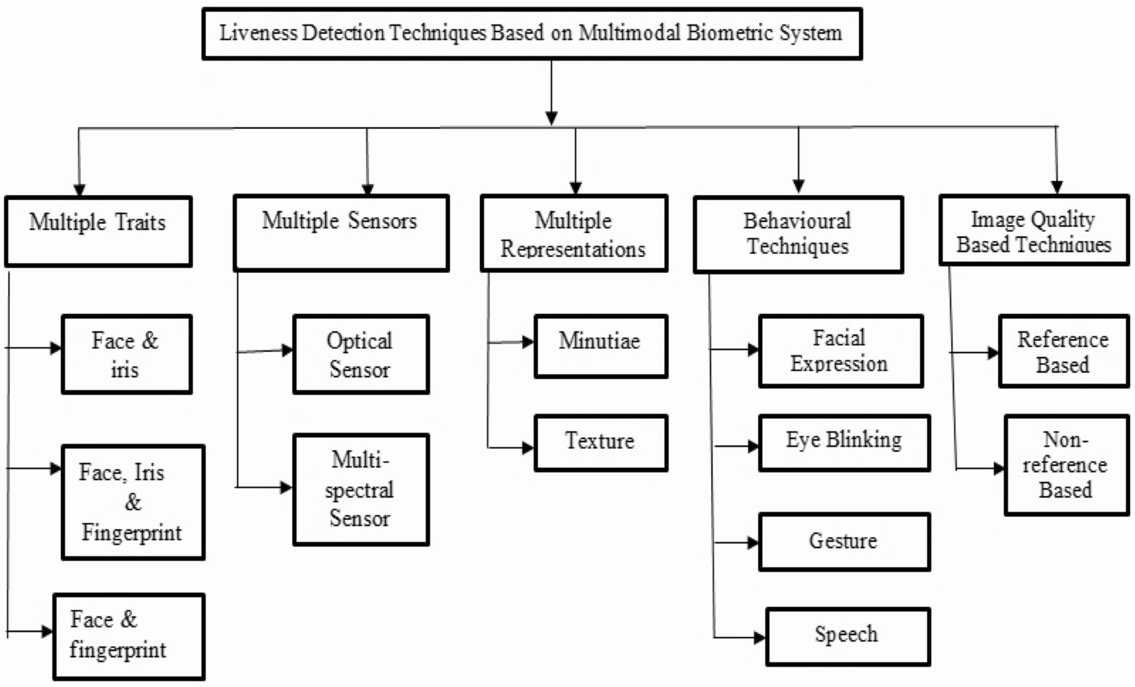

Fig. 2 Proposed classification for presentation attack detection techniques based on the multimodal biometric system

attack against multimodal systems in which face and iris were used to check the performance. Das et al. [8] proposed a structure for software-based liveness detection in multimodal ocular biometrics. The proposed scheme is utilized for direct attack detection. The authors also include class level liveness detection in their work. Kavitha et al. [9] proposed a multimodal biometric framework that utilized feature level fusion to fuse the extracted features and support vector machine (SVM) classifier to detect the fake face.

Multiple Traits

In this method, two or more biometric characteristics such as face and iris, face, fingerprint, and iris, etc. are used to know about liveness. To make the system more robust multiple traits are used, as a single trait can be spoofed easily. In [10] a multimodal system that overcomes the limitations of a unimodal system was proposed. The authors utilized fingerprint, face, and speech for the identification of the user. For the fingerprint and speech verification, they used the minutiae matching algorithm and left to right hidden Markov model respectively. To recognize the face the author's utilized used Eigen face-based method. Komeili et al. [11] proposed a framework that utilized ECG and fingerprint for user authentication as well as liveness detection. Also, a criterion was proposed based on the averaging and correlation that evaluate heartbeat consistency. In [12] a multimodal biometric system was presented based on optimal score level fusion that can differentiate between real and fake subjects. To optimize the performance of the system backtracking search optimization algorithm was used. Chetty and Wagner [13] proposed a multilevel liveness verification framework based on multimodal fusion and feature extraction for a secure face-voice biometric authentication system. In this framework, face information was obtained from speaking faces. Akhtar et al. [14] have been proposed a mobile biometric liveness detection (MoBio LivDet) method for analyzing the structures of the face, fingerprint, and iris images by utilizing decision level fusion and feature descriptors. In [15] optimized score level fusion was presented that utilized a grasshopper optimization algorithm to enhance the performance of the multimodal biometric system. The proposed system shows high performance and reliability, and robustness against the dynamic environment.

Multiple Sensors

In these various sensors are used on one biometric trait to know the liveness of the system. Wei Bao et al. [16] have proposed an optical flow field method to recognize and find out the liveness of the face.The main limitation of this method was the assumption that fake face will be on a plane. Sahidullah et al. [17] proposed a throat microphone and body-conducted sensor for automatic speaker verification, liveness detection, and enhance security against a replay attack. In [18] an RF sensor-based liveness detection approach was proposed for the capacitive fingerprint system. In [19] a study was presented to assess the liveness detection of 3D cameras. The authors presented a system that utilized Kinect sensor for testing and comparing the effectiveness of depth data in spoof detection. Also, to recognize the faces that appear on the screen Haar Cascade algorithm was used. Wang et al. [20] presented a theoretical model to present the relationship between the oral airflow pressure and the characters in users' speech. The airflow sensor is used to measure the consistency between the actual and estimated pressure signals to determine whether the given command is live or artificial (Table 1).

Multiple Representations

It utilized a representation of minutiae points and image texture to detect the liveness. In [21], the authors presented an approach based on texture analysis for iris recognition in which spatial filters are utilized for differentiating the texture features. In [22] a method based on the extraction of multiple features from multispectral images was presented for iris liveness detection. This method provides high accuracy of classification between fake iris and live iris. Parveen et al. [23] have been proposed a dynamic local ternary pattern that removes the manual threshold setting in local Ternary pattern by utilizing Weber's law. Also, the comparison between the dynamic local ternary pattern and the local ternary pattern was performed. Boulkenafet et al. [24] utilize the color texture analysis approach for face spoofing detection. The authors utilized joint color texture information obtained from the chrominance and luminance channels. The information is obtained from different color spaces by extracting complementary low-level feature descriptors. Agarwal et al. [25] proposed a method for liveness detection in which spatial analysis of the fingerprint pattern and statistical texture features were used to differentiate between fake and real images. For the effectiveness of the method, the authors also used the fusion of fingerprint and texture features of iris. Dempster–Shafer approach was used for the fusion at the decision level.

Behavioral Techniques

In a multimodal system, behavior includes the movement of the face, hand, eyes blinking, voice, etc. and by making the use of these traits liveness is identified. Sun et al. [26] have been proposed a Conditional Random Fields (CRFs) method to detect the liveness of the face for which they utilized blinking of eyes. They also compare the CRFs model with the cascaded Adaboost and Hidden Markov (HM) model, which provides better results as compared to these models. Zhao et al. [27] proposed an approach to recognize the dynamic texture. To deal with the dynamic events, for example, facial expression, a block-based method was developed. Also, the authors have been developed a volume local binary pattern (VLBP) to combine motion and appearance. In [28] a face live detection method that utilized physiological motion was proposed. The authors utilized a conventional active shape structure to recognize the local appearance around each landmark. In [29] a fuzzy fusion approach was presented for liveness detection that was based on mutual dependency models. These models extract the Spatio-temporal correlation between face and voice. Komogortsev et al. [30] proposed an oculomotor plant characteristics (OPC) based liveness detection method which utilized eye movement signals for the identification of people. The live data is taken from 32 individuals. In [31] liveness detection measure was proposed to recognize and find the liveness of the face that was based on the challenge and response method. The author's utilized eye and mouth movement to generate random challenges and observe the response of users. Haar classifier was used to identify eye and mouth movements. Somasundaram et al. [32] have been proposed a Spatio-temporal feature detector based on the sparse representation length of the Spatio-temporal patches measured by residual error. The authors suggested a classification framework based on a bag of features that provide a better result on KTH and UCF sports action datasets. Nagrani et al. [33] proposed a convolution neural network architecture for cross-modal matching between voices and faces, which was used for both binary and multi-way cross-modal face and audio matching. In [34] face liveness detection method was presented, in which deep features are extracted through convolution neural network and to extract the color features rotation invariant local binary patterns were utilized. To differentiate between genuine and fake faces support vector machine was used. Schardosim et al. [35] have been proposed a method that integrates the imaging features with liveness features and used to distinguish between real access and spoofing attacks. These are based on the models learned by an artificial neural network.

Image Quality Based Techniques

Many techniques have been developed to differentiate between fake and genuine face, image quality assessment is one of them. Properties of texture or image quality are used in the image quality-based method. These are categorized into two main parts reference-based and non-reference-based. In the reference-based method, an undistorted

Table 1 Liveness detection techniques used in the multimodal biometric system

References	Features	Attack	Database	Description
Li Ma et al. [21]	Iris	Spoof attack	CASIA Iris	Proposed a method based on texture analysis for iris recognition
Sun et al. [26]	Face	Presentation attack	Self-constructed	Proposed a conditional random fields (CRFs) method
Shahin et al. [4]	Hand vein and Fingerprint	Spoof attack	Self-constructed	Proposed a new prototype design for multimodal biometrics
Rodrigues et al. [5]	Face, Fingerprint	Presentation attack	FVC2004DB1, FERET-b series	Proposed two novel schemes, the extension of the likelihood ratio based fusion and fuzzy logic
Liting et al. [28]	Face	Presentation attack	Self-constructed	Presented a face live detection method which utilized physiological motion
Bao et al. [16]	Face	Photo-attack	Self-constructed	Proposed optical flow field method to recognize the liveness of face
Chetty [29]	Face and voice	Spoof attack	VidTIMIT, DaFeX Corpora	Proposed a new fuzzy fusion technique for liveness detection
Komogortsev et al. [30]	Eye	Spoof attack	Self-constructed	Proposed Oculomotor Plant Characteristics (OPC) based liveness detection method
Barrero et al. [7]	Face, Iris	Indirect Attack	BioSecure	Presented and evaluated the first software-based attack
Singh et al. [31]	Face	Spoofing attack	Self-constructed	Proposed a liveness detection measure to recognize and find the liveness of face, based on challenge and response method
Akhtar et al. [14]	Face, iris fingerprint,	Spoofing attack	ATVS-Flr, ATVS-FFp	Proposed mobile biometric liveness detection (MoBio LivDet) method
Wild et al. [42]	Face and Fingerprint	Direct attack	LivDet 2013, CASIA FASD	Proposed 1-median filtering as a spoofing resistant
Das et al. [8]	sclera and iris	Direct attack	Self-constructed	Proposed a framework for software-based liveness detection
Boulkenafet et al. [24]	Face	Presentation attack	MSU-MFSD,CASIA-FASD	Proposed an approach based on color texture analysis for face spoofing detection
Lee et al. [37]	Finger-vein	Spoof attack	Self-constructed	Proposed a finger-vein biometric recognition system based on image quality assessment
Parveen et al. [23]	Face	Presentation attack	UPM, CASIA FASD, NUAA	A dynamic local ternary pattern has been proposed which utilizes Weber's law
Sollinger et al. [40]	Iris, face fingerprint, and finger vein	Presentation attack	ATVS-Flr, ATVS-FFp, IDIAP	Proposed non-reference image quality measures (IQM) to differentiate between fake and real data
Kavitha et al. [9]	Face	Fake face attack	CASIA FASD, MSU MFSD	Proposed multimodal biometric framework to detect face spoofing
Sahidullah et al. [17]	Voice	Replay attack	Self-constructed	Proposed a body conducted sensor and throat microphone for automatic speaker verification

Table 1 (continued)

References	Features	Attack	Database	Description
Komeili et al. [11]	ECG and fingerprint	Presentation attack	LivDet2015	Proposed a framework in which fingerprint and ECG are combined for user authentication and liveness detection
Schardosim et al. [35]	Face	Presentation attack	NUAA, CASIA	Proposed a method based on the models learned by an artificial neural network
Wang et al. [20]	Voice	Presentation attack	Self-constructed	Proposed a theoretical model to show the relationship between the characters in the user's speech and oral airflow pressure
Agarwal et al. [25]	Fingerprint and iris	Presentation attack	LivDet2011, ATVS-FFp, ATVS Fir	Proposed a liveness detection method which utilized fusion of fingerprint and iris. Dempster–Shafer (D–S) approach is used for the fusion at the decision level

reference image is utilized to estimate the quality of the test image while in the non-reference-based method pre-trained statistical models are utilized to estimate the quality of the test image [36]. In [22] the authors presented a method for iris liveness detection by utilizing multispectral images which can differentiate between real and fake images. Lee et al. [37] have been proposed a finger-vein biometric recognition system based on image quality assessment in which edge detection algorithm and two-dimensional mask-based entropy algorithm were used. In this work, a near-infrared (NIR) image quality assessment module was implemented and the proposed model was a prototype on an embedded field-programmable gate array prototyping (FPGA) platform. Akhtar et al. [38] proposed a face spoof recognition algorithm based on discriminative image patches in which frames were selected randomly from a given face video. The author's utilized seven new methods to obtain discriminative patches from a face image, and then features were selected and fed to a classifier for the final classification of real and spoof faces. Xia et al. [39] proposed a feature extraction method that utilized circularly symmetric.

Gabor feature and weber local binary pattern for liveness detection. Fingerprint images were analyzed in the spatial domain and frequency domain and final features were decided by the co-occurrence probabilities. In [40] non-reference image quality measures were proposed to distinguish between genuine and fake data. In this method, accurate classification of real versus fake iris, fingerprint, face, and finger vein data was achieved. In [41] a sparse representation-based blind image deblurring algorithm was proposed which helps to learn smaller sub-dictionaries from the patches clustered based on dominant orientation instead of learning a single large dictionary.

Conclusion

In this manuscript, we have presented a structured overview of the most relevant work carried out so far in the field of liveness detection. We also proposed a new classification for liveness detection methods based on multimodal biometrics and a review of the existing spoofing attacks. Further, a new classification has been developed for the multimodal biometric system based on liveness detection techniques into the following types namely (1) multiple traits based techniques, (2) multiple sensor-based techniques, (3) multiple representation-based techniques, (4) behavioural techniques, (5) image quality-based techniques. As the review has shown, several approaches have been achieved in the development of countermeasures against spoofing attacks. But, due to the development of new attacking methodologies every day, there is still the need to devote further efforts to the design of new and more efficient liveness detection approaches that may increase the reliability of biometric technology.

Compliance with Ethical Standards

Conflict of interest All authors declare that they have no conflict of interest.

References

1. Hadid A, Evans N, Marcel S, Fierrez J. Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. IEEE Signal Process Mag. 2015;32:20–30.

2. Akhtar Z, Micheloni C, Foresti GL. Biometric liveness detection: challenges and research opportunities. IEEE Secu Priv. 2015;13:63–72.
3. Marcel S, Nixon MS, Li SZ. Handbook of biometric anti-spoofing. London: Springer London; 2014. p. 1–279.
4. Shahin MK, Badawi AM, Rasmy ME. A multimodal hand vein, hand geometry, and fingerprint prototype design for high security biometrics. In: Proceedings of the 2008 Cairo international biomedical engineering conference. IEEE; 2008. p. 1–6.
5. Rodrigues RN, Ling LL, Govindaraju V. Robustness of multimodal biometric fusion methods against spoof attacks. J Vis Lang Comput. 2009;20:169–79.
6. Jiang RM, Sadka AH, Crookes D. Multimodal biometric human recognition for perceptual human–computer interaction. IEEE Trans Syst Man Cybern Part C Appl Rev. 2010;40:676–81.
7. Gomez-Barrero M, Galbally J, Fierrez J. Efficient software attack to multimodal biometric systems and its application to face and iris fusion. Pattern Recognit Lett. 2014;36:243–53.
8. Das A, Pal U, Ferrer MA, Blumenstein M. A framework for liveness detection for direct attacks in the visible spectrum for multimodal ocular biometrics. Pattern Recognit Lett. 2016;82:232–41.
9. Kavitha P, Vijaya K. Optimal feature-level fusion and layered k-support vector machine for spoofing face detection. Multimed Tools Appl. 2018;77:26509–43.
10. Jain AK, Hong L, Kulkarni Y. A multimodal biometric system using fingerprint, face, and speech 1999; 10.
11. Komeili M, Armanfard N, Hatzinakos D. Liveness detection and automatic template updating using fusion of ecg and fingerprint. IEEE Trans Inf Forensics Secur. 2018;13:1810–22.
12. Walia GS, Singh T, Singh K, Verma N. Robust multimodal biometric system based on optimal score level fusion model. Expert Syst Appl. 2019;116:364–76.
13. Chetty G, Wagner M. Multi-level liveness verification for face-voice biometric authentication. In: Proceedings of the 2006 Biometrics Symposium: special session on research at the biometric consortium conference. IEEE; 2006. p. 1–6.
14. Akhtar, Z., Micheloni, C., Piciarelli, C., Foresti, G.L.: MoBio; LivDet: Mobile biometric liveness detection. In: 2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). pp. 187–192. IEEE (2014)
15. Gupta K, Walia GS, Sharma K. Multimodal biometric system using grasshopper optimization. In: 2019 international conference on computing, communication, and intelligent systems (ICCCIS); 2019. IEEE, p. 387–391.
16. Bao W, Li H, Li N, Jiang W. A liveness detection method for face recognition based on optical flow field. In: Proceedings of 2009 international conference image analysing signal process; 2009. IASP 2009, p. 233–236.
17. Sahidullah M, Thomsen DAL, Hautamaki RG, Kinnunen T, Tan ZH, Parts R, Pitkanen M. Robust voice liveness detection and speaker verification using throat microphones. IEEE/ACM Trans Audio Speech Lang Process. 2018;26:44–56.
18. Kim W, Hong W, Kim T, Kim D, Lee M. RF sensor-based liveness detection scheme with loop stability compensation circuit for a capacitive fingerprint system. IEEE Access. 2019;7:152545–51.
19. Albakri G, Alghowinem S. The effectiveness of depth data in liveness face authentication using 3D sensor cameras. Sensors. 2019;19:1928.
20. Wang, Y., Cai, W., Gu, T., Shao, W., Li, Y., Yu, Y.: Secure Your Voice. In: Proceedings of ACM interactive, mobile, wearable ubiquitous technology, vol 3. 2019. p. 1–28.
21. Ma Li, Tan T, Wang Y, Zhang D. Personal identification based on iris texture analysis. IEEE Trans Pattern Anal Mach Intell. 2003;25:1519–33.
22. Chen R, Lin X, Ding T. Liveness detection for iris recognition using multispectral images. Pattern Recognit Lett. 2012;33:1513–9.
23. Parveen S, Ahmad S, Abbas N, Adnan W, Hanafi M, Naeem N. Face liveness detection using dynamic local ternary pattern (DLTP). Computers. 2016;5:10.
24. Boulkenafet Z, Komulainen J, Hadid A. Face spoofing detection using colour texture analysis. IEEE Trans Inf Forensics Secur. 2016;11:1818–30.
25. Agarwal R, Jalal AS, Arya K. A multimodal liveness detection using statistical texture features and spatial analysis. Multimed Tools Appl. 2020;79:13621–13645.
26. Sun L, Pan G, Wu Z, Lao S. Blinking-based live face detection using conditional random fields. In: Advances in Biometrics. vol. 4642 LNCS. Springer: Berlin, Heidelberg; 2007. p. 252–260
27. Zhao G, Pietik M. Patterns with an application to facial expressions. Most. 2007;29:1–14.
28. Wang L, Ding X, Fang C. Face live detection method based on physiological motion analysis. Tsinghua Sci Technol. 2009;14:685–90.
29. Chetty G. Biometric liveness checking using multimodal fuzzy fusion. In: 2010 IEEE world congress computational intelligence; 2010. WCCI, p. 1–8.
30. Komogortsev OV, Karpov A. Liveness detection via oculomotor plant characteristics: attack of mechanical replicas. In: Proceedings of 2013 international conference biology; 2013. ICB.
31. Singh AK, Joshi P, Nandi GC. Face recognition with liveness detection using eye and mouth movement. In: 2014 international conference on signal propagation and computer technology (ICSPCT 2014); 2014. IEEE, p. 592–597.
32. Somasundaram G, Cherian A, Morellas V, Papanikolopoulos N. Action recognition using global spatio-temporal features derived from sparse representations. Comput Vis Image Underst. 2014;123:1–13.
33. Nagrani A, Albanie S, Zisserman A. Seeing voices and hearing faces: cross-modal biometric matching. In: 2018 IEEE/CVF conference on computer vision and pattern recognition; 2018. IEEE, p. 8427–8436.
34. Chen FM, Wen C, Xie K, Wen FQ, Sheng GQ, Tang XG. Face liveness detection: fusing colour texture feature and deep feature. IET Biom. 2019;8:369–77.
35. Schardosim LR, Dos Santos RR, Scharcanski J. Detection of presentation attacks using imaging and liveness attributes. Electron Lett. 2019;55:1226–9.
36. Saad MA, Bovik AC, Charrier C. Blind image quality assessment: a natural scene statistics approach in the DCT domain. IEEE Trans Image Process. 2012;21:3339–52.
37. Lee YH, Khalil-Hani M, Bakhteri R, Nambiar VP. A real-time near infrared image acquisition system based on image quality assessment. J Real Time Image Process. 2017;13:103–20.
38. Akhtar Z, Foresti GL. Face spoof attack recognition using discriminative image patches. J Electr Comput Eng. 2016;2016:1–15.
39. Xia Z, Lv R, Sun X. Rotation-invariant Weber pattern and Gabor feature for fingerprint liveness detection. Multimed Tools Appl. 2018;77:18187–200.
40. Söllinger D, Trung P, Uhl A. Non-reference image quality assessment and natural scene statistics to counter biometric sensor spoofing. IET Biom. 2018;7:314–24.
41. Singh K, Vishwakarma DK, Walia GS. Blind image deblurring via gradient orientation-based clustered coupled sparse dictionaries. Pattern Anal Appl. 2019;22:549–58.
42. Wild P, Radu P, Chen L, Ferryman J. Robust multimodal face and fingerprint fusion in the presence of spoofing attacks. Pattern Recognit. 2016;50:17–25.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.