Insight on Face Liveness Detection: A Systematic Literature Review

Article *in* International Journal of Electrical and Computer Engineering · July 2019

CITATIONS
4

READS
3,016

1 author:

Enas A. Raheem
University of Technology, Iraq
9 PUBLICATIONS **22** CITATIONS

SEE PROFILE

International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 6, December 2019, pp. 5165~5175
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i6.pp5165-5175

Insight on face liveness detection: A systematic literature review

Enas A. Raheem[1], Sharifah Mumtazah Syed Ahmad[2], Wan Azizun Wan Adnan[3]
[1]Department of Computer Engineering, University of Technology, Iraq
[2,3]Department of Computer and Communication Systems, Faculty of Engineering,
Universiti Putra Malaysia (UPM), Malaysia

Article Info

Article history:

Received Jun 21, 2018
Revised Jul 17, 2019
Accepted Jul 29, 2019

Keywords:

Anti-spoofing
Biometric
Face liveness detection
Systematic literature review
Taxonomy

ABSTRACT

To review researcher's attempts in response to the problem of spoofing and liveness detection, mapping the research overview from the literature survey into a suitable taxonomy, exploring the basic properties of the field, motivation of using liveness detection methods in face recognition, and Problems that may restrain the advantages. We presented a subjected search on face recognition with liveness detection and its synonyms in four main databases: Web of science, Science Direct, Scopus and IEEE Xplore. We believe that these databases are widely inclusive enough to cover the literature. The final number of articles considered is 65 articles. 4 of them where review and survey articles that described a general overview about liveness detection and anti-spoofing methods. Since 2012, and despite of leaving some areas unestablished and needs more attention, researchers tried to keep track of liveness detection in several ways. No matter what their category is, articles concentrated on challenges that faces the full utility of anti-spoofing methods and recommended some solutions to overcome these challenges. In this paper, different types of liveness detection and face anti-spoofing techniques are investigated to keep researchers updated with what is being developed in this field.

Corresponding Author:

Enas A. Raheem,
Department of Computer and Communication Systems,
Faculty of Engineering,
Universiti Putra Malaysia (UPM),
Selangor, 43400, Malaysia.
Email: alkinany.enas91@gmail.com

1. INTRODUCTION

Biometrics is a multidisciplinary field involved with measuring and mapping specific biological traits, e.g. fingerprints, face, palm veins, etc. to be used as an individualized recognition code [1]. Biometric traits can be classified into two groups that are physical traits such as aforementioned examples and behavioral traits such as signature, voice and keystrokes. Biometric is essential for a wide range of technologies. However, one of the main obstacles facing biometric recognition systems is fraudulent identity which is conceptually referred as a spoofing attack. Broadly, two types of attacks can be considered: indirect and direct attacks. Indirect attacks are implemented inside the system, intruded by hackers or intruders, e.g. by tampering the feature extractor (i.e. matcher), or by performing modifications to the template database. Indirect attacks can be precluded by various measures including but not limited to anti-virus software, firewalls, encryption and intrusion detection. Direct attacks on the other hand, are carried out at the sensor level outside the digital limits of the system and therefore, no mechanisms for digital protection can be used to anticipate it [1]. Liveness detection is a major area of interest within the field of biometric that encompasses a process of verifying whether the biometric being captured by the recognition system is

genuine (i.e. alive) or has been mimicked by intruders to have an unauthorized access to the biometric system.

In the literature on liveness detection, the relative importance of face liveness detection has been subject to considerable discussion. In this article we provide a review of the state-of-the-art anti-spoofing detection techniques for facial biometrics. Face anti-spoofing techniques requires a genuine photograph, recorded video or dummy evidence etc. to be present at the sensor (i.e. camera). Photographs generally lacks the 3D information's and provides less physiological evidences than videos can provide. This can be exploited in liveness detection as a limitation of static images. However, videos captured by high quality cameras can be also a challenging spoofing attack as they provide a strong sign for vitality through motion. Dummy models on the other hand can be a threat to facial biometric system containing 3D information that static images and videos do not provide [2]. Recent developments in the field of facial biometric have led to a renewed interest in liveness detection as a solution for spoofing attack problems. The purpose of this paper is to review recent research efforts mapping them into a cohesive taxonomy based on liveness indicators and a further classification is provided on face anti-spoofing techniques.

2. LITERATURE REVIEW

A block diagram of face liveness detection system architecture is shown in Figure 1, it is necessary to clarify the exact process of using liveness detection system which involves a user to present a biometric sample to the sensor, which is a camera in our case. The face image is then preprocessed appropriate form (e.g. through noise removal, blur and focus corrections techniques) so that the image is ready to the next step of feature extraction. The output biometric template of feature extraction process is a distinguishable sample with distinct features that allows classifier to decide whether presented sample is real or spoofed by the aid of pre-trained data. Genuine samples will be processed for identification, while spoofed samples will be automatically discarded for authentication, and in order to measure the performance of liveness detection system,
the following measurements are defined [3]:

- False Reject Ratio (FRR): it is the rate where a live sample is identified as a spoof attack.
- False Acceptance Ratio (FAR): it is the rate of system where a fake sample is authenticated as live (genuine) sample.
- Failure to Acquire (FA): it is the rate of the system when it fails to perform samples collection.
- Mean Transaction Time (MTT): it is the average of system's required time for making a decision.
- Receiver Operating Characteristic (ROC): plots that are used to select the operating threshold of the system with prior knowledge of the FRR and FAR probability.

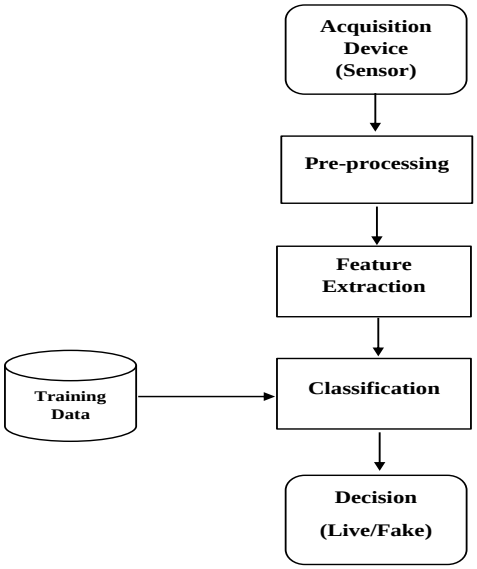

Figure 1. Block diagram of face liveness detection system

Another important aspect of vitality detection that deserves to be highlighted is the publicly available databases that consist of images of various textures which have been utilized extensively in validating liveness detection against spoofing attacks such as high-quality images attacks to video-replays. The available databases and the literature that utilized these databases is described in Table 1. Although these databases provided a very useful tool for researchers, the lack of publicly available datasets of different nature such as eye blinking videos or mouth and head movement, this limitation makes it hard to benchmark with such anti-spoofing methods.

Table 1. Publicly available databases

No	Database	Detection Method			Reference
		Texture	Life sign indicator	3D Properties	
1	Replay Attack	√			[4, 5]
2	NUAA	√			[6-8]
3	CASIA	√			[9, 10]
4	YALE	√			[6]
5	XM2VTS	√	√		[11, 12]
6	FSA	√			[13]
7	OTCBVS	√			[14]
8	UCBN	√	√		[15]
9	3D MAD	√			[16, 17]
10	SC		√	√	[18]
11	ZJU		√	√	[19, 20]
12	AVOZES	√	√		[15]
13	DaFEX		√		[21]
14	VidTIMIT		√		[15]

3. RESEARCH METHOD

The significant keyword in the search domain of this paper is "Face", thus precludes any non-face liveness detection like fingerprint, palm print, iris, etc. We also limited the search the search scope to English literature only.

3.1. Study selection procedure

Four databases were selected to perform the search of required articles: the IEEE Xplore technical literature library in engineering and technology; the (WoS) web of science service; the Science Direct database and Scopus database. To cover all related literature and offer a wider view of researcher's efforts regarding this area. Study selection procedure included searching the sources of the literature, followed by 2 steps of screening and filtering resulted articles, in the first step duplicated and irrelevant articles were excluded by title and abstract scanning. While a full-text reading resulted in filtering the scanned articles as a second step. Both steps were applied based on chosen eligibility criteria which is followed by the authors.

3.2. Search

The search was done in the afore mentioned databases, using a carefully selected keyword including "face recognition" with the "AND" operator and "liveness detection" with different synonyms as shown in the query text as shown in Figure 2. We further applied refinements in each search engine to eliminate any type rather than journal and conference articles to ensure including appropriate scientific works related to our survey.

Query:

("face") AND ("liveness detection" OR "anti spoofing" OR "anti-spoofing" OR "validation detection") refined by
Year: 2012-2017

Figure 2. Search query

3.3. Inclusion criterion

An eligible criterion was specified in PRISMA Flow Diagram as shown in Figure 3 to decide which article to be included and thus, mapping the domain of research [22]. This was done after removal of duplicates and irrelevant articles in the earlier steps screening and filtering. Eligibility of the article was

decided by specific aspects such as English articles only were considered and targeted topic was concerned in face recognition rather than any other biometric field such as iris, fingerprint or palm print etc.

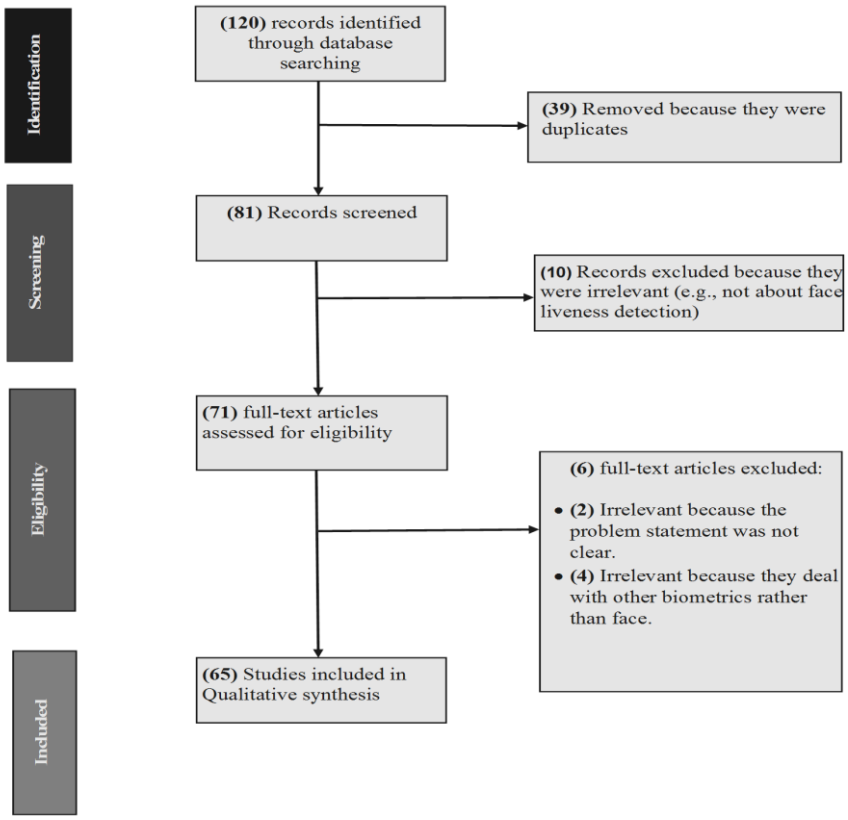

Figure 3. PRISMA flow diagram

4. RESULTS AND ANALYSIS

4.1. Search results

The initial search results were (120) articles: (3) from ScienceDirect, (34) results of IEEE Xplore, 42 from Scopus and 41 articles are from WoS, including the period 2012 to 2017. There were 39 articles duplicates among the four databases. Titles and abstracts scanning was applied, 10 were excluded which results in 71 papers. Next, a full text reading is performed that included (65) articles as a final set. These papers were carefully read to specify the

Research area they belong to in this topic. (4) Of them were review articles that referred to existing methods or provided a general overview about the established techniques. The other branch of this layer of classification was applied based on liveness indicators exist resulting in 61 articles. Liveness indicators layer was further divided into subcategories based on techniques used in each indicator.

a. Review and survey articles: The literature on face liveness detection revealed 4 review articles in earlier specified period of last five years. These reviews mainly investigated literature in terms of state-of-art techniques in liveness detection. Olga *et al.* (2012) presented an overview on 2D face liveness detection that categorized the literature based on live sign clues with a detailed discussion on different spoofing attacks that highlighted their relation to the developed solutions. In her work Olga *et al.* (2012) also shed some light on publicly available datasets and made a clear path for study future directions [23]. Similarly, Sajida *et al.* (2015) classified her review on face anti-spoofing methods into intrusive and non-intrusive approaches and provided a critical review on literature for the architecture of liveness detection system and its implementations [2]. The study by Galbally *et al.* (2015) offers probably the most comprehensive analysis of literature of face anti-spoofing during the past decade. A Chronological evolution of biometric anti-spoofing was represented and theories, methodologies, database evaluation and state-of-art techniques were covered for the period (1903-2014) [24]. One year later Bangga and Singh introduced a review on spoofing detection in face recognition considering facial

motion deduction and facial texture analysis in their classification of techniques [25]. Spoofing mechanisms for facial biometrics were discussed and algorithms and features for various spoofing attacks were also broadly reviewed. Figure 4 shows a taxonomy of research literature on face liveness detection.

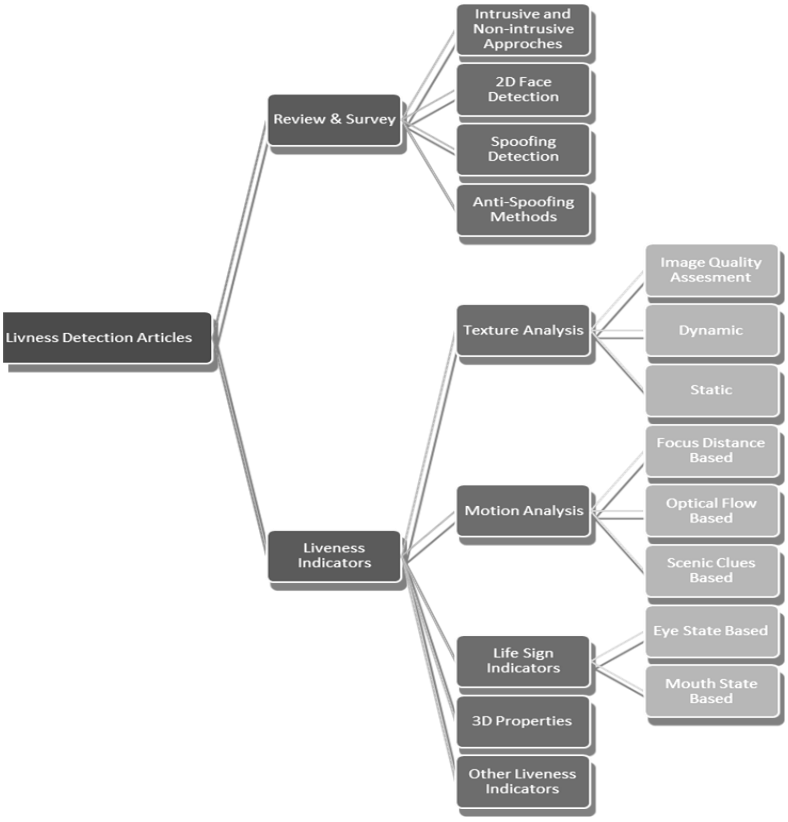

Figure 4. A taxonomy of research literature on face liveness detection

b. Face liveness indicators: The existing literature on liveness detection focuses particularly on liveness indicators as a clue that helps to find the appropriate solution for different spoofing problems. Based on the liveness indicator used, approaches of detection are separated into five categories as follows:

4.1.1. Texture analysis

Based on the assumption that fake face produces a different texture pattern that does not exist in real face, texture features are extracted from the face image or sequence of images to provide detectable information that help to distinguish real from fake identities. In this review, texture-based approaches are generally divided into three groups based on detection technique used: image quality assessment (IQA), dynamic, and static. Image quality assessment theory in liveness detection implies that there is a quality difference between fake and real images that can be detected using image quality measures which allows to build a protection method against spoofing attacks. Researchers exploited this assumption to develop various IQA techniquesin [5, 26-33]. An evaluation of several IQA techniques was done in [34].Several studies have tested the efficacy of dynamic texture analysis in liveness detection in [35-43]. Static texture analysis on the other hand have been explored through large number of published studies in our research period in [4, 44-58].

4.1.2. Motion analysis

Three types of techniques were surveyed within motion analysis which assumes that a planar object moves in a different way other than a real face. The method encompasses the calculation of information regarding the moving points of an image in the scene. These types are : Focus distance based [59, 16], Optical flow based [60-63] and Scenic clues based motion analysis [64-67].

4.1.3. Life sign indicators

The movement of a certain part in the face such as a lip movement or eye blinking can be an indicator of liveness, eye state and mouth state are two main signs to be taken into consideration in life sign detection algorithms which were established in [68-72] respectively. A utilization of both indicators to build a robust liveness detection system was also proposed by A.Singh *et al*. (2014) in [73].

4.1.4. 3D properties

Few studies focused on this type of method where detection techniques are proposed to analyze the 3D facial structure to distinguish real from fake samples in liveness detection system [74-77].

4.1.5. Other liveness indicators

The literature on liveness detection has highlighted several other studies with a combination rather than one liveness indicator. These studies were included in our search period are [78-83].

4.2. Data analysis

The initial objective of the paper is to update the state-of-art of liveness detection techniques. The purpose is to highlight recent trends on this topic research. The difference of this review from many previous works is that it focuses on the literature of techniques rather than techniques themselves. Moreover it proposes a taxonomy of the related literature. Mapping the literature into a taxonomy in a research area can provide several benefits. One of which is that it organizes the mass of publications in the literature. For instance, a new researcher in the field of facial biometric detection may be overwhelmed with the huge number of papers in this particular field without any sort of structure and may fail to have clear idea about the existent activities of the area. Taxonomizing the literature can help sorting out the different activities into meaningful layout. Furthermore, a taxonomy mapping the work on liveness detection into certain categories can help to underline the weaknesses and strengths in a research coverage. This is done by indicating several paths that the researcher may go through to find the gaps in a branch of the subject. A data analysis of the literature is probably interesting to provide researchers with proportions of the publications in different aspects. Figure 5 presents the results by number of articles in each of the explored databases before and after applying our eligibility criteria. The final results were mostly found in WOS while Scopus and IEEE Xplore may be equivalent to its results, and science direct shows the least proportion regarding our topic. This may be beneficial to those who don't have access to all database source they can use other engines to get a close enough search results.

Another analysis of data was done on the number of articles in various categories by their year of publication during the period (2012-2017) is shown in Figure 6. It reveals that there is a noticeable increment in number of published works between 2012 and 2016 in this area. And his most significant class of interest is the texture analysis and the least are shown to be the review papers and 3D properties.

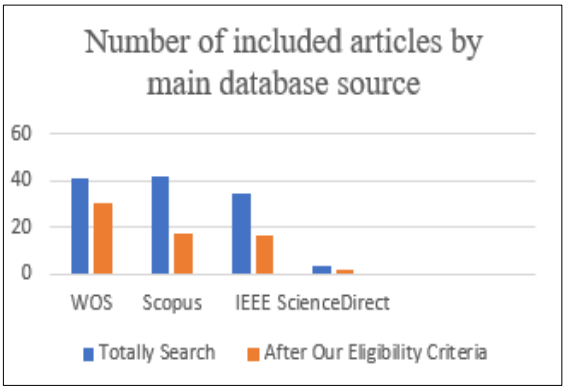

Figure5. Number of included articles by main database source

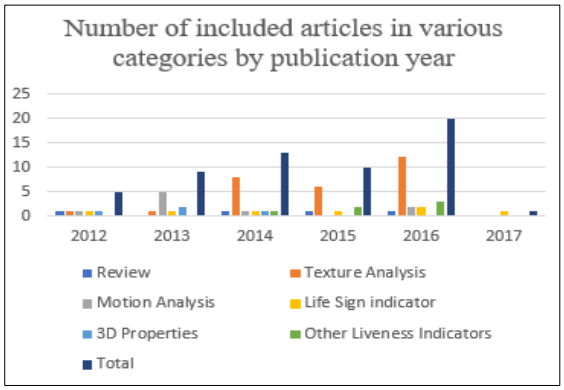

Figure 6. Number of included articles in various categories by publication year

It is clearly shown that texture analysis techniques occupy most of the publication area. Static, IQA, and dynamic techniques respectively shows the highest scores among other techniques. An evaluation of systems performance for liveness detection approaches that presented promising accuracies is briefly

described in Table 2 in terms of accuracy, half total error rate (HTER), area under ROC curve (AUC), equal error rate (EER), and time where calculated.

Table 2. Evaluation of performance

Category	Reference	Accuracy	HTER	EER	AUC	Time
Texture Analysis	[32]	-	0.0	5.83	-	-
	[26]	-	4.78	6.23	-	-
	[5]	-	15.2	-	-	
	[27]	-	15.2,32.4	-	-	-
	[30]	-	0.5	-	-	0.573 sec
	[29]	-	1.65	-	-	-
	[36]				0.84,0.81, 0.83	-
	[37]	-	15.16,8.51, 7.60	17,16, 10	-	-
	[38]	-	3.75,1.38, 1.0	30.2, 1,8	-	-
	[39]	80.95%,90.48	-	-	-	-
	[43]	0.9720	-	-	-	-
	[45]	-	0, 0.29	6.7, 2.9	-	-
	[4]	-	15.16,17.17, 34.01	-	-	-
	[46]	-	10%	-	-	-
	[47]	93.06,93.13, 93.16	6.94,6.87, 6.84	-	-	-
	[48]	-	-	13.3,12.9,8.58,5.82	-	-
	[53]	-	2.7,4.6, 9.5	-	-	-
	[57]	-	16.21, 12.3034, 15.45	-	-	-
Motion Analysis	[59]	97.5%	-		-	-
	[16]	-	-	9.57,3.47, 0.00	-	-
	[60]	-	22.81, 13.33	-	-	-
	[61]	-	4.38, 1.25	-	-	-
	[63]	-	-	9.6,12.5	-	-
	[62]	-	1.52	-	-	-
	[64]	-	-	6.8	-	-
	[65]	100%	-	-	-	-
	[66]	85%,94.5%, 92.9%	-	-	-	-
	[67]	-	5.1%	-	-	-
Life Sign Indicators	[68]	89.7%,98%, 94.8%	-	-	-	-
	[69]	99.4%, 96.77%	-	-	-	-
	[71]	99%	-	-	-	-
	[84]	90.5%, 84.4%	-	-	-	-
3D Properties	[75]	-	-	10%	-	-
	[76]	100%	-	-	-	-
Other Liveness Indicators	[63]	-	2.75	3.3,0.0	-	-
	[79]	-	12.5,13.72	-	-	34msec
	[80]	-	50,34.38	-	-	-

5. CONCLUSION

In this investigation, the aim was to have an insight of face liveness detection through updating and taxonomizing the literature. Another important thing is that the new researchers in this field can have a clear idea about what face liveness detection is and what are the opportunities to develop new methods, adopt new technologies and go through specific direction and explore its research gaps without the need to waste the time on investigating irrelevant works. We have found that generally the liveness indicators are the most suitable tool of theory to classify the literature search results. Moreover, a widely enough reading to have knowledge about the topic would be easier to gain from review papers rather than from books specially in

terms of identifying all the related synonyms of the search query keywords to be able to cover mostly all the related work. The outcome of research effort on liveness detection appears to have a significant progress, However, it remains a challenge for the facial recognition systems. Therefore, we recommend future researchers to focus on directions that have not been established before and try to bridge the gap in those paths. In general, it seems that a green area of the research is the one with few publications and can be a good ground for implanting the new ideas, technologies and methods those would result in significant solutions to the problems of the biometric system. A combination of more than one liveness indicator in one system, a use of test data with different spoofing scenarios, would affect the overall performance of detection system. Finally, the aim is not to get a system 100% secured, but to simply make the system more secure, robust and as accurate as possible.

REFERENCES

[1] M. S. Nixon, *Handbook of Biometric Anti-Spoofing*, Verlag London: Springer, 2014.

[2] S. Parveen, S. Mumtazah, S. Ahmad, M. Hanafi, W. Azizun, and W. Adnan, "Face anti-spoofing methods," *Curr. Sci.*, vol. 108, no. 8, 2015.

[3] A. Adler and S. Schuckers, *Security and Liveness, Overview*, in *Encyclopedia of Biometrics, S. Z. Li and A. Jain, Eds. Boston, MA: Springer US*, 2009, pp. 1146–1152.

[4] I. Chingovska, A. Anjos, and E. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing," *Int. Conf. Biometrics Spec. Interes. Gr.*, 2012, pp. 1–7.

[5] T. De Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "LBP-TOP based countermeasure against face spoofing attacks," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7728 LNCS, no. PART 1, pp. 121–132, 2013.

[6] J. Galbally, S. Marcel, and J. Fierrez, "Image quality assessment for fake biometric detection: Application to Iris, fingerprint, and face recognition," *IEEE Trans. Image Process.*, vol. 23, no. 2, pp. 710–724, 2014.

[7] B. Peixoto, C. Michelassi, and A. Rocha, "Face liveness detection under bad illumination conditions," *Proc. - Int. Conf. Image Process. ICIP*, pp. 3557–3560, 2011.

[8] W. R. Schwartz, *at al.*, "Face Spoofing Detection through Partial Least Squares," *Int. Jt. Conf. Biometrics*, 2011.

[9] J. Määttä, A. Hadid, and M. Pietikäinen, "Face spoofing detection from single images using texture and local shape analysis," *IET Biometrics*, vol. 1, no. 1, p. 3, 2012.

[10] N. Kose and J. L. Dugelay, "Classification of captured and recaptured images to detect photograph spoofing," *2012 Int. Conf. Informatics, Electron. Vision, ICIEV 2012*, pp. 1027–1032, 2012.

[11] J. Galbally and S. Marcel, "Face anti-spoofing based on general image quality assessment," *Proc. - Int. Conf. Pattern Recognit.*, pp. 1173–1178, 2014.

[12] Z. Zhiwei et al., "A face antispoofing database with diverse attacks," in Proc. Int. Conf. on Biometrics (ICB), pp. 26–31, 2012.

[13] K. Kollreider, H. Fronthaler, M. I. Faraj, and J. Bigun, "Real-Time Face Detection and Motion Analysis With Application in ' Liveness ' Assessment," *Analysis*, vol. 2, no. 3, pp. 548–558, 2007.

[14] K. Kollreider, H. Fronthaler, and J. Bigun, "Non-intrusive liveness detection by face images," *Image Vis. Comput.*, vol. 27, no. 3, pp. 233–244, 2009.

[15] M. H. Sun, L., Huang, W. B. and Wu, "TIR/VIS correlation for liveness detection in face recognition.," *in Computer Analysis of Images and Pattern, Springer*, pp. 114–121, 2011.

[16] G. Chetty and M. Wagner, "Co Ru Reme Fron Usera I Chleng," *Biometrics*, 2006.

[17] S. Kim, S. Yu, K. Kim, Y. Ban, and S. Lee, "Face liveness detection using variable focusing," *in Proceedings - 2013 International Conference on Biometrics, ICB 2013*, 2013.

[18] N. Erdogmus and S. Marcel, "Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect," *IEEE 6th Int. Conf. Biometrics Theory, Appl. Syst. BTAS 2013*, 2013.

[19] W. Bao, H. Li, N. Li, W. Jiang, and a O. F. Field, "A Liveness Detection Method for Face Recognition Based on Optical Flow Field," *Computer (Long. Beach. Calif).*, pp. 0–3, 2009.

[20] S. M. Hatture, "Prevention of Spoof Attack in Biometric System Using Liveness Detection," *Int. J. Latest Trends Eng. Technol.*, no. Special Issue-IDEAS-2013, pp. 42–49, 2013.

[21] A. Lagorio, M. Tistarelli, M. Cadoni, C. Fookes, and S. Sridharan, "Liveness detection based on 3D face shape analysis," *2013 Int. Work. Biometrics Forensics*, pp. 1–4, 2013.

[22] G. Pan et al., "Eyeblink-based Anti-Spoo ng in Face Recognition from a Generic Webcamera," *11th IEEE ICCV*, Rio Janeiro, Brazil, Oct., vol. 14, pp. 20, 2007.

[23] G. Pan, L. Sun, Z. Wu, and Y. Wang, "Monocular camera-based face liveness detection by combining eyeblink and scene context," *Telecommun. Syst.*, vol. 47, no. 3–4, pp. 215–225, 2011.

[24] K. Kollreider, H. Fronthaler, and J. Bigun, "Verifying liveness by multiple experts in face biometrics," *2008 IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Work. CVPR Work.*, 2008.

[25] C. Kant, "Fake Face Recognition using Fusion of Thermal Imaging and Skin Elasticity," *Ijcsc*, vol. 4, no. 1, pp. 65–72, 2013.

[26] G. Chetty, "Robust audio visual biometric person authentication with liveness verification," *Intel Multimed. Anal. Secur. Appl. SCI 282, Springer*, pp. 59–78, 2010.

[27] A. Liberati et al., "The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration," *PLOS Med.*, vol. 6, no. 7, pp. 1–28, 2009.
[28] O. Kahm and N. Damer, "2D face liveness detection: An overview," *BIOSIG-Proceedings IEEE Int. Conf. the. Biometrics Spec. Interes. Gr. (BIOSIG)*, 2012, pp. 171–182.
[29] J. Galbally, S. Marcel, and J. Fierrez, "Biometric Antispoofing Methods: A Survey in Face Recognition," *IEEE Journals & Magazine*, vol. 2, 2015.
[30] M. Bagga and B. Singh, "Spoofing Detection In Face Recognition: A Review," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 2037–2042.
[31] S. L. Fernandes and G. J. Bala, "Developing a Novel Technique for Face Liveness Detection," *Phys. Procedia*, vol. 78, no. December 2015, pp. 241–247, 2016.
[32] J. Galbally and S. Marcel, "Face anti-spoofing based on general image quality assessment," in *Proceedings - International Conference on Pattern Recognition*, 2014, pp. 1173–1178.
[33] A. Bhaskar and R. P. Aneesh, "Advanced algorithm for gender prediction with image quality assessment," *2015 Int. Conf. Adv. Comput. Commun. Informatics, ICACCI 2015*, pp. 1848–1855, 2015.
[34] P. Pravallika, "SVM Classification For Fake Biometric Detection Using Image Quality Assessment: Application to iris, face and palm print," in *2016 International Conference on Inventive Computation Technologies(ICICT)*, 2016.
[35] A. A. S. A. Dhole, Patil, "System for Multi-biometric Detection," *2016 Int. Conf. Inven. Comput. Technol.*, vol. 3, no. 2, 2016.
[36] L. Feng, L.-M. Po, Y. Li, and F. Yuan, "Face liveness detection using shearlet-based feature descriptors," *J. Electron. Imaging*, vol. 25, no. 4, pp. 043014, 2016.
[37] L. Feng et al., "Integration of image quality and motion cues for face anti-spoofing: A neural network approach," *J. Vis. Commun. Image Represent.*, vol. 38, 2016.
[38] E. A. Raheem and S. M. S. Ahmad, "Statistical analysis of image quality measures for face liveness detection," in *Lecture Notes in Electrical Engineering*, 2019, vol. 547, pp. 543–549.
[39] I. Chingovska et al., "The 2nd competition on counter measures to 2D face spoofing attacks," *Proc. - 2013 Int. Conf. Biometrics, ICB*, 2013, pp. 1–6.
[40] V. Ravibabu, "A Vary Approach to Face Recognition Veritable Mechanisms for Android Mobile against Spoofing," in *IEEE International Conference on Computational Intelligence and Computing Research*, 2014.
[41] P. J. Arathy and V. V. Nair, "Analysis of Spoofing Detection using Video Subsection Processing," in *Proceedings of the International Conference on Informatics and Analytics - ICIA-16*, 2016, pp. 1–6.
[42] L. Feng, L.-M. Po, Y. Li, and F. Yuan, "Face liveness detection using shearlet-based feature descriptors," *J. Electron.Imaging*, vol. 25, no. 4, pp. 043014, 2016.
[43] S. R. Arashloo, J. Kittler, and W. Christmas, "Face Spoofing Detection Based on Multiple Descriptor Fusion Using Multiscale Dynamic Binarized Statistical Image Features," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 11, pp. 2396–2407, 2015.
[44] J. Peng and P. P. K. Chan, "Face liveness detection for combating the spoofing attack in face recognition," in *International Conference on Wavelet Analysis and Pattern Recognition*, 2014, vol. 2014-Jan., pp. 176–181.
[45] R. R. R. K. M. S. B. C, "Face Presentation Attack Detection Across Spectrum using Time-Frequency Descriptors of Maximal Response in Laplacian Scale-Space," in *2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA)*, 2016, pp. 0–5.
[46] K. G. D. E. S. A, "Short term re-identification of Automatic Teller Machine (ATM) users via face and body appearance features," in *2016 4th International Conference on Biometrics and Forensics (IWBF)*, 2016, pp. 1–6.
[47] F. G. B. D. N. Q.-T. P. D.-T. D.-N. Giulia Boato and Department, "Face spoofing detection using LDP-TOP," in *2016 IEEE International Conference on Image Processing (ICIP)*, 2016.
[48] F. Y. Yuming Li, Lai-Man Po , Xuyuan Xu, Litong Feng, "Face liveness detection and recognition using shearlet based feature descriptors," *ICASSP*, pp. 874–877, 2016.
[49] R. Raghavendra, K. B. Raja, and C. Busch, "Detecting morphed face images," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*, 2016.
[50] A. Agarwal, R. Singh, and M. Vatsa, "Face anti-spoofing using Haralick features," in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016*, 2016.
[51] A. Alotaibi and A. Mahmood, "Enhancing computer vision to detect face spoofing attack utilizing a single frame from a replay video attack using deep learning," in *Proceedings - 2016 International Conference on Optoelectronics and Image Processing, ICOIP 2016*, 2016, pp. 1–5.
[52] H. K. Bashier, L. S. Hoe, P. Y. Han, L. Y. Ping, and C. M. Li, "Face Spoofing Detection Using Local Graph Structure," *Int. Conf. Comput. Commun. Inf. Technol.*, pp. 14–17, 2014.
[53] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 4, pp. 746–761, 2015.
[54] J. Yang, Z. Lei, D. Yi, and S. Z. Li, "Person-Specific Face Antispoofing With Subject Domain Adaptation," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 4, pp. 797–809, 2015.
[55] D. C. Garcia and Ricardo L. de Queiroz, "Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 4, pp. 778–786, 2015.
[56] M. Waris, H. Zhang, I. Ahmad, S. Kiranyaz, and M. Gabbouj, "EUSIPCO 2013 1569744187 Analysis Of Textural Features For Face Biometric Anti-Spoofing," *EUSIPCO*, pp. 1–5, 2013.
[57] Z. Akhtar, C. Michelon, and G. L. Foresti, "Liveness detection for biometric authentication in mobile applications," in *Proceedings - International Carnahan Conference on Security Technology*, 2014, vol. 2014-Oct., no. October.

[58] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face Spoofing Detection Using Colour Texture Analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 8, pp. 1818–1830, 2016.
[59] Y. Binny Reeba and R. Shanmugalakshmi, "Spoofing face recognition," in *ICACCS 2015 - Proceedings of the 2nd International Conference on Advanced Computing and Communication Systems*, 2015, pp. 3–7.
[60] K. Patel, H. Han, and A. K. Jain, "Secure Face Unlock: Spoof Detection on Smartphones," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 10, pp. 2268–2283, 2016.
[61] D. Das and S. Chakraborty, "Face liveness detection based on frequency and micro-texture analysis," *in 2014 International Conference on Advances in Engineering and Technology Research, ICAETR 2014*, 2014, pp. 3–6.
[62] S. Parveen, S. M. S. Ahmed, N. H. Abbas, N. Naeem, and M. Hanafi, "Texture analysis using local ternary pattern for face anti-spoofing," *Sci. Int*, vol. 28, no. 2, pp. 965–971, 2016.
[63] M. Jafari Barani, K. Faez, and F. Jalili, "Implementation of Gabor Filters Combined with Binary Features for Gender Recognition," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 4, no. 1, pp. 108–115, 2014.
[64] L. Yang, "Face liveness detection by focusing on frontal faces and image backgrounds," in *International Conference on Wavelet Analysis and Pattern Recognition, 2014*, vol. 2014-Jan, pp. 93–97.
[65] W. Yin, Y. Ming, and L. Tian, "A face anti-spoofing method based on optical flow field," in *International Conference on Signal Processing Proceedings, ICSP*, 2017, pp. 1333–1337.
[66] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally efficient face spoofing detection with motion magnification," in *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, 2013, pp. 105–110.
[67] A. Anjos, M. M. Chakka, and S. Marcel, "Motion-based counter-measures to photo attacks in face recognition," no. November 2012, pp. 147–158, 2014.
[68] Y. Li, Y. Li, Q. Yan, H. Kong, and R. H. Deng, "Seeing Your Face Is Not Enough: An Inertial Sensor-Based Liveness Detection for Face Authentication," in *CCS 15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 1558–1569.
[69] J. Komulainen, A. Hadid, and M. Pietikainen, "Context based face anti-spoofing," in *IEEE 6th International Conference on Biometrics: Theory, Applications and Systems, BTAS 2013*, 2013.
[70] I. Paper and S. Z. Li, "Face Liveness Detection by Exploring Multiple Scenic Clues," *Int. Conf. Control Autom. Robot. Vis.*, vol. 2012, no. December, pp. 188–193, 2012.
[71] M. Gavrilescu, "Study on using individual differences in facial expressions for a face recognition system immune to spoofing attacks," *IET Biometrics*, vol. 5, no. 3, pp. 236–242, 2016.
[72] J. Komulainen, A. Hadid, M. Pietikainen, A. Anjos, and S. Marcel, "Complementary countermeasures for detecting scenic face spoofing attacks," in *Proceedings - 2013 International Conference on Biometrics, ICB* 2013, 2013.
[73] M. Killioğlu, M. Taşkiran, and N. Kahraman, "Anti-spoofing in face recognition with liveness detection using pupil tracking," in *SAMI 2017 - IEEE 15th International Symposium on Applied Machine Intelligence and Informatics, Proceedings*, 2017, pp. 87–92.
[74] A. Maurya and S. Tarar, "Spoofed Video Detection Using Histogram of Oriented Gradients," in *Proceedings of the Third International Symposium on Computer Vision and the Internet - VisionNet'16*, 2016, pp. 1–7.
[75] A. Ali, F. Deravi, and S. Hoque, "Liveness detection using gaze collinearity," in *Proceedings - 3rd International Conference on Emerging Security Technologies, EST 2012*, 2012, pp. 62–65.
[76] A. Ali, F. Deravi, and S. Hoque, "Directional sensitivity of gaze-collinearity features in liveness detection," in *Proceedings-2013 4th International Conference on Emerging Security Technologies, EST 2013*, 2013, pp. 8–11.
[77] A. Asaduzzaman, A. Mummidi, M. F. Mridha, and F. N. Sibai, "Improving facial recognition accuracy by applying liveness monitoring technique," in *Proceedings of 2015 3rd International Conference on Advances in Electrical Engineering, ICAEE 2015*, 2016, pp. 133–136.
[78] J. Cao, H. Li, Z. Sun, and R. He, "Accurate mouth state estimation via convolutional neural networks," in *International Conference on Digital Signal Processing, DSP*, 2017, pp. 134–138.
[79] Z. Lu, X. Wu, and R. He, "Person identification from lip texture analysis," in *International Conference on Digital Signal Processing, DSP*, 2017, pp. 472–476.
[80] A. K. Singh, P. Joshi, and G. C. Nandi, "Face recognition with liveness detection using eye and mouth movement," in *International Conference on Signal Propagation and Computer Technology (ICSPCT)*, 2014, pp. 592–597.
[81] M. De Marsico, C. Galdi, M. Nappi, and D. Riccio, "FIRME: Face and iris recognition for mobile engagement," *Image Vis. Comput.*, vol. 32, no. 12, pp. 1161–1172, 2014.
[82] A. Lagorio, M. Tistarelli, M. Cadoni, C. Fookes, and S. Sridharan, "Liveness detection based on 3D face shape analysis," in *2013 International Workshop on Biometrics and Forensics (IWBF)*, 2013, pp. 1–4.
[83] T. Wang, J. Yang, Z. Lei, S. Liao, and S. Z. Li, "Face liveness detection using 3D structure recovered from a single camera," in *Proceedings - 2013 International Conference on Biometrics, ICB 2013*, 2013.
[84] X.-J. Chai, "Pose and Illumination Invariant Face Recognition Based on 3D Face Reconstruction," *J. Softw.*, vol. 17, no. 3, pp. 525, 2006.
[85] T. Edmunds and A. Caplier, "Fake face detection based on radiometric distortions," in *2016 6th International Conference on Image Processing Theory, Tools and Applications, IPTA 2016*, 2017.
[86] W. Kim, S. Suh, and J. Han, "Face Liveness Detection From a Single Image via Diffusion Speed Model," *IEEE Trans. Image Process.*, vol. 24, no. 8, pp. 2456–2465, 2015.
[87] A. Pinto, S. Member, H. Pedrini, and S. Member, "Face Spoofing Detection Through Visual Codebooks of Spectral Temporal Cubes," vol. X, no. December, pp. 1–15, 2015.

[88] Y. Wang, X. Hao, Y. Hou, and C. Guo, "A New Multispectral Method for Face Liveness Detection," *2013 Second IAPR Asian Conference on Pattern Recognition*, 2013, pp. 922–926.
[89] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. S. Ho, "Detection of Face Spoofing Using Visual Dynamics," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 762–777, 2015.
[90] H. Steiner, A. Kolb, and N. Jung, "Reliable face anti-spoofing using multispectral SWIR imaging," *in 2016 International Conference on Biometrics, ICB 2016*, 2016.

BIOGRAPHIES OF AUTHORS

Enas Akeel Raheem received B.Sc. from Computer Engineering Department, University of Technology,10001, Baghdad, Iraq, Works as a tutor in same department. Currently M.Sc. graduate Student in Department of Computer and Communication Systems, Faculty of Engineering, Universiti Putra Malaysia (UPM).

Assoc. Prof. Dr. Sharifah Mumtazah bt Syed Ahmad Abdul Rahman received PhD, M.sc And B.sc from University of Kent, UK. Currently works as (Assoc. Prof. Dr.) and Postgraduate Coordinator in Department Computer & Communication Systems Engineering.Faculty of Engineering, Universiti Putra Malaysia 43400 UPM-Serdang, MALAYSIA
E-mail: s_mumtazah@eng.upm.edu.my

Assoc. Prof. Dr. Wan Azizun Binti Wan Adnan received Ph.D. and M. Sc from University of Malaya, Malaysia. B.Sc. from Southampton University, Southampton, England. PgDip in Software Development from University of Northambria, Newcastle Upon Tyne, England. Currently works as (Assoc. Prof. Dr.) in Department of Computer and Communication Engineering, Universiti Putra Malaysia 43400 UPM-Serdang MALAYSIA
E-mail: wawa@eng.upm.edu.my