IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11387

Face Biometric Antispoofing Methods: A Survey

Priyanka S Shivol[1], Sampada H. K[2], Shamitha K. J[3], Saba Khan[4], Dr. Raghavendra R. J[5]

U. G Student, Department of Information Science and Engineering, J N N College of Engineering, Shimoga, India[1,2,3,4]

Associate Professor, Department of Information Science and Engineering, J N N College of Engineering, Shimoga, India[5]

Abstract: Face anti-spoofing is widely used as a biometric approach. The face anti-spoofing systems are increasing due to their advantage of being convenient and contactless compared with other authentication systems. Unfortunately, the face anti-spoofing system is the most vulnerable to spoofing attacks. Hence, the need for the development of countermeasures against such presentation attacks. This paper provides detailed reviews of the different techniques available in face anti-spoofing systems. We give an outline of the research that has been accomplished in the field of face anti-spoofing.

Keywords: Face anti-spoofing, Face recognition, Presentation attack, Convolution neural network, Texture analysis, Information Security.

I. INTRODUCTION

Facial recognition has simplified many processes which were earlier difficult with added security [1]. Even though facial recognition technologies have many advantages, they have their share of drawbacks [2]. Nowadays, biometric systems are broadly used in day-to-day applications including mobile authentication and access control. However, Presentation Attacks (PA) are a big threat to these applications as an unauthorized user can use a photo of the valid user to invade a system. In order to overcome presentation attacks, the system comprises a face anti-spoofing approach. Past few years, face anti-spoofing has attracted a lot of researchers. A high-security requirement is needed for strengthening face recognition systems which is essential to prevent the vulnerability from face spoofing. Spoofing involves an attacker who deceits as a legitimate user to gain the access to a system. There are many other alternatives that have been recognized over the years, such as iris [3], voice [4], fingerprint [5], and handwriting signatures [6]. Among these, face recognition has become a better alternative [7].

Meanwhile, many software-based and hardware-based face anti-spoofing detection systems have been designed. An example of a software-based approach where the real-time liveness detection against a photo attack can be detected by recognizing spontaneous eyeblinks which do not require extra hardware. It is much easier for attackers to obtain photos, videos, or use silicon masks [8].

Nowadays, the face recognition system has become a target of spoof attacks due to the increasing easy accessibility of face modalities [9][10]. This type of security threat can be easily carried out by presenting a face artifact [11]. Deep learning-based face Anti-Spoofing techniques have shown remarkable performance.

The next sections are organized as follows. Section 2 presents some hand-crafted anti-spoofing approaches and some methods for categorization. In section 3 provides a overview of different research works in face anti-spoofing. Section 4 gives a summary the paper.

II. STATE OF THE ART APPROACH

Facial recognition has become the second-largest biometric authentication technique that is used after fingerprint [12]. Nowadays face recognition is being used by many companies in their devices, such as face-ID verification. Even though face recognition has shown promising results in security systems, there is still a need for countermeasures for presentation attack detection (PAD).

There are many face presentation attack types, such as photo attack, video attack, and mask attack. Photo attack [13] is where an unauthorized user prints the photo of an authorized useron a paper and presents it to the verification system. In the video attacks [14], video acquisition of users from social media or even using a hidden camera are used as spoof against the system. In a mask attack [15], a 3D face mask is used as a spoof against a system.Further, PAD can be divided into hardware and software-based approaches as shown in Fig 1, which we discussed in detail in the below sections.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 3, March 2022

DOI: 10.17148/IJARCCE.2022.11387

A. Hardware-Based Approach

This approach inspects the features of the face using hardware. It also requires user cooperation where they need to associate with the hardware or sensor. Further, this method can be categorized into Sensor Characteristics, Blink detection and Challenge Response.

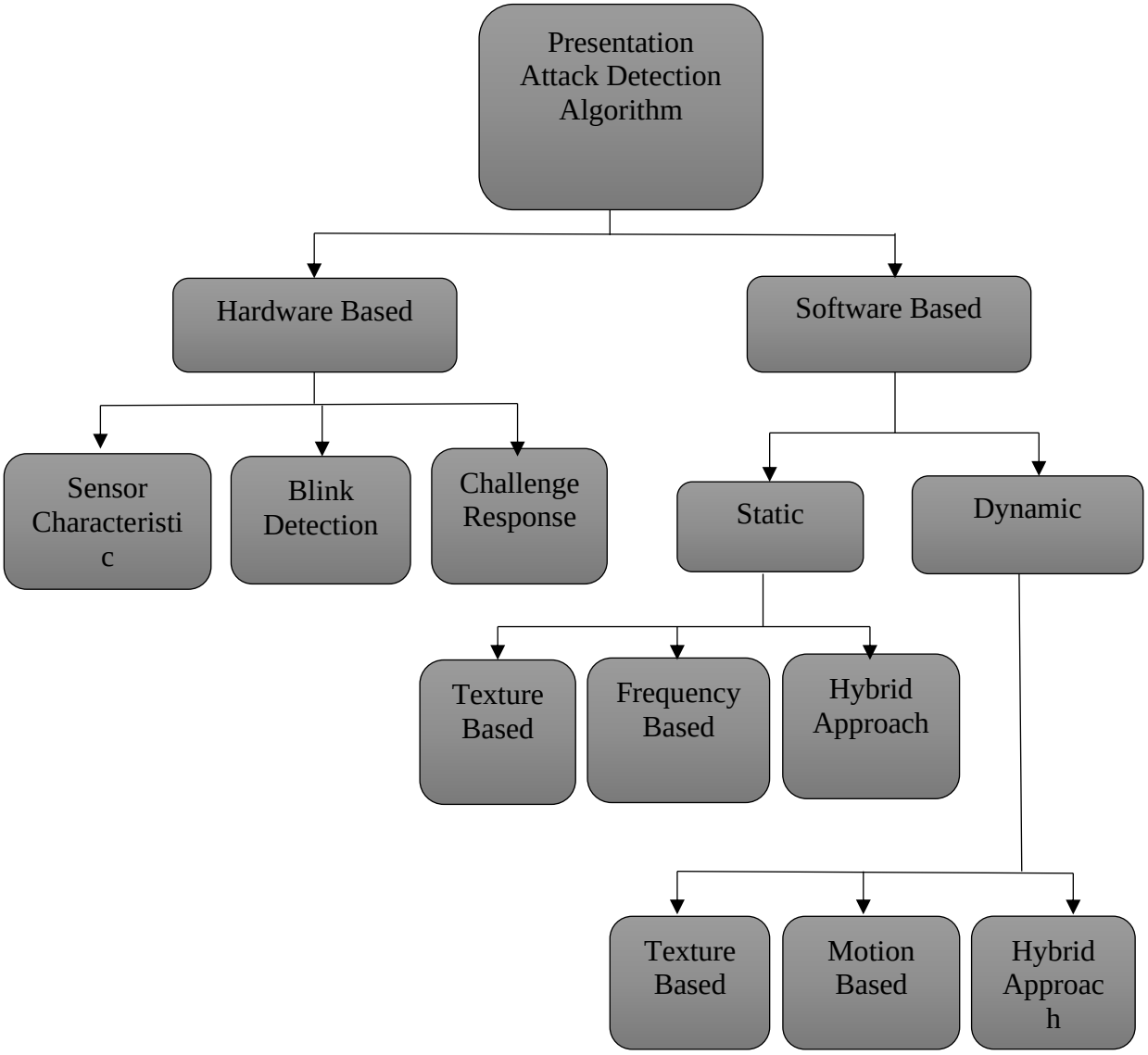

Fig 1: Categorization of face presentation attack detection algorithm

1) Sensor Characteristics:

The features explored from the camera rely on the type of sensor used, such as light field camera [16] where the variation of the focus is measured. The LFC camera characteristic was explored with the capacity to detect photo and display attacks or gauging the reflectance from a near multi-spectral [17] sensor. This measures the reflectance in a 3D scan.

2) Blink detection:

Using blink detection presentation attacks can be reduced. This method detects the blinking action observed in the eye region using hardware [18] or software-based techniques [19]. When compared to other regions maximum movement is

Impact Factor 7.39 ⁜ Vol. 11, Issue 1, January 2022

DOI: 10.17148/IJARCCE.2022.11108

detected in the eye region [20]. Hence blink detection can be used to detect a presentation attack.

3) Challenge Response:

The main intent of this method is to record the response to a challenge in the provided user interface, such as by tracking the response of the user towards a preset stimulus [21]. An approach by Smith et al. [22] used this method to counter video replay attack.

B. Software-Based Approaches

This technique uses an algorithm that determines whether a captured face image is either genuine or spoof. This technique has proven to have high precision and lower price. The software-based approach does not require user involvement as compared to hardware-based approach and it also prevents the need for hardware. They can be divided into two types: static methods and dynamic methods.

1) Static Methods:

These methods analyze an individual image and also a video sequence, where every frame is evaluated separately. They are faster when compared with dynamic methods. Static methods have three types namely: texture-based approach, frequency-based approach and hybrid approaches.

Texture Based Approach: In texture-based approaches, micro-textural outlines in the face image are evaluated. This method is efficient in differentiating photos and artifact. One example of a texture-based approach uses Local Binary Patterns (LBP) [23]. In another illustration, where the features are extracted from the image using Quaternionic Local Ranking Binary Patter and evaluated using two different classifiers, namely the KNN and the SVM [24]. Raghavendra et al. [25-29] proposed more innovative feature descriptors such as ELTCP, DOG-ADTCP and EDDTCP for face anti-spoofing.

Frequency Based Approach: Fourier spectrum analysis [30] was the first work in this category. This analysis can be applied to detect video replay attacks by calculating the Fourier spectra for head hair [31]. Frequency component can be estimated using Discrete Cosine Transforms (DCT) [31], DoG filters [33] and high-frequency components [34].

Hybrid Approach: Hybrid methods integrate more than one trait [35] such as time-frequency information with a texture descriptor [36], shape and texture [37] or the use of contextual information [38].

2) Dynamic Method:

These methods detect presentation attacks by analyzing the motion. The analysis includes tracing any indication of life, such as continuous movement of eye, facial expressionsor head movements [39]. In this method, a certain degree of motion should be observed in the head region or between the head and the background [40]. As this method requires more time to analyze a video some of these techniques cannot be applied where there are time constraints.

III. FACE ANTI-SPOOFING APPROACHES

Researchers have proposed many methods to counter face-spoofing. One cannot select a particular technique to defend against all presentation attacks. By combining other algorithms best outcomes can be obtained, where the weaknesses of some are covered by the strengths of others and vice-versa. There are three types of face anti-spoofing: i) sensor level approach ii) feature level approach iii) score level approach.

A. Sensor-Level Approach

Sensor level approach also referred as hardware-based approach, is a technique that tracks specific characteristics of a human using a hardware or sensor [41], which helps us to detect a spoof.
These methods measure some features, such as (i) innate properties of a living body [42], (ii) reflex of a living body such as pulse [43], blood pressure (BP) [44] and brain wave signals (EEG) [45]; (iii) challenge-response [46].

Impact Factor 7.39 ⁜ Vol. 11, Issue 1, January 2022

DOI: 10.17148/IJARCCE.2022.11108

Some of the notable approaches by researchers are: a dual-band fusion system by Pavlidis et al. [47] which demonstrates that more precise human face segments can be done using a near-infrared band rather than a conventional visible band. Another approach by Marcel et al. [42] used the multispectral face sensor for liveness detection. In 2007, to exploit intrinsic features which are under the skin, Buddharaju et al. [48] developed a system based on using the bio-heat information contained in heat imagery.

B. Feature-Level Approach

The feature-level approach is a software-based technique. In this, the features used to detect a spoof face are extracted from the biometric sample, and not from the human body. This method is broadly divided into static and dynamic methods based on whether they analyze an image or a video.

1) Feature Level Static Approach:

The feature level static approaches uses a person's image, a method by Galbally [49] uses 14 image quality characteristics extracted from an image to differentiate between bona-fide and imposter samples. Another illustration by Chang et al. [50] where the features from the image are divided into three models: generalized Gaussian density-based, asymmetric generalized Gaussian density-based, and top gradient similarity deviation features.

2) Feature Level Dynamic Approach:

Feature level dynamic approach uses many publicly available face anti-spoofing databases such as Reply-Attack database, CASIA, NUUA, MSU-MFSD datasets. Alotaibi et al. [51] proposed a method which uses deep convolution neural network (CNN) to extract complex and high characteristics of the input diffused frame. Xiaobai et al. [52] proposed a method in which spoof is detected using a pulse from a video. Since plus signals are not present in mask or printed photos, this can be an efficient method. Chen et al. [53] proposed a method which explores differences between multi-modal cameras and construct a cross-domain multi-modal face anti-spoofing dataset under surveillance scenarios called GREAT-FASD-S.

C. Score-Level Approach

A third type of protection method is score-level approach. It aims to focuses on the study of fusion methods that enhance their performance against presentation attacks.

Shifeng et al. [54] proposed an approach to select the more informative channel feature by re-weighting the modality-dependent features and also suppressing less informative ones. Another demonstration by Nguyen et al. [55] uses the concept of Dempster-Shafer theory to upgrade the working of multi-biometric systems. In 2018, a secure multimodal biometric system was proposed depending on different fusion levels by Hammad et al. [56], that uses CNN and Q-Gaussian multi-support vector machine.

IV. CONCLUSION

Many methods have been designed to safeguard the authentication system against presentation attacks. A great amount of research has ben carried out concerning the vulnerabilities of biometric systems to spoofing attacks and multiple approaches to secure them against this threat have been proposed. Moreover, various independent evaluations have shown that some of these protection approaches are able to achieve very competitive results.

Although substantial work has been done in the face spoofing detection and many advances have been reached, attacking approaches have also evolved becoming more and more sophisticated. Even though advanced methods have been designed for spoof detection, direct attack methods have also evolved. As a result, there are huge challenges to be confronted in the safety of direct attack, which in the near future will lead to a more secure authentication system.

REFERENCES

[1] Ane C., Iwan S., Gunawan D., "Face Anti-spoofing Method based on Quaternionic Local Ranking Binary Pattern Features", in proceeding of International Conference on Signals and Systems, pp. 92-97, 2018.

DOI: 10.17148/IJARCCE.2022.11108

[2] R. Raghavendra, K. B. Raja and C. Busch, "Presentation Attack Detection for Face Recognition Using Light Field Camera," in Journal of Image Processing, vol. 24, no. 3, pp. 1060-1075, 2015.

[3] M. Ren, C. Wang, Y. Wang, Z. Sun and T. Tan, "Alignment Free and Distortion Robust Iris Recognition," in proceedings of International Conference on Biometrics (ICB), pp. 1-7, 2019.

[4] C. Zhang, M. Yu, C. Weng and D. Yu, "Towards Robust Speaker Verification with Target Speaker Enhancement," in proceedings of International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6693-6697, 2021.

[5] N. Shuping and W. Feng, "The research on fingerprint recognition algorithm fused with deep learning," in proceedings of International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA), pp. 1044-1047, 2020.

[6] H. Pham et al., "Robust Handwriting Recognition with Limited and Noisy Data," in proceedings of International Conference on Frontiers in Handwriting Recognition (ICFHR), pp. 301-306, 2020.

[7] J. Yu, Y. Zhao, S. Zhu, A. Wang and Y. Wang, "A Bibliometric Analysis on Face Recognition Technology Research," in proceedings of International Conference of Safety Produce Information (IICSPI), pp. 755-759, 2018.

[8] Guangcheng W., Zhongyuan W., Kui J., Baojin H., Zheng H., Ruimin H., "Silicone mask face anti-spoofing detection based on visual saliency and facial motion", in Journal of Neurocomputing, vol. 458, pp. 416-427, 2021.

[9] T. Dee, I. Richardson and A. Tyagi, "Continuous Transparent Mobile Device Touchscreen Soft Keyboard Biometric Authentication," in proceedings of International Conference on VLSI Design and International Conference on Embedded Systems (VLSID), pp. 539-540, 2019.

[10] I. Chingovska et al., ‘‘The 2nd competition on counter measures to 2D face spoofing attacks,’’ in Proc. IAPR Int. Conf. Biometrics (ICB),Jun. 2013, pp. 1–6.

[11] M. M. Chakka et al., ‘‘Competition on counter measures to 2-D facial spoofing attacks,’’ in Proc. IEEE Int. Joint Conf. Biometrics (IJCB),Oct. 2011, pp. 1–6.

[12] P. Coli, G. L. Marcialis, and F. Roli, ‘‘Fingerprint silicon replicas: Static and dynamic features for vitality detection using an optical capture device,’’ Int. J. Image Graph., vol. 8, pp. 495–512, Jan. 2008.

[13] G. D. Simanjuntak, K. N. Ramadhani, A. Arifianto, "Face Spoofing Detection using Color Distortion Features and Principal Component Analysis," in proceedings of International Conference on Information and Communication Technology, pp. 1-5, 2019.

[14] H. E. Utami, H. Nugroho, "Face Spoof Detection by Motion Analysis on the Whole Video Frames," in proceedings of International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering, pp. 213-218, 2017.

[15] S. Chen, W. Li, H. Yang, D. Huang and Y. Wang, "3D Face Mask Anti-spoofing via Deep Fusion of Dynamic Texture and Shape Clues," in proceedings of International Conference on Automatic Face and Gesture Recognition, pp. 314-321, 2020.

[16] V. Chiesa and J. Dugelay, "Advanced Face Presentation Attack Detection on Light Field Database," in proceeding of International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1-4,2018.

[17] H. Steiner, A. Kolb and N. Jung, "Reliable face anti-spoofing using multispectral SWIR imaging,"in proceeding of International Conference on Biometrics (ICB),pp. 1-8,2016.

[18] R, Hammoud, “Passive eye monitoring: Algorithms, applications and experiments” Springer Science & Business Media, 2008.

[19] P. Gang, S. Lin, W. Zhaohui, and L. Shihong, “Eyeblink-based Anti-Spoofing in Face Recognition from a Generic Webcamera” in proceedings of International Conference, 2008.

[20] A. Nema, "Ameliorated Anti-Spoofing Application for PCs with Users’ Liveness Detection Using Blink Count," in preceedings of International Conference on Computational Performance Evaluation (ComPE), 2020.

[21] Ali. Ali, Farzin. Deravi, and S. Hoque, “Directional Sensitivity of Gaze-Collinearity Features in Liveness Detection” in proceeding of International Conference on Emerging Security Technologies, 2013.

[22] D. Smith, A. Wiliem, and B. Lovell “Face Recognition on Consumer Devices: Reflections on Replay Attacks”, 2015.

[23] Wanling Z., Shijum X., "Face anti-spoofing detection based on DWT-LBP-DCT features", in Journal of Signal Processing, vol. 89, 2020.

[24] Ane C., Iwan S., Gunawan D., "Face Anti-spoofing Method based on Quaternionic Local Ranking Binary

DOI: 10.17148/IJARCCE.2022.11108

Pattern Features", in proceeding of International Conference on Signals and Systems, pp. 92-97, 2018.

[25] Raghavendra, R. J., & Kunte, R. S, " Extended Local Ternary Co-relation Pattern: A novel feature descriptor for face Anti-spoofing", in *Journal of Information Security and Applications*, vol. 52, pp. 1-10, 2020

[26] Raghavendra, R. J., & Kunte, R. S, " A Novel Feature Descriptor for Face Anti-Spoofing using Texture Based Method", in *International Journal of Cybernetics and Information Technologies*, vol. 20, pp. 159-176, 2020.

[27] Raghavendra, R. J., & Kunte, R. S, " Extended Local Ternary Pattern for Face Anti-Spoofing", in Proceedings of *International Conference on Advances in Cybernetics, Cognition and Machine Learning for Communication Technologies*, Springer, vol. 643, pp. 221-229, 2020.

[28] Raghavendra, R. J., and Kunte, R. S., " Anisotropic Smoothing for Illumination Invariant Face Anti-spoofing", in Proceedings of *IEEE International Conference on Trends in Electronics and Informatics*, pp. 901-905, 2020.

[29] Raghavendra, R. J., & Kunte, "DOG-ADTCP: A new feature descriptor for protection of face identification system", in Journal of Expert Systems with Applications, vol. 201, pp. 1-16, 2022.

[30] J. Li, Y. Wang, T. Tan, and A. K. Jain, "Live face detection based on the analysis of Fourier spectra", 2004.

[31] L. Weiwen, "Face liveness detection using analysis of Fourier spectra based on hair" in proceedings of International Conference on Wavelet Analysis and Pattern Recognition pp. 75–80, 2014.

[32] M.H. Teja, "Real-time live face detection using face template matching and DCT energy analysis" in proceedings of International Conference on Soft Computing and Pattern Recognition pp. 342–346, 2011.

[33] Z. Zhang, J. Yan, S. Liu, Z. Lei, D. Yi, S.Z. Li, "A face anti-spoofing database with diverse attacks." in proceedings of International Conference on Biometrics, 2012.

[34] J. Peng and P.P.K. Chan, "Face liveness detection for combating the spoofing attack in face recognition" in proceedings of International Conference on Wavelet Analysis and Pattern Recognition, pp. 176–181, 2014.

[35] J. Galbally, S. Marcel, and J. Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition", pp. 710–724, 2014.

[36] R. Raghavendra, C. Busch, "Novel presentation attack detection algorithm for face recognition system: Application to 3D face mask attack", pp. 323–327, 2014.

[37] J. Maatta, A. Hadid, M. Pietikainen, "Face spoofing detection from single images using texture and local shape analysis", Biometrics, pp. 3–10, 2012.

[38] J. Komulainen, A. Hadid, and M. Pietikainen, "Context based face anti-spoofing", pp.1–8, 2013.

[39] K. Kollreider, H. Fronthaler, M. Faraj, and J. Bigun, "Real-Time Face Detection and Motion Analysis With Application in Liveness Assessment" in journal of Information Forensics and Security 2, 3 , pp.548–558,2007.

[40] M. De Marsico, M. Nappi, D. Riccio, and J. Dugelay, "Moving face spoofing detection via 3D projective invariants" in proceedings of 5th IAPR International Conference on Biomet- (ICB), 73–78,2012.

[41] Baldisserra, Denis, Franco, Annalisa, Maio, Dario, Maltoni, Davide, "Fake Fingerprint Detection by Odor Analysis ", Springer, 2005.

[42] S. Marcel, M. S. Nixon, J. Fierrez, N. Evans, "Handbook of Biometric Anti-Spoofing", 2nd Edition, Springer, 2019.

[43] Liu, Siqi,Yuen, Pong C., Zhang, Shengping, Zhao, Guoying, "3D Mask Face Anti-spoofing with Remote Photoplethysmography", 2016.

[44] M. Drahansky, R. Notzel and W. Funk, "Liveness Detection based on Fine Movements of the Fingertip Surface", in proceedings of IEEE Information Assurance Workshop, pp. 42-47, 2016.

[45] F. S. Liwen, X. A. Cai and J. Ma, "A dual-biometric-modality identification system based on fingerprint and EEG," in proceedings of International Conference on Biometrics: Theory, Applications and Systems (BTAS), pp. 1-6, 2010.

[46] J. Galbally, S. Marcel and J. Fierrez, "Biometric Anti-spoofing Methods: A Survey in Face Recognition," in IEEE Access, vol. 2, pp. 1530-1552, 2014.

[47] I. Pavlidis and P. Symosek, ''The imaging issue in an automatic face/disguise detection system,'' in Proc. IEEE Workshop Comput. Vis.Beyond Vis. Spectr., Methods Appl., Jun. 2000, pp. 15–24.

[48] P. Buddharaju, I. T. Pavlidis, P. Tsiamyrtzis, and M. Bazakos,''Physiology-based face recognition in the thermal infrared spectrum'', IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 613–626, Apr. 2007.

[49] J. Galbally and S. Marcel, "Face Anti-spoofing Based on General Image Quality Assessment," in proceedings of International Conference on Pattern Recognition, pp. 1173-1178,2014.

DOI: 10.17148/IJARCCE.2022.11108

[50] H. Chang and C. Hsiao Yeh, "Face anti-spoofing detection based on multi-scale image quality assessment", in proceedings of Image and Vision Computing, vol.121 pp. 104428, 2022.

[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 proceeding of *International Conference on Optoelectronics and Image Processing (ICOIP)*, pp. 1-5,2016.

[52] Xiaobai Li, J. Komulainen, G. Zhao, Pong-Chi Yuen and M. Pietikäinen, "Generalized face anti-spoofing by detecting pulse from face videos" *in proceeding of International Conference on Pattern Recognition (ICPR)*, pp. 4244-4249, 2016.

[53] X. Chen, S. Xu, Q. Ji and S. Cao, "A Dataset and Benchmark Towards Multi-Modal Face Anti-Spoofing Under Surveillance Scenarios", vol. 9, pp. 28140-28155, 2021.

[54] Shifeng Z., Ajian L., Jun W., Yanyan L., Guodong G., Sergio E., Hugo Jair E., and Stan Z. Li, "CASIA-SURF: A Large-Scale Multi-Modal Benchmark for Face Anti-Spoofing", in Journal of Biometrics, Behavior, and Identity Science, vol. 2, pp. 182-193, 2020.

[55] K. Nguyen, S. Denman, S. Sridharan, and C. Fookes, "Score-level multibiometric fusion based on dempster–shafer theory incorporating uncertainty factors," IEEE Transactions on Human-Machine Systems, vol. 45, no. 1, 2015.

[56] M. Hammad, Y. Liu, and K. Wang, "Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint," IEEE Access, vol. 7, pp. 26527–26542, 2019.

BIOGRAPHY

Dr. Raghavendra R. J. received a B.E. degree in Computer Science and Engineering from Kuvempu University in 1996 and M.Sc(Engg) by Research degree in Computer Science Engineering from Visvesveraya Technological University (VTU), Belgavi in 2008. He has been awarded a Ph.D. degree in Computer Science and Engineering from VTU, Belgavi in 2021.

Since 2011, he has been an Associate Professor in the Information Science Engineering Department, JNNCE, Shimoga, Karnataka, India. He has published many technical papers in reputed journals. His research interests include Face Anti-spoofing, Biometrics, Information security and Computer Vision.