International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.9756/INTJECSE/V14I5.429 ISSN: 1308-5581 Vol 14, Issue 05 2022

# ROBUST FACE ANTI-SPOOFING DETECTION SYSTEM: AN REVIEW

***Avinash Bajirao Lambat ,**Dr. R. J. Bhiwani**
*Research Scholar, Department of Electronics & Telecommunication Engineering, BabasahebNaik College of Engg ,Pusad
**Professor & Head, Department of Electronics & Telecommunication Engineering, BabasahebNaik College of Engg ,Pusad

**Abstract**
Automatically recognising people by their biometric characteristics is a well-established research area. Biometric systems are vulnerable to many different types of presentation attacks made by persons showing photo, video, or mask to spoof the real identity. This study introduces a novel approach to detect face-spoofing, by extracting the local features local binary pattern (LBP) and simplified weber local descriptor (SWLD) encoded convolutional neural network (CNN) models, WLD and LBP features are combined together to ensure the preservation of the local intensity information and the orientations of the edges. These two components are complementary to each other. Specifically, differential excitation preserves the local intensity information but omits the orientations of edges. On the contrary, LBP describes the orientations of the edges but ignore the intensity information, the proposed approach presents a very low degree of complexity which makes it suitable for real-time applications, Finally, a non-linear support vector machine (SVM) classifier with kernel function was used for determining whether the input image corresponds to a live face or not. Authors' experimental analysis on two publicly available databases REPLAY-ATTACK and CASIA face anti-spoofing showed that their approach performs better than state-of-the-art techniques following the provided evaluation protocols of each database.
Keyword-

## Introduction

The performance of face recognition systems has been improved over the last decade but presentation attacks called spoofing have imposed a challenge on researchers to develop a robust face detection system. Literature shows different standard datasets being used for evaluating the performance of their proposed system. Bio-metrics is the giant in utilizing physiological characteristics, such as fingerprint, face, and iris, or behavioural characteristics, such as typing rhythm and gait, that uniquely identify or authenticate an individual. As biometric systems are widely used in real-world applications including mobile phone authentication and access control, biometric spoof attacks are becoming a larger threat, where a spoofed biometric sample is presented to the biometric system and attempted to be authenticated. Facial spoof attack is a process in which a fraudulent user can subvert or attack a face recognition system by masquerading as a registered user and thereby gaining illegitimate access and advantages. A spoofing attack is an attempt to acquire someone else's privileges or access rights by using a photo, video or a different substitute for an authorized person's face.

- Print attack: The attacker uses someone's photo. The image is printed or displayed on a digital device. This is the most common type of attack since most people have facial pictures available on the internet or photos could be obtained without any permission.
- Eye-cut photo attack: Eye regions of a printed photo are cut off to exhibit blink behaviour of the impostor.
- Warped photo attack: It consist in bending a printed photo in any direction to simulate facial motion.


Figure 1 - Photo attacks

- Replay/video attack: A more sophisticated way to trick the system, which usually requires a looped video of a victim‟s face. This approach ensures behaviour and facial movements to look more „natural‟ compared to holding someone‟s photo. This type has physiological signs of life that are not presented in photos, such as eye blinking, facial expressions, and movements in the head and mouth, and it can be easily performed using tablets or large smartphones.
- 3D mask attack: During this type of attack, a mask is used as the tool of choice for spoofing. It‟s an even more sophisticated attack than playing a face video. In addition to natural facial movements, it enables ways to deceive some extra layers of protection such as depth sensors. These attacks are addressed to anti-spoofing systems that analyse 3D face structures, being one of the most complex attacks to be detected. This has been classified as life-size wearable mask and paper cut mask.

Figure 2 - Life-size wearable mask

Figure 3 - Paper cut mask 3


Figure 4 - Attacks

Generally, face spoofing classification can be expressed as follows as presented by researchers.

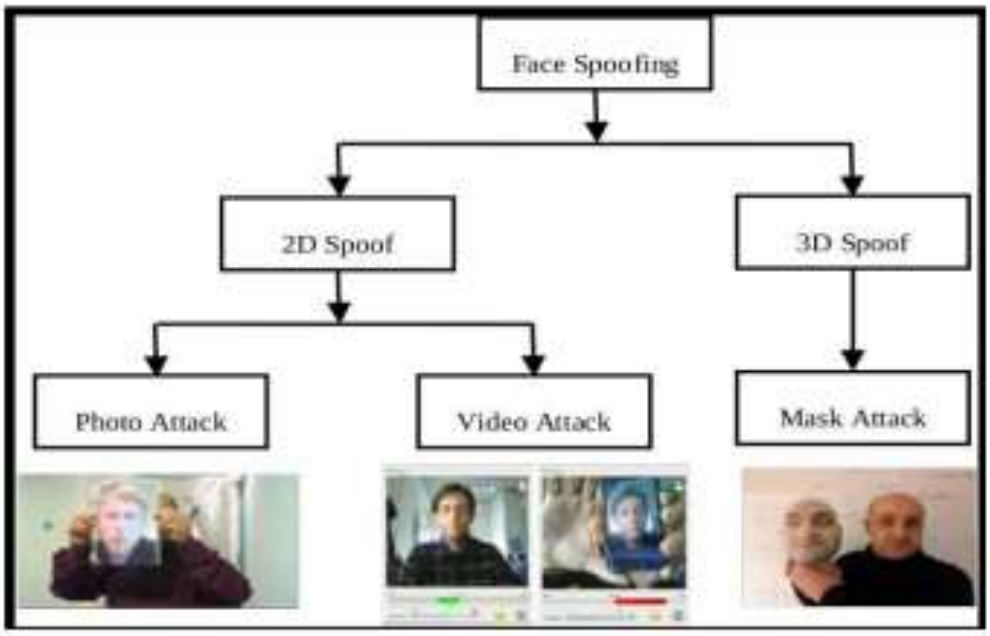


Figure 5 - Face spoofing methods classification

**Literature Reviews**

The work proposed in [15] tackles the zero-shot face antispoofing problem among 13 types of spoof attacks. The proposed method leverages a deep tree network to route the unknown attacks to the most proper leaf node for spoof detection. The tree is trained in an unsupervised fashion to find the feature base with the largest variation to split the spoof data. They collected SiW-M dataset that contained more subjects and spoof types than any previous databases. Finally, they experimentally showed superior performance of their proposed method.

Authors in [16] proposed a simple yet effective Total Pairwise Confusion (TPC) loss for Convolutional Neural Network(CNN) training, which enhances the generalizability of the learned Presentation Attack (PA) representations. Then they incorporated a Fast Domain Adaptation (FDA) component into the CNN model to alleviate negative effects brought by domain changes. Besides, their proposed model, which is named Generalizable Face Authentication CNN (GFA-CNN), works in a multi-task manner, performing face anti-spoofing and face recognition simultaneously. Experimental results show that GFA-CNN outperforms previous face anti-spoofing approaches and also well preserves the identity information of input face images. In order to learn more generalizable PA representations for face antispoofing, they proposed a novel TPC loss to balance the contribution of each spoof 7 pattern, preventing the PA representations from overfitting to dataset-specific spoof patterns. The FDA was also incorporated into their framework to reduce distribution dissimilarity of face samples from different domains, further enhancing the robustness of PA representations.

The work in [17] casts face anti-spoofing as a domain generalization problem, and attempts to address this problem by developing a new meta-learning framework called Regularized Fine-grained Meta-learning to further enhance the generalization ability of their model. The proposed framework adopts a fine-grained learning strategy that simultaneously conducts meta-learning in a variety of domain shift scenarios in each iteration. The proposed framework conducts meta-learning in the feature space regularized by the domain knowledge supervision. In this way, bettergeneralized learning information for face antispoofing can be meta-learned. Besides, a fine-grained learning strategy is adopted which enables a variety of domain shift scenarios to be simultaneously exploited for meta learning so that their model can be trained to generalize well to unseen attacks of various scenarios.

Peng Zhang et. Al. [18] proposed an extremelite network architecture (Feather Net A/B) with Streaming module, to achieve a well trade-off between performance and computational complexity for multi-modal face anti-spoofing. Furthermore, a novel fusion classifier with “ensemble + cascade” structure is proposed for the performance preferred use cases. Meanwhile, Multi-Modal Face Presentation Attack Detection (MMFD) dataset was collected to provide more diverse samples and more attacks to gain better generalization ability.

The work carried in [19] suggested a multi-channel face antispoofing solution, being motivated by the need of high security Presentation Attack Detection (PAD) systems, capable of dealing with challenging attacks, such as 3D and partial Presentation Attack Instruments (PAIs). The work introduced a number of novelties. First, a CNNbased Multichannel (MC) face PAD algorithm, which is decomposed into a set of encoders, processing

individual MC facial regions, and an Multi-layer Perceptron (MLP), categorizing latent encodings into real or attacks classes. Second, CNN decomposition allows us to introduce a special training procedure, transferring the knowledge of facial appearance from RGB to multichannel domain. Domain adaptation is done via autoencoders, which are first pre-trained on a large set of RGB 8 facial data from CelebFaces Attributes Dataset (CelebA), and are then partially finetuned on the Balck& White – Near Infrared – Depth (BW-NIR-D) data from Wide Multi-channel Presentation Attack database (WMCADB). Third, they demonstrated that learning the features of individual facial regions, is more discriminative than the features learned from an entire face. Successful large-scale training of CNNs from synthetically generated spoof data was proposed in [20]. For the data imbalance brought by the spoof data, the authors exploited two methods for balancing it: balanced sampling and adding external live samples. Experimental results showed that their synthetic spoof data and data balancing methods greatly promote the performance for face anti-spoofing. They presented a method to synthesize virtual spoof data in 3D space to alleviate this problem. Specifically, they considered a printed photo as a flat surface and mesh it into a 3D object, which is then randomly bent and rotated in 3D space. Afterward, the transformed 3D photo is rendered through perspective projection as a virtual sample. The synthetic virtual samples can significantly boost the anti-spoofing performance when combined with a proposed data balancing strategy.

The work in [21] proposed a novel two-stream CNN-based approach for face antispoofing, by extracting the local features and holistic depth maps from the face images. The local features facilitate CNN to discriminate the spoof patches independent of the spatial face areas. On the other hand, holistic depth map examines whether the input image has a face-like depth. The first CNN stream is based on patch appearance extracted from face regions. This stream demonstrates its robustness across all presentation attacks, especially on lower-resolution face images. The second CNN stream is based on face depth estimation using the full-face image. The experiments of this CNN show that our depth estimation can achieve promising results specifically on higher-resolution images.

The importance of data and the necessity of fair evaluation methodologies to improve the generalization of existing face-PAD methods was listed in [22]. They presented a new open source evaluation framework to study the generalization capacity of face PAD methods, coined here as face-GPAD. This framework facilitates the creation of new protocols focused on the generalization problem establishing fair procedures of evaluation and comparison between PAD solutions. The authors also introduced a 9 large aggregated and categorized dataset to address the problem of incompatibility between publicly available datasets. Finally, a benchmark adding two novel evaluation protocols: one for measuring the effect introduced by the variations in face resolution, and the second for evaluating the influence of adversarial operating conditions was proposed.

The work in [23] introduced a Convolutional Neural Network (CNN) based framework for presentation attack detection, with deep pixel-wise supervision. The framework uses only frame level information making it suitable for deployment in smart devices with minimal computational and time overhead. They demonstrated the effectiveness of the proposed approach in public datasets for both intra as well as cross dataset experiments. Liveness assurance of the face using real depth technique is rarely used in biometric devices and in the literature, even with the availability of depth datasets. Therefore, this technique of employing 3D cameras for liveness of face authentication is underexplored for its vulnerabilities to spoofing attacks.

The research in [24] reviewed the literature on this aspect and then evaluated the liveness detection to suggest solutions that account for the weaknesses found in detecting spoofing attacks. They conducted a proof-of-concept study to assess the liveness detection of 3D cameras in three devices, where the results show that having more flexibility resulted in achieving a higher rate in detecting spoofing attacks. None the less, it was found that selecting a wide depth range of the 3D camera is important for anti-spoofing security recognition systems such as surveillance cameras used in airports. Therefore, to utilise the depth information and implement techniques that detect faces regardless of the distance, a 3D camera with long maximum depth range (e.g., 20 m) and highresolution stereo cameras could be selected, which can have a positive impact on accuracy.

The proposed scheme in [25] is two-fold: Tier I integrate fingerprint, palm vein print and face recognition to match with the corresponding databases, and Tier II uses fingerprint, palm vein print and face anti-spoofing convolutional neural networks (CNN) based models to detect spoofing. In first stage, the hash of a fingerprint is compared with the fingerprint database. After a successful match of the fingerprint, it is tested on a CNN-based model of the fingerprint to verify whether it is a spoof or 10 real. A similar process is repeated for the palm and face, and based on collective evidence, the system permits the user to login the system.

A CNN-RNN (Reccurent Neural Networks) model is learned to estimate the face depth with pixel-wise supervision, and to estimate rPPG signals with sequence-wise supervision. The estimated depth and Remote Photoplethysmography (rPPG) are fused to distinguish live vs. spoof faces in [26].

A Comparative Study on Face Spoofing Attacks by Sandeep Kumar et. Al. in [27] provided a detailed study of anti-spoofing methodologies and evaluation of databases. The study concluded that there is a need to provide more generalized algorithms for detection of unpredictable spoofing attacks in order to make the system more secure, computationally efficient and reliable.

In [28], the authors proposed a virtually blind image quality assessment procedure for detecting spoofed images based on their contrast profile. The reference images constitute natural images of subjects from the database. The contrast scores from these natural reference images are compared with the contrast score derived from the query image to detect OUTLIERS. The base statistic for quantifying contrast was as simple as a ratio of the mean value over an image/image block to the standard deviation of the image. This base statistic was deployed in face anti-spoofing, through a one class in-house TUNING procedure for defining only the inlier population comprising of only these reference images from the database. To their knowledge that was the only solution where the tuning process for setting up the system parameters, is one sided (wherein only images from one class are used) for a twoclass (real-spoof) face classification problem.

Another work carried in [29] by Kannan Karthik presented a novel procedure for arriving at a sharpness profile for performing spoof-checks on facial images (or portraits). Photos of photos tend to have lower sharpness diversity and overall mean sharpness as compared to natural photographs. This aspect has been quantified and used to train an SVM classifier. Proposed system was tested on the Chinese Academy of Sciences (CASIA) dataset and showed a recognition rate of 98.38% corresponding to a false positive rate of 10%. The proposed algorithm is computationally less intensive and better than the state-of-the-art model-independent Wen‟s anti-spoofing system. 11 Consistent counter-measures need to meet certain requirements, mainly regarding reliable robustness and low complexity.

Emna Fourati et. Al. in their work in [30] aimed to find the best compromise between these two criteria, as they proposed an anti-spoofing solution based on Image Quality Assessment (IQA) to distinguish between genuine and fake face appearances. We have also exploited motion-based cues of a given video sample, to extract the most relevant frames on which quality measures are computed following a novel approach. The results showed that their method outperformed state-of-the-art solutions using the low-complexity Linear Discriminant Analysis (LDA) classifier.

[31] A Dataset and Benchmark for Large-scale Multi-modal Face Anti-spoofing by Shifeng Zhang To facilitate face anti-spoofing research, the researchers in [31] introduced a largescale multi-modal dataset, namely CASIA-SURF (synthetic unit-record files), which is the largest publicly available dataset for face anti-spoofing in terms of both subjects and visual modalities. Specifically, it consists of 1,000 subjects with 21,000 videos and each sample has 3 modalities (i.e.,RGB, Depth and IR). We also provide a measurement set, evaluation protocol and training/validation/testing subsets, developing a new benchmark for face anti-spoofing. Moreover, they presented a new multi-modal fusion method as baseline, which performs feature re-weighting to select the more informative channel features while suppressing the less useful ones for each modal. In this paper, they presented and released a large-scale multi-modal face antispoofing dataset. The CASIA-SURF dataset is the largest one in terms of number of subjects, data samples, and number of visual data modalities. Owing to the largescale learning, they found that traditional evaluation metrics in face anti-spoofing (i.e., Attack presentation classification error rate (APCER), and Average classification error rate (ACER)) did not clearly reflect the utility of models in real application scenarios. In this regard, they proposed the usage of the Region of convergence (ROC) curve as the evaluation metric for large-scale face anti-spoofing evaluation. Furthermore, they proposed a multi-modal fusion method, which performs modal-dependent feature re-weighting to select the more informative channel features while suppressing the less informative ones.

In [32] This paper introduces the research progress of face anti-spoofing algorithm, and divides the existing face anti-spoofing methods into two categories: methods based on manual feature expression and methods based on deep learning. Then, the typical algorithms included in them are classified twice, and the basic ideas, advantages and disadvantages of these algorithms are analyzed. Finally, the methods of face anti-spoofing are summarized, and the existing problems and future prospects are expounded.

In [33] The focus of the work in this paper is to explore the area of face anti spoofing, research done in terms of quantitative analysis and its impact. The keyword analysis table indicates face recognition as a widely used keyword followed by biometrics and face anti spoofing as per the Scopus dataset search. The citation analysis indicates that texture based systems have contributed majorly for Face anti spoofing detection. The Bibliometric analysis done in this paper tends to provide some future research directions in the area of Face anti spoofing analyse the trends of research done.

In [34] this paper, they extend the Central difference convolutional networks (CDCN) to a multimodal version, intending to capture intrinsic spoofing patterns among three modalities (RGB, depth and infrared). Meanwhile, they also give an elaborate study about singlemodal based CDCN. Their final submission obtains 1.02±0.59% and 4.84±1.79% ACER in “Track Multi-Modal” and “Track SingleModal (RGB)”, respectively In [35] this paper they rephrase face anti-spoofing as a material recognition problem and combine it with classical human material perception, intending to extract discriminative and robust features for Face anti-spoofing. To this end, they propose the Bilateral Convolutional Networks (BCN), which is able to capture intrinsic material-based patterns via aggregating multi-level bilateral macro- and microinformation. Furthermore, Multilevel Feature Refinement Module (MFRM) and multi-head supervision are utilized to learn more robust features. Comprehensive experiments are performed on six benchmark datasets, and the proposed method achieves

superior performance on both intra- and cross-dataset testings. One highlight is that they achieve overall 11.3±9.5% EER for cross-type testing in Spoofing in the Wild Database – MSU computer vision lab (SiW-M) dataset, which significantly outperforms previous results.

**Methodology**

A block diagram of a proposed work of anti-spoofing techniques is shown in the This figure 6 below. The proposed work is basically focused on the photos of photos.exhibit greater homogeneity in the sharpness profiles and have overall lower sharpness values than their natural counterparts. Also the photographs taken under different lighting conditions, establishes and quantify the quality in terms of their contrast profile. Figure 6 – Block diagram of the proposed system 5.1 Algorithm

1. The spoofed/real images are input to the system.
2. The input image is then subjected to improved sharpness and contrast optimization algorithm based on two considerations below:

a. The degree of misalignment increases because of the carelessness of the photographer, it becomes possible to segregate the primary and 15 secondary photographs based on the extent of sharpness (or its antipodal property viz. blur).

b. The basic idea is to examine and qualify an image based on its "clarity" or "discernibility" of the face captured. Without focussing on the edge profile or the richness in texture, an indirect indication in terms of the image "contrast" will be adopted. Contrast here is defined as the extent of clarity perceived in a given image. This "clarity" can be quantified and extracted from any given image without any form of reference. Hence the approach virtually becomes a blind image quality assessment procedure.

3. The texture descriptors are then extracted from the image along with motion descriptors, frequency domain features, colour and shape features.
4. The features are provided to the classifier for training and validation. The process includes modifying the structure of a pretrained network. Many sophisticated pretrained networks are available with high class performance over thousands and millions of images. These networks have flexibility to be modified in terms of layers and parameters so as to suit our requirements. Also, dynamic and static inputs can be applied to achieve complex task in classification problems with fusions of outputs from multiple subnets.
5. Once the network has been trained properly, the images under test can be tested for performance. The network will be capable of distinguishing the spoofed types and the real types of images with high performance.
6. The performance parameters will then be evaluated for comparison with other benchmark techniques.

Metrics Commonly evaluated on face anti-spoofing techniques:

The following performance parameters will be used to evaluate the performance of the proposed work such as:

- False Acceptance Rate
- False Rejection Rate 16
- Equal Error Rate
- Half Total Error Rate
- Accuracy
- Area under Curve.

**Conclusion**

In this paper, a countermeasure against face-spoofing attacks was proposed. The proposed technique uses a deep CNN architecture with combination of LBP and SWLD descriptor, SVM with non-linear kernel to train classifiers. Our proposed method test on two publiclyavailable datasets. Between real access and impostor attacks, a perfect discrimination was achieved on the REPLAY-ATTACK and very competitive result on CASIA dataset. As a future direction, other filtering techniques and different network structures are planned to explore to find a way to adapt the model to new data (Ex. detect spoofing attacks using facial mask sand 3D models) and further studies will be done in decreasing the number of features.

**Reference**

1. A. Cornujols, C. Wemmert, P. Ganarski and Y. Bennani, "Collaborative clustering: Why, when, what and how, Information Fusion", 39 (2018) 81-95, Elsevier.
2. Agarwal, A., Singh, R., Vatsa, M.: 'Face anti-spoofing using haralick features'. 2016 IEEE 8th Int. Conf. on Biometrics Theory, Applications and Systems (BTAS), Cancún, Mexico, 2016, pp. 1–6.
3. Anjith George and Sebastien Marcel, "Deep Pixel-wise Binary Supervision for Face Presentation Attack Detection", arXiv:1907.04047v1 [cs.CV] 9 Jul 2019.
4. Anjos, A., Marcel, S.: 'Counter-measures to photo attacks in face recognition:a public database and a baseline'. Proc. Int. Joint Conf. on Biometrics (IJCB),Washington, DC, USA, 2011.
5. Artur Costa-Pazo et. Al., "Generalized Presentation Attack Detection: a face anti-spoofing evaluation proposal", arXiv:1904.06213v1 [cs.CV] 12 Apr 2019.

6. Asim, M., Ming, Z., Yaqoob Javed, M.: 'CNN based spatio-temporal featureextraction for face anti-spoofing'. 2nd Int. Conf. on Image, Vision andComputing (ICIVC), New Delhi, India, 2017.
7. Atoum, Y., Liu, Y., Jourabloo, A., et al.: 'Face anti-spoofing using patch anddepth-based CNNs'. Int. Joint Conf. on Biometrics (IJCB), 2017.
8. B. Biggio, Z. Akhtar, G. Fumera, G.L. Marcialis, F. Roli, "Security evaluation of biometric authentication systems under real spoofing attacks". IET Biometrics, 1 (1)(2012) 11–24.
9. Bharadwaj, S., Dhamecha, T.I., Vatsa, M., et al.: 'Computationally efficient face spoofing detection with motion magnification'. Proc. of IEEE Conf. on Computer Vision and Pattern Recognition, Workshop on Biometrics, 2013.
10. Boulkenafet, Z., Komulainen, J., Hadid, A.: 'Face anti- spoofing usingspeeded-up robust features and fisher vector encoding', IEEE Signal Process.Lett., 2017, 24, (2), pp. 141–145.
11. Boulkenafet, Z., Komulainen, J., Hadid, A.: 'Face anti-spoofing based oncolor texture analysis'. 2015 IEEE Int. Conf. on Image Processing (ICIP),2015, pp. 2636–2640.
12. Boulkenafet, Z., Komulainen, J., Hadid, A.: 'Face spoofing detection using colour texture analysis', IEEE Trans. Inf. Forensics Sec., 2016, 11, pp. 1818–1830.
13. Chang, C.C., Lin, C.J.: 'Libsvm: A library for support vector machines', ACMTrans. Intell. Syst. Tech., 2011, 2, (3), p. 27
14. Chen, J., Shan, S., He, C., et al.: 'WLD: a robust local image descriptor',IEEE Trans. Pattern Anal. Mach. Intell., 2010, 32, pp. 1705–1720.
15. Chetty, G.: 'Biometric liveness checking using multimodal fuzzy fusion'.2010 IEEE Int. Conf. on Fuzzy Systems (FUZZ), 2010, pp. 1–8.
16. Chingovska, I., Anjos, A., Marcel, S.: 'On the effectiveness of local binarypatterns in face anti-spoofing'. Proc. Int. Conf. of the Biometrics SpecialInterest Group (BIOSIG), Darmstadt, Germany, 2012, pp. 1–7.
17. de Souza, G.B., Papa, J.P., Marana, A.N.: 'On the learning of deep local features for robust face spoofing detection'. 2018 31st SIBGRAPI Conf. on Graphics, Patterns and Images (SIBGRAPI), Phuket, Thailand, 2018, pp.258–265.
18. de Freitas Pereira, T., Anjos, A., De Martino, J.M., et al.: 'Lbp- top basedcountermeasure against face spoofing attacks'. Computer Vision-ACCV 2012Workshops, Daejeon, South Korea, 2013, pp. 121–132.
19. Devakumar, P., Sarala, R.: 'An intelligent approach for anti-spoofing in amultimodal biometric system', Int. J. Adv. Res. Comput. Sci. Soft. Eng., 2017,7, (3), pp. 70–76.
20. Di Wen et. Al., "Face Spoof Detection with Image Distortion Analysis", IEEE Transactions on Information Forensics and Security, 2015.
21. E. Learned-Miller, G. B. Huang, A. RoyChowdhury, H. Li and G. Hua, "Labeled Faces in the Wild: A Survey, Advances in Face Detection and Facial Image Analysis", (2016) pp. 189-248, Springer.
22. Emna Fourati et, al., "Face anti-spoofing with Image Quality Assessment", 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART), 2017.
23. Erdogmus, N., Marcel, S.: 'Spoofing in 2D face recognition with 3D masksand anti-spoofing with kinect'. Proc. IEEE Biometrics: Theory, Applicationsand Systems (BTAS), Arlington, VA, USA, 2013.
24. Freitas Pereira, T., Komulainen, J., Anjos, A., et al.: 'Face livenessdetection using dynamic texture', EURASIP J. Image Video Process., 2014,2014, p. 2, 10.1186/1687-5281-2014-2.
25. G. Fischer, "Lifelong learning more than training", Journal of Interactive Learning Research, 11 (3/4) (2000) pp. 265-294.
26. Galbally, J., Marcel, S., Fierrez, J.: 'Image quality assessment for fakebiometric detection: application to iris, fingerprint and face recognition',IEEE Trans. Image Process., 2014, 23, (2), pp. 710–724.
27. Galbally, J., Marcel, S.: 'Face anti-spoofing based on general image qualityassessment'. Proc. IAPR/IEEE Int. Conf. on Pattern Recognition, ICPR,Stockholm, Sweden, 2014, pp. 1173–1178.
28. Ghazel Albakri and Sharifa Alghowinem, "The Effectiveness of Depth Data in Liveness Face Authentication Using 3D Sensor Cameras", Sensors 2019, 19, 1928; doi:10.3390/s19081928.
29. Gragnaniello, D., Poggi, G., Sansone, C., et al.: 'An investigation of localdescriptors for biometric spoofing detection', IEEE Trans. Inf. Forensics Sec.,2015, 10, (4), pp. 849–863.
30. H. Yu, Y. Chen, J. Liu, X. Jiang, "Lifelong and fast transfer learning for gesture interaction", Journal of Information & Computational Science 11 (4) (2014) 1023- 1035.
31. Jain, A.K.: 'Fundamentals of digital signal processing' (Prentice-Hall,Englewood Cliffs, NJ, 1989)[29] Chen, J., Zhao, G., Pietikinen, M.: 'An improved local descriptor andthreshold learning for unsupervised dynamic texture segmentation'. 12th Int.Conf. on Computer Vision Workshops, October 2009, pp. 460–467.
32. Jianzhu Guo et. Al., "Improving Face Anti-Spoofing by 3D Virtual Synthesis", arXiv:1901.00488v2 [cs.CV] 8 Apr 2019.

33. Kannan Karthik and K. Balaji Rao, "Face Anti-spoofing based on Sharpness Profiles", ICIIS, IEEE 2017.
34. Kannan Karthik and K. Balaji Rao, "Image Quality Assessment Based Outlier Detection for Face Anti-Spoofing", 2nd International Conference on Communication Systems, Computing and IT Applications (CSCITA), IEEE 2017.
35. Kollreider, K., Fronthaler, H., Bigun, J.: 'Non-intrusive liveness detection byface images', Image Vis. Comput., 2009, 27, (3), pp. 233–244.
36. Komulainen, J., Hadid, A., Pietikainen, M.: 'Context based face anti-spoofing'. 2013 IEEE Sixth Int. Conf. on Biometrics: Theory, Applicationsand Systems (BTAS), Arlington, VA, USA, 2013, pp. 1–8.
37. Li, L., Feng, X., Boulkenafet, Z., et al.: 'An original face anti-spoofingapproach using partial convolutional neural network'. 2016 6th Int. Conf. onImage Processing Theory Tools and Applications (IPTA), 2016, pp. 1–6.
38. Luiz Souza, Luciano Oliveira, Mauricio Pamplona, "How far did we get in face spoofing detection?", in Engineering Applications of Artificial Intelligence, vol. 72, pp. 368-381, 2018.
39. M. Farmanbar and O. Toygar "A robust anti-spoofing technique for face liveness detection with morphological operations", Optik - International Journal for Light and Electron Optics, 139 (2017) 347-354, Elsevier.
40. M.Farmanbar and O. Toygar "Spoof detection on face and palmprint biometrics, Signal, Image and Video Processing", 11 (7) (2017) 1253- 1260, Springer.
41. Maatta, J., Hadid, A., Pietikainen, M.: 'Face spoofing detection from singleimages using micro-texture analysis'. 2011 Int. Joint Conf. on Biometrics(IJCB), Washington, DC, USA, October 2011, pp. 1–7.
42. Meigui Zhang, Kehui Zeng and Jinwei Wang, "A Survey on Face Anti-Spoofing Algorithms" in Nanjing University of Information Science and Technology, Nanjing, 210044, China Received: 21 May 2020; Accepted: 10 June 2020.
43. Menotti, D., Chiachia, G., Pinto, A., et al.: 'Deep representations for iris, face,and fingerprint spoofing detection', IEEE Trans. Inf. Forensics Sec., 2015, 10,(4), pp. 864–879.
44. Muhammad Sajjad, Salman Khan, Tanveer Hussain, Khan Muhammad, Arun Kumar Sangaiah, Aniello Castiglione, Christian Esposito, Sung Wook Baik, "CNNbased Anti-Spoofing Two-Tier Multi-Factor Authentication System", Pattern Recognition Letters (2018), doi: 10.1016/j.patrec.2018.02.015.
45. Ojala, T., Pietikainen, M., Harwood, D.: 'A comparative study of texture measures with classification based on feature distributions', Pattern Recognit., 1996, 29, (1), pp. 51–59.
46. Olegs Nikisins, Anjith George and Sebastien Marcel, "Domain Adaptation in Multi-Channel Autoencoder based Features for Robust Face Anti-Spoofing", arXiv:1907.04048v1 [cs.CV] 9 Jul 2019.
47. P. Johnson, B. Tan, S. Schuckers, "Multimodal fusion vulnerability to non-zero effort (spoof) imposters", in Proc. WIFS, 2010, pp. 1–5.
48. Patel, K., Han, H., Jain, A.K.: 'Secure face unlock: spoof detection onsmartphones', IEEE Trans. Inf. Forensics Sec., 2016, 11, (10), pp. 2268–2283.
49. Patel, K., Han, H., Jain, A.K., et al.: 'Live face video vs. Spoof face video: use of moiré patterns to detect replay video attacks'. 2015 Int. Conf. on Biometrics (ICB), New York, USA, 2015, pp. 98–105.
50. Patel, K., Han, H., Jain, A.K.: 'Cross-database face anti-spoofing with robustfeature representation'. Chinese Conf. on Biometric Recognition, Barcelona,Spain, 2016, pp. 611–619.
51. Peixoto, B., Michelassi, C., Rocha, A.: 'Face liveness detection under badillumination conditions'. ICIP, Bangalore, India, 2011, pp. 3557–3560.
52. Peng Zhang et. Al., "FeatherNets: Convolutional Neural Networks as Light as Feather for Face Anti-spoofing", arXiv:1904.09290v1 [cs.CV] 22 Apr 2019.
53. R.N. Rodrigues, L.L. Ling, V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks", Journal of Visual Languages and Computing, 20 (3) (2009), pp. 169-179.
54. R.N. Rodrigues, N. Kamat, V. Govindaraju, "Evaluation of biometric spoofing in a multimodal system", in Proc. BTAS, 2010, pp. 1–5.
55. Rui Shao, Xiangyuan Lan and Pong C. Yuen, "Regularized Fine-grained Meta Face Anti-spoofing", arXiv:1911.10771v1 [cs.CV] 25 Nov 2019.
56. Sandeep Kumar, Sukhwinder Singh and Jagdish Kumar, "A Comparative Study on Face Spoofing Attacks", International Conference on Computing, Communication and Automation, IEEE 2017.
57. Shifeng Zhang et. Al., "A Dataset and Benchmark for Large-scale Multi-modal Face Anti-spoofing", arXiv:1812.00408v3 [cs.CV] 1 Apr 2019.
58. Shinde, Swapnil Ramesh, Phansalkar, Shraddha and Thepade, Sudeep D., "A Bibliometric Analysis of Face Anti Spoofing" (2020). Library Philosophy and Practice (e-journal). 4434.
59. Siddiqui, T.A., Bharadwaj, S., Dhamecha, T.I., et al.: 'Face anti-spoofing with multi feature videolet aggregation'. 2016 23rd Int. Conf. on Pattern Recognition (ICPR), Kuala Lumpur, Malaysia, 2016, pp. 1035–1040.

60. Sun, L., Pan, G., Wu, Z., et al.: 'Blinking-based live face detection usingconditional random fields', in 'Advances in biometrics' (Springer, Barcelona,Spain, 2007), pp. 252–260.
61. T. de Freitas Pereira, A. Anjos, J. M. De Martino and S. Marcel, "Can face antispoofing countermeasures work in a real world scenario?", in Proc. ICB, Madrid, 2013, pp. 1-8.
62. Tan, X., Li, Y., Liu, J., et al.: 'Face liveness detection from a single imagewith sparse low rank bilinear discriminative model'. ECCV (6), Crete,Greece, 2010, pp. 504–517.
63. Viola, P., Jones, M.: 'Rapid object detection using a boosted cascade of simple features'. Proc. of the 2001 IEEE Computer Society Conf. on Computer Vision and Pattern Recognition, 2001. CVPR 2001, Beijing, China,2001, vol. 1, p. I–511.
64. Wang, Y., Nian, F., Li, T., et al.: 'Robust face anti-spoofing with depth information', J. Vis. Commun. Image R., 2017, 49, pp. 511–518.
65. Wen, D., Han, H., Jain, A.: 'Face spoof detection with image distortionanalysis', Trans. Inf. Forensics Secur., 2015, 10, (4), pp. 746–7611884IET Image Process., 2019, Vol. 13 Iss. 11, pp. 1880-1884© The Institution of Engineering and Technology 2019.
66. Xiaoguang Tu et. Al., "Learning Generalizable and Identity-Discriminative Representations for Face Anti-Spoofing", arXiv:1901.05602v1 [cs.CV] 17 Jan 2019.
67. Xu, Z., Li, S., Deng, W.: 'Learning temporal features using lstm-cnnarchitecture for face anti-spoofing'. 2015 3rd IAPR Asian Conf. on Pattern Recognition (ACPR), Darmstadt, Germany, 2015, pp. 141–145.
68. Yang, J., Lei, Z., Li, S.Z.: 'Learn convolutional neural network for face anti-spoofing'. CoRR, abs/1408.5601, 2014.
69. Yang, J., Lei, Z., Liao, S., et al.: 'Face liveness detection with componentdependent descriptor'. ICB, Madrid, Spain, 2013.
70. Yaojie Liu et. Al, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision", Computer Vision and Pattern Recognition, arXiv:1803.11097.
71. Yaojie Liu, Joel Stehouwer, Amin Jourabloo and Xiaoming Liu, "Deep Tree Learning for Zero-shot Face Anti-Spoofing", arXiv:1904.02860v2 [cs.CV] 9 Apr 2019.
72. Yousef Atoum et. Al., "Face Anti-Spoofing Using Patch and Depth-Based CNNs", IEEE International Joint Conference on Biometrics (IJCB), 1-4 Oct. 2017.
73. Z. Akhtar, G. Fumera, G.L. Marcialis, F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks", in Proc. BTAS, 2012, pp. 283–288.
74. Zhang, Z., Yan, J., Liu, S., et al.: 'A face anti-spoofing database with diverseattacks'. 2012 5th IAPR Int. Conf. on Biometrics (ICB), New Delhi, India,2012, pp. 26–31.
75. Zhang, Z., Yan, J., Liu, S., et al.: 'A face antispoofing database with diverseattacks'. 2012 5th IAPR int. Conf. on Biometrics (ICB), 2012, pp. 26–31.
76. Zitong Yu, Yunxiao Qin, Xiaobai Li, Zezheng Wang, Chenxu Zhao, Zhen Lei, Guoying Zhao, "Multi-Modal Face Anti-Spoofing Based on Central Difference Networks", (2020).
77. Zitong Yu1, Xiaobai Li, Xuesong Niu, Jingang Shi, and Guoying Zhao, "Face Anti-Spoofing with Human Material Perception" ( 2020).