IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A REVIEWS ON FACE ANTI-SPOOFING METHODS

Srikanta Datta Kashyap A P[+], Samarth B N[+], Sathvik S R[+] , Shashikumara K [+],Dr. Raghavendra R. J[*]

[+]Department of Information Science and Engineering,
J N N College of Engineering, Shimoga.
[*]Associate Professor, Department of Information Science and Engineering,
J N N College of Engineering, Shimoga.

ABSTRACT: *There are several developments in face recognition systems, in spite of that current face recognition systems are exposed to presentation attacks (PA) such as photo, video and 3D masks attacks. Plenty of anti-spoofing methods have been developed to classify a person is real or spoof. An effective method is to develop to protect against face recognition system is challenging work. In order to overcome this, many face anti-spoofing techniques of various types have been in discussed in this paper. It consists of sensor-based methods, Challenge Response, Handcrafted feature and Deep learning approaches. We discussed it's their drawbacks, execution and advantages and also some modern face anti-spoofing approaches.*

Keywords: **Face anti-spoofing, Presentation Attack Detection (PAD), ELTCP, Information Security, Face Recognition, Convolution Neural Network.**

1. Introduction

A Face Biometric system is a new technology capable of matching a human face with database of faces which includes digital image or a video frame . In previous decades passwords and a shared secret key was the authentication tools in many automatic identity scenarios. Face Biometrics technology have gradually replaced the old scenarios. Face biometrics have been widely used in criminal investigation, research area entry control systems, and security inspection equipment [1]. The face recognition (FR) is used to control and restrict the access to specified area, secured boxes or high-technology computing systems. The face recognition has involved widespread consideration because to its features such as security, good stability, interactive artificial intelligence systems for its convenience. Face biometric recognition is the process of identifying, verifying a person using their face. It captures, examines and compares the person's face with some patterns and parameters of faces, such as color texture, background light intensity, Depth-based CNN [2], Deep pixels [3].

Due to the development in technologies and research area of image processing and pattern recognition of high-quality images, which can process new modern images, many challenges occur on the face presentation attack (or spoofing attack) of FR in the past years. The face biometric systems which are used for security purposes can be simply misled by spiteful presentation attacks making the system relatively vulnerable [4]. When an unauthorized user tries to access the system by impersonating a real user this type of attack is considered a presentation attack. Presentation attacker can be made by various means. The presentation attack are two types: Impersonation attacks and obfuscation attacks. Fig 1 shows various types of attack and classification.

Among them photo attacks [5], video attacks [6], reply attacks [7] and 3D mask attacks are the commonly used type of attacks. Obfuscation attacks includes hiding the user's true distinctiveness, such as face makeup [7], plastic surgeries, or blockage eyes and the face region. Face anti-spoofing detection is an extremely concerned research topic in the domain of computer vision. The existing methods of face anti-spoofing methods are categorized into three main varieties: Illumination peculiarity-based approaches, physiological sign-based approaches [8] and texture-based approaches [9]. A very vital role is by face anti-spoofing systems for a consistent and secure deployment of face recognition systems. To reinforce the security of FR systems. In the past decade many researches have been made on face presentation attack detection methods (PAD). The aim these methods is to improve the generalization ability of attack detection. When an authorized user is present in front of the camera, the system captures the face image analyses it and allow access the system for that that real user. When an unknown user enters by using various means either the system has found the malicious or it has to prevent the unknown persons to enter the system.

This survey paper is organized as, Introduction and various types of attacks, an overview of the recent research approaches on face anti-spoofing and then, modern approaches in face anti-spoofing. Finally, the conclusions of the paper.

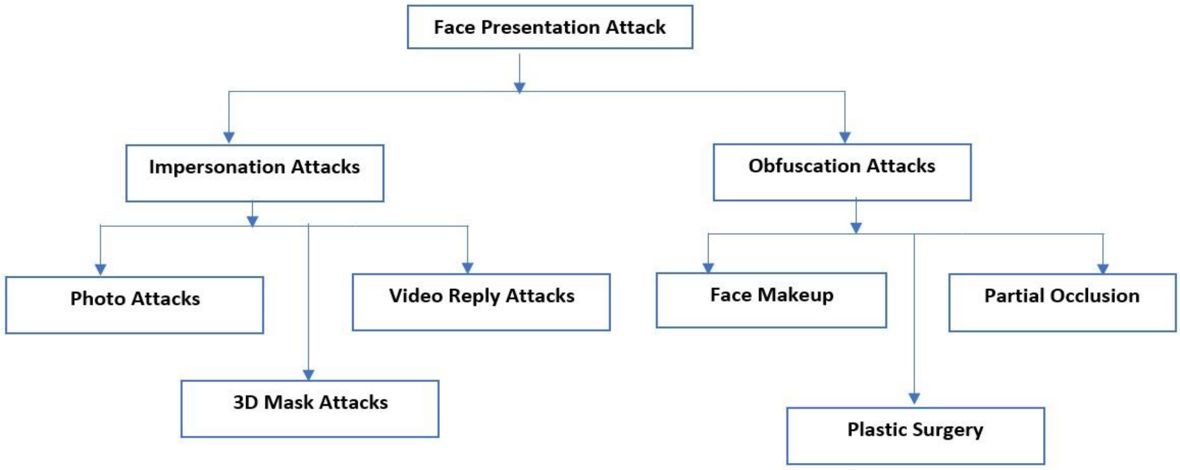

Fig 1: Types of Face presentation attacks

2. Presentation Attack Detection Methods (PAD)

As shown in Fig.2, the different approaches of PAD are reviewed, they are sensor methods, challenge response methods, handcrafted feature-based methods, deep learning methods and other methods. we will examine these methods accordingly.

2.1 Sensor-based Methods

Depth cameras [10], IR-cameras [11], and Multimodal Biometric sensors [12], Light-field cameras (LFC) are sensor-based methods, which can provide extensive auxiliary information and are helpful for presentation attack detection (PAD). However, these methods tend to increase the economic cost and application complexity of face anti-spoofing systems, while they can strengthen the security of face recognition (FR) systems. The primary goal of a face anti-spoofing system is to protect sensitive data [13], reduce theft, and detect various predefined presentation attacks. To achieve this, a large amount of data is necessary to cover most of the possible attacks. To overcome these challenges, the detector should learn discriminative features and quickly adapt to new spoofing types by learning from both the predefined attacks and unseen attacks. One such method is the Adaptive Inner-Update Meta Face Anti-Spoofing (AIM-FAS) approach.

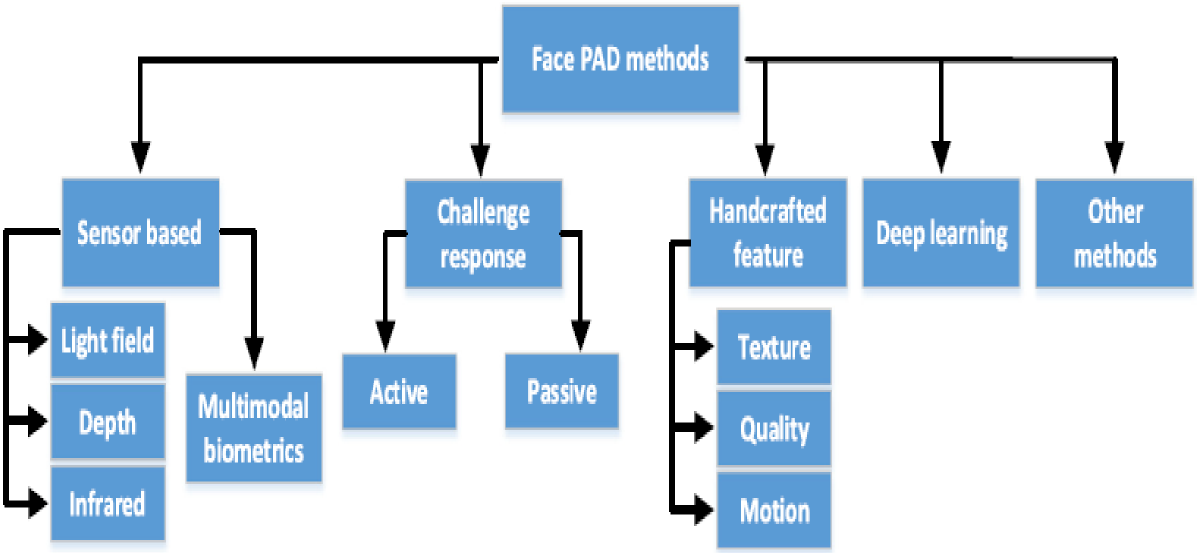

Fig 2: Face anti-spoofing methods

The susceptibility of most face recognition is face presentation attacks (PA) [14]. In this work used a statistical model of image noise. The attack face has some specific textural features which makes them different from real faces. The differences among real and spoof faces can be understood by differences in noise statistics and skin zone. Presentation attacks seek to conceal or impersonate a person's identity. They are primarily studied in the visible spectrum. For face presentation attacks utilising latex and paper masks, this work [15] introduces a distinctive multispectral video face database. Physiological indicators of liveness, such as eye blinking [12], eye movement, or lip movement, are detected using dynamic anti-spoofing algorithms that analyze motion over a facial video series.

2.2 Challenge-Response Approaches

Challenge response approaches are further classified into active liveness check and passive liveness check.

a. ***Active liveness check:*** Liveness check techniques are used to check and confirm whether the user is present in front of system or not by interacting with the system. This approach requires a user to deliberately confirm the presence. The active liveness detection technology [12], which is based on gesture flow and artificial intelligence. In this approach two images are captured, and the liveness is verified by the movement between the captured images. The 3D face-image movement is different than a 2D face images. Hence this system resolves whether the person is trying to access the system is live or spoof.

b. ***Passive liveness check:*** passive liveness approach is a kind of fake detection method which does not requires any kind movements and actions from the user. Typically, only once image is taken from the user and analysed using artificial intelligence. Capturing entire videos of the session or flashing lights on the user are most commonly used for analysis. The passive liveness detection method without known it can even run as background process.

2.3 Handcrafted Feature-based Methods

This method analyses the spoof faces and real faces and in terms of both facial background content and regions, and extracts suitable features to detect facial expression attacks. Characteristic methods are quality of image analysis [16], motion information analysis [17], motion blur analysis, and image-texture methods. Texture-based methods can be further classified into dynamic texture-based and static texture-based methods. In static texture-based methods, block LBPs are extracted from face images for PAD, and further a support vector machine is used for classification Maatta et al. [18]. For a dynamic texture-based method, LBP are extracted from the three orthogonal planes of facial PAD proposed by Pereira et al. [19] and Z. Boulkenafet et al. [20]. Later, this method was prolonged to local binary counting and spatial-temporal networks. Color distortion analysis [21] for face-spoofing detection provides promising results. This method extracts histogram and color moments features and produces the labelled vectors for further analysis. In order to perform reduction analysis, the vector is then passed to principal component analysis (PCA). This method has better performance than other methods.

The color texture-based face anti-spoofing uses an image of a spoof face and considering it as actual image. Then two camera or a display device are used to pass the image, or a printing system, hence by doing this twice the image is considered as recaptured image. As a result, the detected fake image will grieve from various kinds of quality issues, such as, printing defects video artifacts, color variations, PAI dependent and limited color reproduction (gamut), that can be analyzed the texture content by capturing the both luminance and chrominance channels. By calculating histograms [22], the Local binary pattern (LBP) is constructed and it is originally proposed for texture classification. For the optimization of quantization schemes, some complex quantization methods were projected in order reduce information loss by sign-based quantization, such as completed Local directional ternary pattern and LBP [23]. Further, Raghavendra et al. [46-50] proposed more innovative feature descriptors such as ELTCP, DOG-ADTCP and EDDTCP for face anti-spoofing.

Chan et.al [24] proposes, to extract facial colour texture from a user and pass it to seven descriptors for anti-spoofing. The PAD solution is built to decide between fake face images and real image but the print attacks in different circumstances. In this work [25], uses auto encoder-based detection algorithm and one-Class SVM in order to solve the UPAD problems and detect spoofing attacks in different scenarios. The goal of this work [26] is to counter attacks in a face recognition system by developing a face anti-spoofing system based on accompanied scale texture. To reduce the effect of unwanted noise group corruption, accompanied scale texture space is proposed to reduce the repeated additional data of the original facial texture and obtain facial edges. To obtain liveness finding features, two guided scale texture descriptors are proposed: The Local guided binary pattern (LGBP)and Guided scale-based local binary pattern (GS-LBP), this uses the concept of joint quantization and property of the guided scale space for edge-preserving. Further which encodes the neighboring relationships of the real face and also the guided scale face without using extra properties.

2.4 Deep Learning Methods

This method of presentation attacks is based on artificial intelligence and neural network methods, which extract features based on deep learning models, unlike traditional methods that require manual feature construction. Distinctive methods include neural networks, deep dictionary learning [27], spatial domain adaptation [28], 3D convolutional neural networks, local binary pattern networks, local homographic parameterization [29], discriminative representation combinations, deep dynamic texture, convolutional feature fusion, and deep tree learning. Silicone masks used in movies are easily available on the market and can be used for criminal activities and to bypass face recognition systems. Thus, it is important to defend attacks on biometric systems from such false attacks. In this work [30], the first-of-its-kind silicone mask attack database was presented, which contains 150 real and attacked videos.

Previous work on depth supervised learning has shown effectiveness for face anti-spoofing, a but single frame is considered depth as auxiliary supervision. A new method [31] was proposed with multiple RGB frames to estimate depth information are taken. To propose a depth-supervised architecture that can efficiently encode spatiotemporal information for presentation attack detection. It includes two novel modules: the convolution gated recurrent units and the optical flow guided feature block (OFFB).

3. Modern Approaches

In the new modern approaches, we have analysed the contemporary methods used in anti-spoofing which will address the problems like color images and datasets comprised of high-quality images. Zinelabidine et al. [32] provides the focus of research on detecting software-based face spoofing without intrusion has mostly been on analysing the brightness of face images while ignoring the chroma component, which can be valuable in distinguishing between fake and genuine faces. The present work uses the colour texture-based method for detecting the spoof face. Luminance and the chrominance channels are the two joint colour texture information of images which are extracted from an image for analysis. The result is true for same as well as the cross-databases. For example, in [33], researchers are made on the social networks, social media-based images are disclosed and are used for attacks. While an average 40% of face images published on social media and other sites can be used for spoofing attacks. Many techniques of face attacks analyzing static (and dynamic) facial appearance properties. The face image is captured with two cameras and printed or displayed for analysis. The face image will have lower image quality, high frequency information [34]. Also, the images which are captured again contains other quality issues, such as printing artefacts or, background distraction in videos [35], content-independence. Algorithms that map colors can be used on an original image to maintain the perception of colour and appearance on different types of devices.

The other approach includes multi-spectral [46], 3D technique of hardware-based [37, 38] imaging provides to detect face spoofs effectively. Various techniques can be employed which provide valuable insights into the surface reflectivity properties or depth of the face. These techniques include the co-occurrence of adjacent local binary patterns (CoALBP), the binarized statistical image features (BSIF), local phase quantization (LPQ), and the scale-invariant descriptor (SID) are facial colour descriptors. The objective of the face anti spoofing methods is generalization via training the target set and source set of databases jointly. Considering the privacy, it is difficult to make such things. Therefore, a new framework known as source-free domain are used. The training data are labelled source data are not labelled also, the movement differences between fake and real faces can be captured by utilizing dynamic images that incorporate the background. This approach also applicable for generalization in public domain databases. Initially, hand-crafted features were utilized for binary classification in early approaches [39, 40]. Later, Yang et al. [41] extract deep features by CNN to differentiate between real and fake faces.[42]. Notably, some source data-free classification methods have shown significant progress [43, 44], where the primary focus is on training the target model using reliable pseudo labels. The work proposes the usage of dynamic images to obtain motion deviations of the face with respect to background. To avoid dependence on source data, the aim is to develop a predictive model that can generalize across various domains with unlabeled data only. Due to drop in performance of cross domain, kernel Hilbert spaces approach [45] a deep adaptation network was suggested to transfer deep features in order to achieve desired mapping.

4. Conclusions

In this paper, we had gone through important face anti-spoofing approaches. We have shown how PAD has drastically changed in 20 years. As face PAD is influenced by different environments, lighting conditions, demographics, PAIs, cameras, and presentation distances, the developed schemes only consider different cameras and PAIs, it still has room to improve its performance. The recommended replay attack detection and liveness algorithms, on the other hand, work on standard spoof materials. As a result, for undetectable and unexpected spoofing attacks, generalized techniques must be utilized. We've also recognized a few of the most significant developments in facial presentation attack detection, such as merging techniques to block many types of assaults or tackling previously undiscovered attacks.

References

[1] Xiong, Fei, and Wael Abd Almageed, "Unknown presentation attack detection with face rgb images", in proceedings of IEEE International Conference on Biometrics Theory, Applications and Systems, pp. 1-8, 2018.

[2] Atoum, Yousef, et al. "Face anti-spoofing using patch and depth-based CNNs", In proceedings of IEEE International Joint Conference on Biometrics (IJCB), 2017.

[3] George, Anjith, and Sébastien Marcel. "Deep pixel-wise binary supervision for face presentation attack detection." In proceedings of IEEE International Conference on Biometrics (ICB), 2019.

[4] M. S. Hossain, L. Rupty, K. Roy, M. Hasan, S. Sengupta and N. Mohammed, "A-DeepPixBis: Attentional angular margin for face anti-spoofing", in proceedings of IEEE Digital Image Computing: Techniques and Applications, pp. 1-8, 2020.

[5] Chou, Chao-Lung. "Presentation attack detection based on score level fusion and challenge-response technique", in Journal of Supercomputing, Vol 7, 2021.

[6] K. Patel, H. Han, A. K. Jain and G. Ott, "Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks," in proceedings of International Conference on Biometrics (ICB), 2015.

[7] C. Chen, A. Dantcheva, T. Swearingen and A. Ross, "Spoofing faces using makeup: An investigative study," in proceedings of International Conference on Identity, Security and Behavior Analysis (ISBA) , pp. 1-8, 2017.

[8] Kiselev, Gleb Andreevich, and Aleksandr Igorevich Panov. "Sign-based approach to the task of role distribution in the coalition of cognitive agents", in proceedings of SPIIRAS, pp 161-187,2018.

[9] Z. Boulkenafet, J. Komulainen, A. Hadid, "On the generalization of color texture-based face anti-spoofing", in Journal of Image and Vision Computing, vol. 77, pp. 1–9, 2018.

[10] Z. Akhtar, C. Micheloni, G.L. Foresti, "Biometric liveness detection: Challenges and research opportunities", in proceedings of IEEE Transaction on Challenges and Research Opportunities in Security, pp. 63–72, 2017.

[11] F. Peng, L.B. Zhang, M. Long, "FD-GAN: Face de-morphing generative adversarial network for restoring accomplice's facial image", in Journal of IEEE Access, vol. 7, pp. 75122-75131, 2019.

[12] R. Ramachandra, C. Busch, "Presentation attack detection methods for face recognition systems: A comprehensive survey", in Journal of ACM Computing Surveys, vol. 50, pp. 1-37, 2017.

[13] Zezheng Wang, Chenxu Zhao, Yunxiao Qin, Qiusheng Zhou, Guojun Qi, Jun Wan, Zhen Lei, "Exploiting temporal and depth information for multi-frame face anti-spoofing", in Journal of Computer Vison and Pattern Recognition, pp. 1-10, 2018.

[14]H. P. Nguyen, A. Delahaies, F. Retraint and F. Morain-Nicolier, "Face Presentation Attack Detection Based on a Statistical Model of Image Noise," in Journal of IEEE, vol. 7, pp. 175429-175442, 2019.

[15] A. Agarwal, D. Yadav, N. Kohli, R. Singh, M. Vatsa and A. Noore, "Face Presentation Attack with Latex Masks in Multispectral Videos," in proceedings of IEEE Transactions on Computer Vision and Pattern Recognition Workshops, pp. 275-283,2017.

[16] J. Galbally, S. Marcel, J. Fierrez, Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition, in proceedings of IEEE,vol 23, pp.710–724,2014.

[17] T. Edmunds, A. Caplier, "Motion-based countermeasure against photo and video spoofing attacks in face recognition", in proceedings of IEEE, Vol 50 pp.314–332 2018.

[18] J.Maatta, A. Hadid, M. Pietikäinen, Face spoofing detection from single images using micro-texture analysis",in proceedings of IEEE International Joint Conference on Biometrics, pp. 1–7,2011.

[19] Pereira T de Freitas, A. Anjos, J.M. De Martino, et al., "LBP_ TOP based countermeasure against face spoofing attacks", in proceedings of Asian Conference on Computer Vision, pp. 121–132, 2012.

[20] Z. Boulkenafet, J. Komulainen, A. Hadid, "Face anti-spoofing based on color texture analysis", in proceedings of IEEE International Conference on Image Processing, pp. 2636–2640, 2015.

[21] G. D. Simanjuntak, K. Nur Ramadhani and 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.

[22] I. Chingovska, A. Anjos, S. Marcel, "On the effectiveness of local binary patterns in face anti-spoofing,in proceedings of International Conference of the Biometrics, 2012.

[23] B. Biggio, G. Fumera, G.L. Marcialis, et al., "Statistical meta-analysis of presentation attacks for secure multibiometric systems",in proceedings of IEEE Transactions, vol 3, pp. 561–575.2017

[24] P.P.K. Chan, W. Liu, D. Chen, et al., "Face liveness detection using a flash against 2D spoofing attack", in proceedings of IEEE Transactions, vol 13, pp.521–534,2018.

[25] Xiong, Fei, and Wael Abd Almageed, "Unknown presentation attack detection with face rgb images", in proceedings of IEEE International Conference on Biometrics Theory, Applications and Systems, pp. 1-8, 2018.

[26] Wael Abd Almageed, Fei, Xiong, "Unknown presentation attack detection with face RGB images", in proceedings of IEEE International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1-9, 2018.

[27] F. Peng, L.B. Zhang, M. Long, "FD-GAN: Face de-morphing generative adversarial network for restoring accomplice's facial image", in Journal of IEEE Access, vol. 7, pp. 75122-75131, 2019.

[28] H. Li, P. He, S. Wang, et al., “Learning generalized deep feature representation for face anti-spoofing”, in proceedings of IEEE Transaction, pp. 2639–2652.2018.

[29] Z. Sun, L. Sun, Q. Li, “Investigation in spatial-temporal domain for face spoof detection”, in proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 1538–1542,2018.

[30] C. Lin, Z. Liao, P. Zhou, et al., “Live Face verification with multiple instantialized local homographic parameterization”, in proceedings of International Joint Conference on Artificial Intelligence, pp. 814–820,2018.

[31] Sushil Bhattacharjee, Amir Mohammadi, Andre Anjos & Sebastien Marcel, "Recent advances in face presentation attack detection”, in Handbook of Biometric Anti-Spoofing, pp. 207-228, 2019.

[32] Zinelabidine, Jukka Komulainen, and Abdenour Hadid. "Face spoofing detection using colour texture analysis", in proceedings of IEEE Transactions on Information Forensics and Security, pp.1818-1830, 2016.

[33] Zezheng Wang, Chenxu Zhao, Yunxiao Qin, Qiusheng Zhou, Guojun Qi, Jun Wan, Zhen Lei, "Exploiting temporal and depth information for multi-frame face anti-spoofing", in Journal of Computer Vison and Pattern Recognition, pp. 1-10, 2018.

[34] Y. Li, K. Xu, Q. Yan, Y. Li, and R. H. Deng, “Understanding OSN-based facial disclosure against face authentication systems,” in Proceedings of the Symposium on Information, Computer and Communications Security, pp. 413–424, 2014.

[35] D. Wen, H. Han, and A. Jain, “Face spoof detection with image distortion analysis,” Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 746–761, 2015.

[36] J. Yang, Z. Lei, S. Liao, and S. Z. Li, “Face liveness detection with component dependent descriptor,” in IAPR International Conference on Biometrics, ICB, 2013.

[37] I. Pavlidis and P. Symosek, “The imaging issue in an automatic face/disguise detection system,” in Proceedings on Computer Vision Beyond the Visible Spectrum: Methods and Applications, pp. 15–24, 2000.

[38] N. Erdogmus and S. Marcel, “Spoofing attacks to 2D face recognition systems with 3d masks,” in IEEE International Conference of the Biometrics Special Interest Group, 2013.

[39] Keyurkumar Patel, Hu Han, and Anil K Jain, “Secure face unlock: Spoof detection on smartphones,” in proceedings of IEEE Transactions on Information Forensics and Security, vol.11, pp. 2268–2283, 2016.

[40] DiWen, Hu Han, and Anil K Jain, “Face spoof detection with image distortion analysis,” in proceedings of IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp.746–761, 2015.

[41] Jianwei Yang, Zhen Lei, and Stan Z Li, “Learn convolutional neural network for face anti-spoofing,” in proceedings of IEEE Conference on Computer Vision and Pattern Recognition, 2014.

[42] Yaojie Liu, Amin Jourabloo, and Xiaoming Liu, “Learning deep models for face anti-spoofing: Binary or auxiliary supervision,” in proceedings of IEEE Conference on computer vision and Computer Vision and Pattern Recognition, pp. 389–398, 2018.

[43] Zhenqi Xu, Shan Li, and Weihong Deng, “Learning temporal features using lstm-cnn architecture for face anti-spoofing,” in Journal of IEEE Access, pp. 141–145, 2015.

[44] R. Li, Q. Jiao, W. Cao, H.-S. Wong, and S. Wu, “Model adaptation: Unsupervised domain adaptation without source data,” in proceedings of IEEE Conference on Computer Vision and Pattern Recognition, 2020.

[45] Cheng, Jiaming, et al. "A deep adaptation network for speech enhancement: Combining a relativistic discriminator with multi-kernel maximum mean discrepancy”, In proceedings of IEEE Transactions on Audio, Speech, and Language Processing, vol. 29, pp. 41-53, 2020.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.