International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228248

A Survey on Anti-Spoofing Methods for Facial Recognition

Manoj G[+], Yashas D. S[+], Jeevan K. P[+], Likith M[+], Dr. Raghavendra R. J[*]

[+]Department of Information Science and Engineering, J N N College of Engineering, Shimoga, India

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

ABSTRACT

Article Info
Volume 8, Issue 2
Page Number : 259-268

Publication Issue :
March-April-2022

Article History
Accepted: 10 April 2022
Published: 29 April 2022

Despite significant development in facial recognition (FR), current FR systems are exposed to spoofing attacks like printed photo attacks, 3D mask attacks, video replay attacks, and many more. Several anti-spoofing approaches have been proposed to assess whether the person in front of the camera is real or fake. Developing effective protection mechanisms against these threats is a challenging task. This paper gives a brief overview of various presentation attack detection (PAD) techniques, which are categorized into intrusive and non-intrusive approaches. Each technique is examined in terms of its execution, benefits, and drawbacks and also provides information on modern anti-spoofing techniques.

Keywords: Face anti-spoofing, Facial Presentation Attack Detection (PAD), ELTCP, Information Security, face recognition, convolution neural network.

I. INTRODUCTION

As internet technology evolved, biometrics have received increasing attention. In the past few decades, the use of biometrics in numerous day-to-day applications, such as online payment security, online shopping security, mobile phone authentication, etc. Facial recognition has been one of the most researched technologies in the field of biometrics since the 1990s. With the growth, facial recognition had attained breakthroughs such as the achievement of SphereFace [1], FaceNet [2], DeepIDs [3], DeepFace [4], VGG Face [5] and ArcFace [6]. Individual faces are extremely distinguishable, and facial recognition can be performed in a non-intrusive manner (without user intervention) or from the ability to resist presentation attacks (PAs) [7].

A presentation attack is a process of demonstrating the user trait to the sensor. A face anti-spoofing system is a process of presenting the face of a person to the camera. When a genuine user presents his/her face to the camera, the system will allow access for that user. However, an unauthorized user may try to access the system by trying to impersonate a real genuine user. This type of attack is considered a presentation attack it may be performed by various means. All those means are to spoofing the system into thinking that the genuine user is accessing the system.

Spoofing is the act of impersonating a genuine user in order to obtain illegal access to a biometric system. The face is the easiest one to suffer from spoofing attacks as facial images are easily accessible. Face spoofing is a method of fooling the system using a picture, video recording, or 3D mask as a replacement for another individual face.

Presentation attacks are a threat to face anti-spoofing systems. Presentation attacks are roughly divided into two types: one, Impersonation attacks and two, Obfuscation attacks. ISO standard [8] recorded these types of attacks dedicated to biometric PAD as shown in Figure 1. In impersonation (spoofing) attacks, the intruder can use biometric data directly from a genuine user or create spoofs or fakes. Obfuscation attacks, on the other hand, are based on approaches to hide the user's true identity, such as plastic surgery, facial makeup or blockage of the face region. Impersonation attacks include photo attacks by displaying a photograph of the genuine user to the sensor. Playing a video of the genuine user to the sensor/camera video replay attacks is performed. In 3D Mask Attacks, a 3D replica of the face is shown to the sensor/camera.

Obfuscation attacks, in comparison to impersonation attacks, have a distinct objective (as the attacker's goal is to remain undetected by the system). Extreme makeup can significantly modify a person's facial features, such as making them appear older/younger by adding/hiding wrinkles, changing the shape of eyebrows, beard, and mustache, and partial occlusion (cloths/masks/sunglasses, etc.). Plastic surgery (to imitate a real user) or blockage of the face region (e.g., by using sunglasses or scarves). However, in some situations of obfuscation attacks copy of another person's biometric information is used. In this paper, we are reviewing both impersonation and Obfuscation anti-spoofing methods.

This paper is structured in this manner. Section 2 presents an overview of the most recent approaches for face anti-spoofing. Section 3 provides an analysis of modern approaches. Finally, in Section 4, we draw our conclusions.

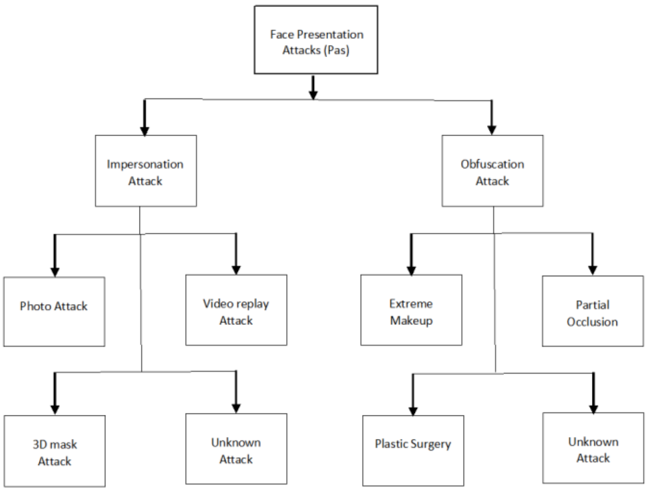

Figure 1. Different types of facial presentation attacks (PAs)

II. FACE ANTI-SPOOFING APPROACHES

Face anti-spoofing has become the main study direction for academia and industry due to the benefits of face biometrics such as safety, naturalness, and non-contact. However, the face anti-spoofing system is subject to spoofing attacks by unauthorized users, which introduce a serious threat to the performance of the system. Real and spoof faces have some variances we can develop several face anti-spoofing approaches by analyzing the advantages of these variances to differentiate between genuine and spoof faces. As a result, designing a face anti-spoofing system with very high accuracy is necessary.

By considering these criteria we are reviewing face PAD methods as shown in Figure 2. PAD methods are classified into liveness cues, texture cues, 3D geometric cues, multiple cues and convolutional neural network-based methods. In the following sections, we review each method in detail.

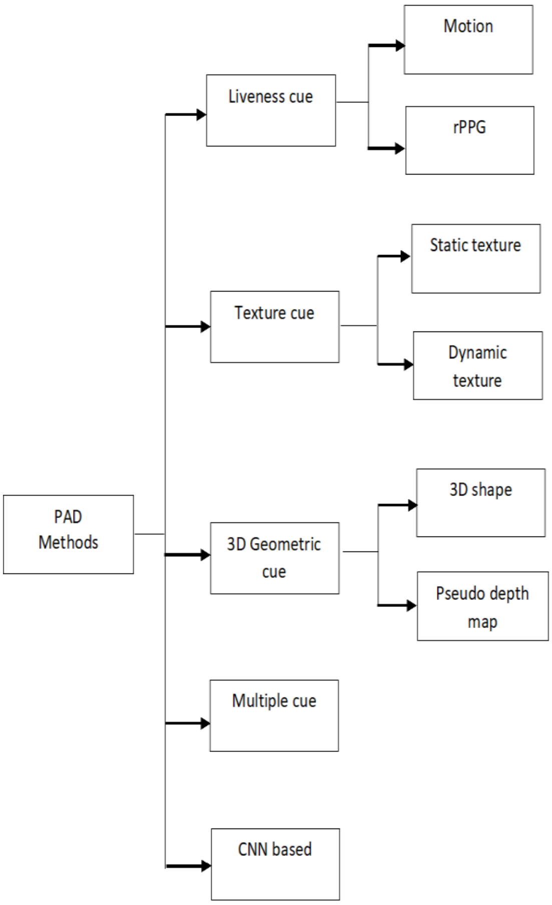

Figure 2. Classification of facial PAD methods

2.1 Liveness cue

The first attempt for facial PAD was based on liveness cues. A liveness cue-based method detects physiological signs facial movements, changes in facial expression, and pulse rate. Liveness cue-based methods may be further classified into motion-based and rPPG-based methods.

2.1.1 Motion-Based Methods

Static presentation attacks, such as photo attacks efficiently detected by conventional motion-based methods, by analyzing face/facial movement.

For the sake of facial authentication security, to improve the ability of face anti-spoofing techniques, a hierarchical neural network-based extensible multi-cues integration framework is presented. An interactive method is proposed by Kollreider et al. [10] for detecting replay attacks and photo attacks by analyzing the lips of the face presented when the user is instructed to utter some words or digits. The author used optical flowfield (OFF) to extract mouth motion. Pan et al. [11] proposed a non-intrusive spoof detection approach against photo attacks, by identifying natural eyeblinks. The optical flow was also used by Bao et al. [12] for this technique. The proposed method can identify whether the subject used is a 3D face or a printed photograph.

2.1.2 rPPG-Based Methods

It is hard to detect changes in the intensity of pulse/heartbeat in facial skin compared to head/facial movements, where it is not complex to detect. Remote PhotoPlethysmoGraphy (rPPG) in order to automatically detect these types of changes. rPPG can detect blood from a distance from an RGB image based on the study of differences in light absorption and reflection through the surface of human skin (in a non-intrusive way).

Nowara et al. [13] proposed PPG Secure; an RGB camera that can detect PPG signals caused by blood flowing through the circulatory system of a live skin region. These PPG signals are absent in areas that do not contain live skin regions. Signals from the rPPG are extracted from the face. The magnitudes of the Fourier spectrum of rPPG signals are then inputted into a Random Forest classifier [14]. A deep learning-based approach was proposed by Liu et al. [15] for learning rPPG signals, rPPG estimations were integrated with the 3D geometric cue estimation to block not only photo, also video replay attacks and 3D mask attacks. For heart rate prediction Fernandes et al. [16] proposed Neural-ODE [17]. In this, the heart rate is taken out from the original videos to train the model. Then, the trained Neural-ODE is utilized to project the heart rate of Deepfake videos.

2.2 Texture cue

Texture cue methods are the most popular and provide several advantages over other PAD methods. It gives very good results for different types of attacks. Static texture and dynamic texture cues are the two types of texture cue approaches. Static texture-based methods use a single image to extract spatial or frequential features. Spatiotemporal features are extracted from Video Sequences using dynamic texture-based methods.

2.2.1 Static Texture-Based Methods

The spatial texture features that may be extracted from a single image are known as static texture cues. A real-time and non-intrusive method is proposed by Tan et al. [18] by taking individual photos from a web webcam to tackle spoofing. The task is considered a binary classification problem. It is based on the Lambertian model [19]. Samples for testing are derived using Difference of Gaussian (DoG) filtering [20]. For classification Sparse Nonlinear Logistic Regression (SNLR) and Support Vector Machines are used.

A static texture-based approach was proposed by Kose et al. [21]. By using the depth image of the 3D mask attacks or texture (original) image, the LBP-based method effectively detects 3D mask assaults (from a database that is self-constructed).

2.2.2 Dynamic Texture-Based Method

Spatiotemporal characteristics are extracted using dynamic texture-based methods from a sequence of images. In contrast, spatial features are extracted from a single image in static texture-based methods. Pereira et al. [22] proposed the application of a dynamic texture using an operator, integrating both temporal and spatial information into a single descriptor. Using multiresolution strategy.

Using Dynamic Mode Decomposition (DMD) [24] and Tirunagari et al. [23] proposed a single image to represent the dynamic features of a video. This approach selects a representative frame by applying DMD to the original video. After that Local Binary Patterns (LBP) feature of the Dynamic Mode Decomposition (DMD) image is obtained and input into the support vector machine(SVM) to differentiate it as a real or spoof face. Using the LBP operator Pereira et al. [25] proposed an approach for face anti-spoofing detection using the dynamic texture. The methods main purpose is to analyze the facial microtextures that differentiate real from spoof faces. Raghavendra et al. [26-30] proposed more innovative feature descriptors such as ELTCP, DOG-ADTCP and EDDTCP for face anti-spoofing.

2.3 3D Geometric cue

The 3d (three-dimensional) geometric cues use two kinds of PAD that can be distinguished two-dimensional planar PAD that uses 3D geometric characteristics (e.g.,as a video replay or photo as attack) and a real face as with a three-dimensional structure. The three-dimensional form reconstructed from the two-dimensional picture acquired byas the face depth as as map and the RGB camera is the most extensively utilized three-dimensional geometric cue.

2.3.1. 3D Shape-Based Methods

3D shape-based methods are used for detecting facial landmarks and selecting the keyframes by capturing several images and videos from more than two viewpoints. Then, from the selected keyframes, 3D facial structures can be recovered.

Bai et al. [31] suggested and tested a new physics-based approach for detecting images recovered from printed material using a single image. The reflective component of the image reflects the micro-textures seen in the printed paper. A linear SVM classifier can obtain a False Acceptance as Rate of 2.2% and a False as Rejection Rate of 13% using features taken from this component (6.7% Equal Error Rate). By as recovering sparse 3D facial structures, Wang et al. [32] suggested a unique face liveness detection technique to prevent spoofing assaults. Authors can recognize facial landmarks and pick keyframes for a given movie or numerous photos collected from more than two angles, and then apply the spare 3D facial structure recovered from the selected keyframes.

For more than a decade, the computer version community has been working on deformable model fitting [33]. As a result, a variety of treatments have been offered, all of which have had various degrees of effectiveness. A method for making independent predictions about the locations of the model's landmarks and then combining them by enforcing a prior over their combined motion has shown a lot of promise. Ahadet al. [34] present an overview of MHI (Motion History Image) approaches and applications.

2.3.2 Pseudo as Depth Map-Based Methods

Depth as map methods can as produce a dense depth map from a sparse input, yielding a comprehensive 3D representation of as the world. Jourabloo et al. [35] proposed a as face alignment technique for as large-pose face photos that used the powerful as cascaded CNN regressor approach with 3DMM(3D Morphable model). A cascade as of CNN-based regressors estimates the camera projection as matrix and 3D form parameters in the face alignment issue, which is defined as a 3DMM fitting problem. Feng et al. [36] suggested a simple approach for reconstructing the 3D face anatomy while also providing dense alignment. To accomplish this, a 2D representation known as the XY position map is used to store the 3D form of a whole face in XY space, and then a basic convolutional neural network (CNN) is used to regress it from a single image.

Blanz et al. [37] presented a method for face recognition in various poses from full face to profile view and in a wide range of lighting including cast shadows and specular reflections. To account for these changes, algorithms use computer graphics to model the imaging process in 3D space and estimate the 3D shape and texture of a face from individual images. Atum et al. [38] proposed a novel dual-stream CNN approach to prevent face spoofing by extracting local features and integrated depth.

2.4 Multiple Cue-Based Methods

Multiple cues-based approaches identify a wide range of face presentation threats by combining diverse cues. Liveness features that rely on a single cue aren't always effective against all kinds of face spoofing attacks. A combination of complimentary multi-cues from many aspects can concurrently solve several attacks on particular sub-problems. As a result, multi-cues integration-based techniques achieved state-of-the-art outcomes.

Pan et al. [39] proposed a as method for facial PAD that used eye-blinking detection with context-matching texture-based scenes. The texture-based technique (reference image) is used to verify the consistency between the actual background and the background region. For accurate and efficient face anti-spoofing, Yan et al. [40] proposed 3 scenic clues as which are non-rigid motion (blinking, yawning, etc.), face-background as consistency and imaging banding as effect (imaging quality as defects in the spoof face are given). Face anti-spoofing cues can be obtained by combining three clues into a as single feature vector.

For combining the pseudo-depth as map cue and remote Photo Plethysmo Graphy (rPPG) for face PAD, Liu et al. [41] proposed employing CNN and recurrent neural as network (RNN) architecture. To jointly assess the depth of face pictures and the rPPG signal of as face video, CNN and RNN architectures are integrated. To as detect the shown face as real or fake, the estimated depth and rPPG are combined.

2.5 CNN Based Methods

A convolutional neural network (CNN) is a type of artificial neural network (ANN) used to evaluate visual imagery in deep learning. Several authors have recently demonstrated that CNN-based techniques perform well in PAD.

The first attempt to detect spoofing attacks using CNNs was claimed by Yang et al. [42]. A one-path AlexNet is utilized in this technique to learn the texture characteristics that best differentiate PAs. An SVM with binary classes replaces AlexNet's regular output (a 1000-way softmax). The fully as connected bottleneck layer is retrieved and put into the binary classifier SVM as a learned texture feature. Li et al. [43] proposed training a deep as CNN based on VGG-Face for facial PAD. In addition, the features retrieved from the CNN's multiple layers were combined into a single feature and put into an SVM for facial PAD.

To identify photo/video replay scams, Jourabloo et al. [44] first estimate the noise of given fake facial images (spoof pictures). The spoof picture contains both noise (such as reflection, blurring, and moire pattern) than the actual image in this study. A spoof picture may be recognized by thresholding the calculated noise because the distortion of a real image was considered to be null in this study. De-Spoof Net (DS Net), a Generative Adversarial Network (GAN) based on CNN, was presented to estimate the noise.

Liu et al. [45] proposed a as Deep Tree Network (DTN) based on CNN which analyses thirteen different attack types, including impersonation and obfuscation attempts. They adopted unsupervised tree learning to cluster the known PAs into eight semantic subgroups, which they then used as the DTN's eight leaf nodes.

III. MODERN APPROACHES

The mechanisms that make up some of the modern face anti-spoofing systems based on RGB cameras are described in this section. Face anti-spoofing recognition rate has substantially improved, and many new concepts have been proposed Some of them are:

1) Silicone mask face anti-spoofing detection.
2) Zero/Few-Shot learning-based PAD Method.

3.1 Silicone Mask Face Anti-Spoofing Detection

As high-quality silicone masks have living features, their assaults represent a bigger danger to face recognition systems. Based on facial motion and visual saliency features, Wang et al. [46] presented a face anti-spoofing spoofingsspoofing technique that detects silicone mask attacks. They created a Silicone as Mask Face Motion Video Dataset (SMFMVD) of 200 silicone mask face as videos and 200 genuine face videos for face anti-spoofing detection. These videos feature a variety of facial expressions from a total of 20 people. Furthermore, inspired by the observation that the facial movement of the silicone as mask face is not appropriate as that of the real face. To extract face texture features LBP operator was used, as well as a saliency-guided as histogram of the oriented as optical flow operator to collect facial motion as features in the temporal domain. Finally, to discriminate between actual and spoof faces and SVM is employed to integrate 2 groups of facial traits.

3.2 Zero/Few-Shot Learning-Based PAD Method:

The zero-shot learning-based PAD method involves training a model on some classes and then predicting a new class that the model has never seen before. As a result, multiple research teams are working on a new method to detect previously undetected face PAs. Hence this situation is named as Zero-Shot as Face Anti-spoofing (ZSFA).

Liu et al. [47] developed a CNN-based Deep Tree Network (DTN) that assessed multiple different types of attacks, including obfuscation and impersonation attacks. They employed unsupervised tree learning to cluster the known PAs into 8 semantic sub-groups, which they then used as the DTN's eight leaf nodes. The Tree Routing Unit (TRU) was then trained to route the known PAs to the appropriate tree leaf using the attributes of known PA learned by the tree nodes. To distinguish between spoofing attempts, a mask estimator module and a binary classifier were used in each leaf node. The depth map estimation presented in a previous study by the same author [48] is related to mask estimation. The anticipated mask and binary softmax classifier’s score may then be used to identify unseen assaults.

IV. CONCLUSION

In this paper, we look at some of the most prominent face Presentation Attack Detection (PAD) techniques. We've illustrated how facial PAD has changed over the last two decades. 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. While adding additional capability to make the device more resilient and computer-efficient for undetectable and unanticipated spoof assaults, the weaknesses of features against spoofing attacks must be addressed. We've also recognized a few of the most prominent contemporary developments in facial presentation attack detection, such as merging techniques to block many types of assaults or tackling previously undiscovered attacks.

V. REFERENCES

[1]. Liu, Weiyang, Yandong Wen, Zhiding Yu, Ming Li, Bhiksha Raj, and Le Song. "Sphereface: Deep hypersphere embedding for face recognition." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 212-220, 2017.

[2]. Schroff, Florian, Dmitry Kalenichenko, and James Philbin. "Facenet: A unified embedding for face recognition and clustering." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 815-823, 2015.

[3]. Sun, Yi, Xiaogang Wang, and Xiaoou Tang. "Deeply learned face representations are sparse, selective, and robust." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 2892-2900, 2015.

[4]. Taigman, Yaniv, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf. "Deepface: Closing the gap to human-level performance in face verification." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 1701-1708, 2014.

[5]. Parkhi O.M, Vedaldi A, Zisserman A, “Deep Face Recognition” In Proceedings of the BMVC, Volume 1, p. 6, 2015.

[6]. Deng, Jiankang, Jia Guo, Niannan Xue, and Stefanos Zafeiriou. "Arcface: Additive angular margin loss for deep face recognition." In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition, pp. 4690-4699, 2019.

[7]. Souza, Luiz, Luciano Oliveira, Mauricio Pamplona, and Joao Papa. "How far did we get in face spoofing detection?." Engineering Applications of Artificial Intelligence, pp. 368-381, 2018.

[8]. ISO/IEC JTC 1/SC 37 Biometrics. Information Technology—Biometric Presentation Attack Detection—Part 1: Frame-Work; International Organization for Standardization: Geneva, Switzerland, 2016.

[9]. Litong, Feng & Po, Lai & Li, Yuming & Xu, Xuyuan& Yuan, Fang & Cheung, Terence Chun-Ho & Cheung, Kwok-Wai, “Integration of image quality and motion cues for face anti-spoofing: A neural network approach”, In Journal of Visual Communication and Image Representation, pp. 451-460,2016

[10]. Kollreider, Klaus, Hartwig Fronthaler, Maycel Isaac Faraj, and Josef Bigun. "Real-time face detection and motion analysis with application in “liveness” assessment." IEEE Transactions on Information Forensics and Security 2, no. 3, pp. 548-558, 2007

[11]. Pan, Gang, Lin Sun, Zhaohui Wu, and Shihong Lao. "Eyeblink-based anti-spoofing in face recognition from a generic webcamera." In Proceedings of IEEE 11th international conference on computer vision, pp. 1-8, 2007.

[12]. Bao W, Li H, Li N, Jiang W, “A liveness detection method for face recognition based on optical flow field” In Proceedings of the International Conference on Image Analysis and Signal Processing, Kuala Lumpur, pp. 233–236, 2009.

[13]. Nowara E.M., Sabharwal A., Veeraraghavan A., “Ppgsecure: Biometric presentation attack detection using photopletysmograms” In Proceedings of IEEE International Conference on Automatic Face & Gesture Recognition, pp. 56–62, 2017.

[14]. Ho T.K.,"Random decision forests" In Proceedings of the 3rd International Conference on Document Analysis and Recognition, Volume 1, pp. 278–282,1995.

[15]. Liu, Yaojie, Amin Jourabloo, and Xiaoming Liu. "Learning deep models for face anti-spoofing: Binary or auxiliary supervision." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 389-398. 2018.

[16]. Fernandes S, Raj S, Ortiz E, Vintila I, Salter M, Urosevic G, Jha S, "Predicting Heart Rate Variations of Deepfake Videos using Neural ODE", In Proceedings of the IEEE International Conference on Computer Vision Workshops, Seoul, Korea, 2019.

[17]. Chen R.T, Rubanova Y, Bettencourt J, Duvenaud D.K, "Neural ordinary differential equations", In Proceedings of the Advances in Neural Information Processing Systems, pp. 6571–6583, 2018.

[18]. Tan, Xiaoyang, Yi Li, Jun Liu, and Lin Jiang. "Face liveness detection from a single image with sparse low rank bilinear discriminative model." In European Conference on Computer Vision, pp. 504-517. Springer, Berlin, Heidelberg, 2010.

[19]. Oren, Michael, and Shree K. Nayar. "Generalization of the Lambertian model and implications for machine vision." International Journal of Computer Vision 14, no. 3, pp. 227-251, 1995.

[20]. Tan, Xiaoyang, and Bill Triggs. "Enhanced local texture feature sets for face recognition under difficult lighting conditions." IEEE transactions on image processing 19, no. 6, pp. 1635-1650, 2010.

[21]. Kose N, Dugelay J.L, "Countermeasure for the protection of face recognition systems against mask attacks" In Proceedings of 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition (FG), pp. 1–6, 2013.

[22]. Freitas Pereira, Tiago de, André Anjos, José Mario De Martino, and Sébastien Marcel. "LBP–TOP based countermeasure against face spoofing attacks." In Proceedings of Asian Conference on Computer Vision, pp. 121-132. Springer, Berlin, Heidelberg, 2012.

[23]. Tirunagari, Santosh, Norman Poh, David Windridge, Aamo Iorliam, Nik Suki, and Anthony TS Ho. "Detection of face spoofing using visual dynamics." IEEE transactions on information forensics and security 10, no. 4, pp. 762-777, 2015.

[24]. Schmid P.J, Li L, Juniper M.P, Pust O, "Applications of the dynamic mode decomposition" Theor. Comput. Fluid Dyn, pp. 249–259, 2011.

[25]. Freitas Pereira, TD, Jukka Komulainen, André Anjos, José Mario De Martino, Abdenour Hadid, Matti Pietikäinen, and Sébastien Marcel. "Face liveness detection using dynamic texture." EURASIP Journal on Image and Video Processing 2014, no. 1, pp. 1-15, 2014.

[26]. 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.

[27]. 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.

[28]. 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.

[29]. 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.

[30]. 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.

[31]. Bai J, Ng TT, Gao X, Shi Y.Q, “Is physics-based liveness detection truly possible with a single image?”, In Proceedings of the 2010 IEEE International Symposium on Circuits and Systems, pp. 3425–3428, 2010.

[32]. Wang T, Yang J, Lei Z, Liao S, L, “Face liveness detection using 3D structure recovered from a single camera” In Proceedings of the 2013 international conference on biometrics (ICB), pp. 1–6, 2013.

[33]. Saragih, Jason M., Simon Lucey, and Jeffrey F. Cohn. "Deformable model fitting by regularized landmark mean-shift." International journal of computer vision 91, no. 2, 200-215, 2011.

[34]. Ahad Md, Atiqur Rahman, J. K. Tan, H. Kim, and S. Ishikawa. "Motion history image: its variants and applications." Machine Vision and Applications, pp. 255-281, 2012.

[35]. Jourabloo A, Liu X, “Large-pose face alignment via CNN-based dense 3D model fitting” In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 4188–4196, 2016.

[36]. Feng Y, Wu F, Shao X, Wang Y, Zhou X, “Joint 3d face reconstruction and dense alignment with position map regression network” In Proceedings of the European Conference on Computer Vision, pp. 534–551, 2018.

[37]. Blanz, Volker, and Thomas Vetter. "Face recognition based on fitting a 3d morphable model." IEEE Transactions on pattern analysis and machine intelligence 25, no. 9, 1063-1074, 2003.

[38]. Atoum Y, Liu Y, Jourabloo A, Liu X, “Face anti-spoofing using patch and depth-based CNNs”, In Proceedings of IEEE International Joint Conference on Biometrics (IJCB), Denver, pp. 319–328, 2017.

[39]. Pan, Gang, Lin Sun, Zhaohui Wu, and Yueming Wang. "Monocular camera-based face liveness detection by combining eyeblink and scene context." Telecommunication Systems 47, no. 3, pp. 215-225, 2011.

[40]. Yan J, Zhang Z, Lei Z, Yi D, Li S.Z,“Face liveness detection by exploring multiple scenic clues.”, In Proceedings of 12th International Conference on Control Automation Robotics & Vision (ICARCV), Guangzhou, China, pp. 188–193, 2012.

[41]. Liu, Yaojie, Amin Jourabloo, and Xiaoming Liu. "Learning deep models for face anti-spoofing: Binary or auxiliary supervision." In Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 389-398. 2018.

[42]. Yang, Jianwei, Zhen Lei, and Stan Z. Li. "Learn convolutional neural network for face anti-spoofing." arXiv preprint arXiv:1408.5601, 2014.

[43]. Li L, Feng X,Boulkenafet Z, Xia Z, Li M, Hadid A,“An original face anti-spoofing approach using partial convolutional neural network”, In Proceedings of the 2016 Sixth International Conference on Image Processing Theory, Tools and Applications (IPTA), Oulu, Finland, pp. 1–6, 2016.

[44]. Jourabloo A, Liu Y, Liu X, “Face de-spoofing: Anti-spoofing via noise modeling” In Proceedings of the European Conference on Computer Vision (ECCV), Germany, pp. 290–306, 2018.

[45]. Liu Y, Stehouwer J, Jourabloo A, Liu X, “Deep tree learning for zero-shot face anti-spoofing” In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, USA, pp. 4680–4689, 2019.

[46]. Wang G, Wang Z, Jiang K, Huang B, He Z, & Hu R, “Silicone mask face anti-spoofing

detection based on visual saliency and facial motion" Neurocomputing, 458, 416–427, 2021.

[47]. Liu Y, Stehouwer J, Jourabloo A, Liu X, "Deep tree learning for zero-shot face anti-spoofing" In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 4680–4689, 2019.

[48]. Liu Y, Jourabloo A, Liu X, "Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision" In Proceedings of Computer Vision and Pattern Recognition, pp. 389–398, 2018.

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.

Cite this article as :

Manoj G, Yashas D. S, Jeevan K. P, Likith M, Dr. Raghavendra R. J, "A Survey on Anti-Spoofing Methods for Facial Recognition", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 2, pp. 259-268, March-April 2022. Available at doi : https://doi.org/10.32628/CSEIT228248

Journal URL : https://ijsrcseit.com/CSEIT228248