Face Spoofing Detection: A Survey on Different Methodologies

Gency V G[1], Mrs. Chaithanya C[2], Mrs. Aysha Fymin Majeed[3]

[1]M.Tech Student in Image Processing, Govt. Model Engineering College, Thrikkakara, Kochi, India
[2]Assistant Professor, Dept. of Computer Engineering, Govt. Model Engineering College, Thrikkakara, Kochi, India
[3]Assistant Professor, Dept. of Computer Engineering, Govt. Model Engineering College, Thrikkakara, Kochi, India

---

Abstract - *Biometric authentication is a process which is based on the uniqueness of person's biological attributes or traits. Face recognition is a challenging field in the framework of biometric authentication where work is still in progress. The protection of these systems is crucial, as face recognition systems are vulnerable to different attacks. Face spoofing is a method of fooling the system using a picture, video recording or a 3D mask as a replacement for another person's face by impersonating a legitimate user to gain illegal access. Spoof attacks are categorized as 2D and 3D attacks. 2D attacks are performed with images and videos. 3D spoof attacks are primarily performed by using real user's mask. 3D mask counter-spoofing methods are important for an effective and fool proof face recognition system. Exploration of non-invasive facial spoofing detection systems based on software is primarily focused on analysing facial image luminance detail, thus discarding the chroma component, which is helpful in separating fake faces from real ones. The aim of this paper is to provide an outlook on the work that has been carried out in the field of face anti-spoofing over the last decade. The paper covers the different methodologies for the detection of face spoofing.*

Key Words: **Face anti-spoofing, Biometrics, Authentication, Spoof attacks, Face Recognition**

1. INTRODUCTION

In this modern era, everything is digitalized from ordering food to booking a taxi. All applications need an effective authentication scheme to provide data preservation and protection. Most of the conventional keys are now replaced by passwords. There exists a wide variety of authentication methods such as keys, passwords, biometrics, etc. Biometrics has the power to speed up authentication considerably faster, easier and more secure than traditional passwords on the basis of measurable physical traits such as face, iris and voice of an individual. Each individual possesses a unique collection of characteristics such as iris, face, DNA, fingerprint, voice and hand geometry. Apart from these, biometrics based on ECG signals has also emerged.

The processing flow of face recognition consists of feature extraction, training of the classifier and matching process. Face-recognition systems are vulnerable to various types of attacks which are divided into two major categories such as direct attack and indirect attack [1]. Direct attack occurs before information is inserted into the network by posing in front of the camera as a legitimate user. Anyone can perform a direct attack with the biometrics features of the legitimate user. Photographs or video of the user is sufficient to bypass the face recognition system while fingerprints can be taken from places such as doorknob and false fingerprint can be created using some copying material. Indirect attack requires a knowledge about the network and hacking expertise to intrude into the system. In indirect attack, at the time of feature extraction or classifier training, a hacker can change the details in the system.

2. FACE SPOOFING ATTACKS

Spoofing is the act of impersonating a genuine user to gain illegal access over the biometric system. Face is the easiest one to suffer from spoofing attacks as facial images are easily accessible ones. Face spoofing can be classified into two. They are 2D spoof attacks and 3D spoof attacks [2] shown in fig.1 .2D spoofing is done by photos and video of a legitimate user. Spoof attacks by using 3D mask of genuine user is 3D spoofing.

2.1 Photo Attack

The photo attack is a 2D spoof classification and the photo is displayed to the biometric device by an attacker to enter the system, such as a cell phone screen, notebook, and laptop, etc. The photo could have been captured by a digital camera, or retrieved from the social media. The dramatically advanced method of photo-attack in which high-resolution eye and mouth prints are morphed is photographic masks. The impostor is positioned behind at the moment of the attack so that such facial expressions are repeated, such as eye blinking.

2.2 Video Attack

Video attack is an advanced version of photo attacks. In this attack attacker takes a video of the real person using smartphone, tablet etc. The attacker plays the video at the time of facial detection and accesses the biometric modality due to proper face part movement Thus, it is more difficult to distinguish or track these forms of attacks.

2.3 3D Mask Attack

The 3D mask attack is a more advanced version of video and photo attacks due to the depth elements in the facial features. In 3D mask attack, the attackers make a 3D mask of the original person and thus making it more difficult to generate countermeasures against the spoofing. These attacks are less prevalent as compared to the other categories. The 3D masks are usually made of different materials and sizes i.e. paper, plastics and silicon etc.

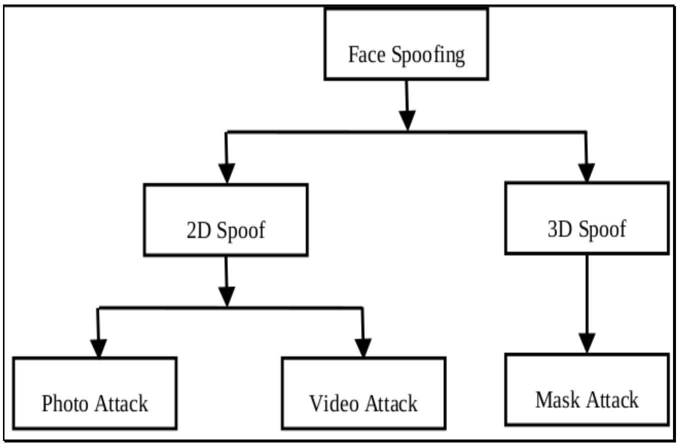

Fig -1: Face Spoofing Classification

3. LITERATURE SURVEY

Since face spoofing detection gains increasing attention recently, researchers have proposed a large quantity of methods in the literature to counter face spoofing [3]. Face Spoofing detection can be categorized into three: Motion based approaches, Image quality and reflectance-based approaches and Texture Based approaches. Motion based methods make use of the motions of face such as lips movements, eye blinking and some other motions to counter the photo attacks and display attacks. Image Quality and reflectance-based techniques are developed by the truth that the recapture image and video may cause an image quality drop and a reflectance difference. Texture based approaches simply divide into two types: hand-crafted features and CNN-based features. Handcrafted methods are algorithms used to describe texture features. CNN based methods are the recent methodology for face spoofing detection.

The general block diagram of a generic biometric system in which all three types of anti-spoofing techniques have been used is shown in Fig-2.

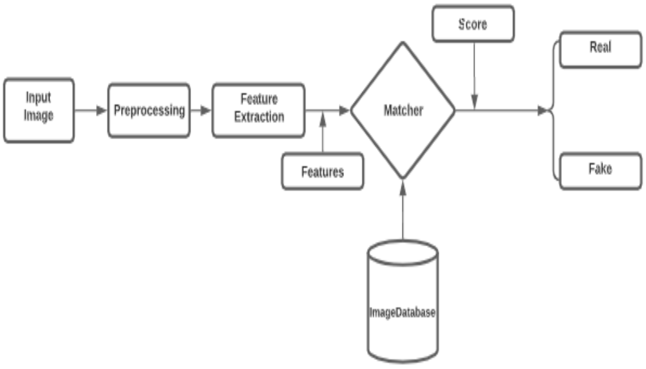

Fig.2: Face Recognition System

In 2010, Xiaoyang Tan *et al.* [4] implemented a method which is real time and non-intrusive one, focused on individual photographs from a web camera to detect face spoofing. The challenge is conceived as a problem of binary classification, where the distribution of positive and negative is essentially overlapping in the input space, and thus an adequate representation space is important. Using the Lambertian model, in terms of latent samples, two methods are used to obtain the critical details about various surface properties of a living human face or fake face. Two new extensions are built on the basis of these to the sparse logistic regression model that allows for fast and precise detection of spoof.

Jukka Mtitittti *et al.* [5] suggested a spoofing identification technique focused on learning micro-texture patterns that discriminate against fake live face images in 2011. Indeed, face prints usually include flaws in the material of printing that can be well recognized using micro-texture patterns. In comparison, human faces and prints reflect light in multiple ways, since a human face is a dynamic non-rigid 3D object, whereas an image can be viewed as a rigid planar object. This can cause various thoughts and shades of speculation. There are also distinct surface properties of actual faces and prints, such as pigments. In order to codify the micro-texture patterns into an improved function histogram, this technique used multi-scale local binary patterns (LBP). The support vector machine classifies the resultant histogram into fake and real.

Kose *et al.* [6] developed the Eulerian action magnification technique used in a recorded video in 2013 to improve the facial gestures typically shown by subjects. The fusion of Local Binary Patterns and Histogram of Optical flow descriptor is used for classification. The local binary patterns (LBP)encode the patterns of micro-texture into an improved feature histogram. The resultant is fed into a support vector machine classifier which determines whether there is a live person in front of the camera or not. This approach is efficient method for video attacks, robust, computationally fast and does not require user-cooperation.

In 2013, Pereira *et al.* [7] suggested a method using an operator named LBP-TOP that incorporates space and time data into a single descriptor using a multi-resolution technique. For dimensionality reduction and categorizing false and true faces, Linear Discriminant Analysis (LDA) is used in this approach. Low computation cost and good generalization capability are the main advantages.

Anil K Jain *et al.* [8] proposed an efficient and robust face spoof detection approach based on Image Distortion Analysis (IDA) in 2015. Four different characteristics that are derived to form the IDA feature vector are specular reflection, blurriness, chromatic moment, and color diversity. An ensemble classifier, consisting of multiple SVM classifiers trained for numerous face spoof attacks (e.g. written image and replayed video), is used to differentiate between real and spoof images. This technique is generalized using a voting-based scheme to multi-frame face spoof detection in videos.

S. Tirunagari *et al.* [9] proposed a motion-based approach by exploiting the information dynamics of the videos. The properties used for discriminating a live and fake face are blinking eyes, moving lips, and facial dynamics. As the primary algorithm, dynamic mode decomposition (DMD) is used to capture the liveness cues. A classification pipeline with a histogram intersection kernel composed of DMD, Local Binary Patterns (LBP), and Support Vector Machines (SVM) is used. DMD's special property is to reflect the entire video's temporal details as a single image that has the same dimensions as the images found in the video. DMD+LBP+SVM's pipeline proves to be reliable, easy to use and efficient method for face spoof detection.

Boulkenafet *et al.* [10] proposed a face anti-spoofing approach based on color texture analysis in 2015. Here, local binary pattern texture descriptor is used for texture analysis from luminance and chrominance component part of input image. The histograms are separately extracted from each image band. SVM classifier distinguish real and fake faces.

Visual codebooks of spectral-temporal cube strategies for face spoofing techniques were proposed by Allan Pinto *et al.* [11] in 2015. This algorithm was developed to detect spoofing attacks that take advantage of noise and artifacts produced during processing and recapture of synthetic biometric samples. Mid-level feature descriptors were used rather than low-level feature descriptors for discriminating real and fake faces. This proposed approach was tested on databases of images, videos, and 3D mask and the results obtained were 0.6 percent error rate on the different databases.

In 2016, Litong Feng *et al.* [12] suggested an extendable multi-cues integration architecture for face anti-spoofing using deep learning concept. The fusion method image quality and motion-based method is used for liveness detection. Shearlet is used to generate an image quality-based liveness feature. Motion-based features are extracted by dense optical flow. A fusion strategy for the bottleneck mechanism successfully combines various liveness characteristics. This fusion method incorporates liveness features from three aspects: the shearlet-based image quality feature, the optical flow-based face motion feature, and the optical flow-based scene motion feature.

Zinelabidine Boulkenafet *et al.* [13] in 2016 developed a method on CNN for face spoofing detection. This method is a hybrid solution for face spoofing using CNN, PCA and SVM. Firstly, on the facial spoofing data sets, the CNN is fine-tuned. Then, to reduce the dimensionality of features that can prevent the over-fitting problem, the block principal component analysis (PCA) approach is used. Finally, the support vector machine (SVM) is used to differentiate between the true and the false faces of the real.

In 2016, Aziz et al. [14] presented a measure to differentiate between a real face and a printed paper photo based on physical features of the materials based on reflection properties. To differentiate the reflections on different materials, polarized light (light that vibrates in a single direction) can be used. To produce the Stokes images, the Stokes parameters are applied, which are then used to construct the final image known as the Stokes linear polarization degree (SDOLP) image. All the SDOLP images are statistically analyzed and the mean, standard deviation and kurtosis of both materials (face and paper) are compared. The True Positive Probability (TPR) and the False Positive Rate (FPR) are calculated and compared the results, the SDOLP images provide significant distinguishable values between the real face and the paper mask. This method is robust for a small dataset which does not requires the specific classifier.

In 2017, Xiaochao Zhao *et al.* [15], presented a method on the representation and recognition of dynamic textures. A spatio-temporal descriptor based on LBC is utilized to achieve the goal. The VLBC descriptor thresholds the neighboring pixels with the central pixel in a local volume. The completed version of VLBC provides local contrast and central pixel intensity detail, which improves performance significantly. A joint 3D histogram is used exclusively to represent a sequence of Dynamic Texture (DT). For DT classification, the negative log probability distance-based closest neighbor classifier is used in the experimental assessment.

A new two-stream CNN-based approach for face anti-spoofing was introduced by Yousef Atoum *et al.* [16] by extracting local characteristics and holistic depth maps from the face images in 2017.The local features aids CNN to discriminate the spoof patches regardless of the spatial face regions. On the other hand, the holistic depth map explores whether a face-like depth is present in the input image. This approach utilizes both local and holistic features acquired for classifying real and spoof face samples. I The dense depth map for a live or spoof face image is estimated. A deep neural network is trained for the patch-based CNN stream to learn rich appearance features that can distinguish between live and spoof face images using patches randomly extracted from face images.

Arti and Meenakshi *et.al* [17] in 2018, introduced an approach to discriminate between real attempt and 3D mask attacks. The method is utilizing the texture as well as frequency for feature extraction. The facial skin and mask have different frequencies components. The mask has fewer high-frequency component. The signal is decomposed by wavelets into low-frequency and high-frequency sub-bands without any data loss. It is able to separate very fine details in a signal, so when LBP is applied on these separate sub-bands for better information. SVM classification is performed for distinguishing real and masked faces. The evaluation is performed on the publicly available dataset, 3D MAD Dataset from Idiap Research Center.

Mayank Yadav *et al.* [18] in 2018, propose the countermeasure for spoofing attacks in face recognition system. The Discrete Wavelet Transform algorithm is utilized for the analysis of spoof detection. The main purpose of discrete wavelet transform is decomposition of signal into high and low frequency components. The basis is that the spoof images lacks in higher frequency components. KNN classifier will be applied on the detected features in order to classify whether the face is spoofed or non-spoofed. KNN and SVM classifiers are used for comparative study on the performance of the system. KNN Classifiers outperforms SVM with respect to accuracy as well as execution time.

Taiamiti Edmunds *et al.* [19] in 2018, dealt with the problem of spoof detection by modelling the radiometric distortions created by the recapturing process. To model these radiometric transformations, a compact parametric representation is used and is used as characteristics for classification. Complex non-linearity transformations normally associated with lighting shifts are not taken into account in this model. The challenge of anti-spoofing comes down to recovering the radiometric transform. In reality, to solve this problem, heuristics are used as the exact luminance of the scene is unclear. It then calculates the radiometric transition between the image detected and its corresponding enrolled sample. The main advantages of this method are that accurate detection of print and replay attacks.

Shilpa *et al.* [20] in 2019, developed a fully unique wavelet CNN design for face spoofing detection. The convolution and pooling layers in CNNs are replaced with wavelet decomposition of image with auto stack encoder. A well-referenced network model, with wavelet CNN and stacked auto encoder as primary components. The input is given to both stacked autoencoder and wave CNN. After processing, a prediction from the output of stacked autoencoder and modified CNN is obtained which is given further for the detection output. The result of detection is obtained in the SoftMax layer in the form of whether the spoofing attacks are an original one or a printed or relay attack. The output is obtained in accordance with the input image given and the comparison of the trained images.

Zang *et al.* [21] in 2019, introduced an extreme light network architecture called Feather Nets as a countermeasure for face spoofing. The FeatherNet architecture consist of two blocks which is used as convolution layer and average pooling layer. The streaming module included in the architecture reduces the computational cost and storage cost, which is replaced for fully connected layer in CNN. For multimodal strategies a fusion classification with ensemble+ cascade classifiers are performed.

Haonan Chen *et al.* [22] in 2019, proposed a cascade face spoofing detector based on face anti-spoofing R-CNN and improved Retinex based LBP. The improved retinex based LBP uses iterative guided filter for illumination estimation and extracts improved retinex based LBP feature on different colour spaces. Finally, the two detectors output are cascaded to discriminate real and fake faces. The CASIA-FASD, REPLAY-ATTACK and OULU-NPU are the face anti spoofing datasets used in this method.

Wang et al. [23] in 2020, introduced an approach to detect presentation attacks in face recognition system. The stacked vanilla convolutions are used, where the detailed discriminative hints such as spatial gradient magnitude characteristics between living and spoofing are refined. In detecting the spoofing faces, the dynamics of 3D moving faces offer major clues. Here, the Residual Spatial Gradient Block discriminative information is effectively captured and encoded from the Spatio-Temporal Propagation Module. In addition, for more detailed depth supervision, a new Contrastive Depth Loss is used.

4. FACE ANTISPOOFING DATASETS

The earlier studies on face Presentation Attack Detection are based on private datasets. These private datasets, both in terms of volume and range of attack types, are very small, making it quite difficult to compare the various approaches equally.

NUAA Database [4] is the first freely open PAD face dataset for printed photo attacks. It requires some variability in the PAs, since the images are moved / distorted as follows in front of the PA acquisition device:

- 4 Translations
- 2 Rotations

- 2 Bending

The genuine face photographs are captured using a generic webcam. The attacks are performed by using printed photographs. The dataset, for testing and tests, is split into two different subsets. There are 1743 real face pictures and 1748 PAs in the training set impersonating 9 genuine people. 3362 authentic samples and 5761 PAs are in the test set.

PRINT-ATTACK Database [24] is the second public dataset suggested, containing photo-attacks that represent 50 separate legitimate people. The data is obtained in two distinct circumstances: controlled and adverse. The backdrop of the scene is uniform and the light of a fluorescent lamp illuminates the scene in controlled conditions. The atmosphere of the scene is non-uniform in adverse circumstances and daylight illuminates the scene.

CASIA-FASD Database [25] is the first publicly accessible face PAD dataset that includes printed picture and video replay attacks. This database consists of three types of attacks: warped printed photos (which simulates paper mask attacks), printed photos with cut eyes and video attacks (motion cue such as eye blinking is also included). The entire database is divided into a training set (20 subjects included) and a testing set (30 subjects included). Considering three different picture quality, three different attacks (warped / cut photo attack and video replay attack) and the overall test that incorporates all the details, seven test scenarios are planned.

The REPLAY-ATTACK Database [2]is an addendum to the **PRINT-ATTACK** database described above. REPLAY-ATTACK incorporates two more attacks compared to the PRINT-ATTACK database, which are Phone-Attack and Tablet-Attack. To view a video or photo attack, the Phone-Attack uses an iPhone screen and the Tablet-Attack uses an iPad screen to display high-definition digital images or videos (1024x768). Thus, REPLAY-ATTACK database can evaluate photo attacks with printed photo or screens, and video replay attacks.

The 3DMAD Database [26] is the first public face spoofing database available for a 3D mask attack. Previous databases provide threats with 2D attacks (i.e. photos or video) that are typically unable to fool PAD systems that rely on 3D signals. The attackers wear resin/plastic/silicon 3D face masks of a valid user in the 3DMAD database to access the system. It consists of paper-craft mask files. A total of 255 videos from 17 topics was included in the dataset.

MSU-MFSD Database [8] is the first publicly available database for mobile phones to take original accesses. MSU-MFSD database includes real access and attack videos for 55 subjects.

MSU-RAFS Database [27] is an extension to MSU-MFSD, CASIA-FASD and REPLAY-ATTACK. Here, the video replay attacks are produced by replaying the real face videos in MSU-MFSD, CASIA-FASD and REPLAY-ATTACK.

MSU-USSA Database [27] is as an extension of the **MSU-RAFS** dataset. It contains mainly two sub-sets is the database. The first subset consists of 140 subjects where 50 subjects are from REPLAY-ATTACK, 50 subjects from CASIA-FASD and 40 subjects from MSU-MFSD. The second subset consists of 1000 subjects collected from the web faces database.

OULU-NPU Database [28] is a newer dataset released in 2017 which covers mobile device-acquired PAD attacks. The photographs were obtained in restricted situations and has a spectrum of motion, blur, illumination, landscapes and head poses.

SiW Database [29] is the first database which provide facial spoofing attacks with multiple poses and facial expressions. This dataset contains 165 subjects from which 1320 genuine access videos are captured and also contains 3300 attack videos.

CASIA-SURF Database [27] is actually the largest multi-modal image facial anti-spoofing dataset mostly used for PAD. With 1000 subjects in 21,000 frames, RGB (1280x720), Depth (640x480) and Infrared (IR) (640x480) photos. Each sample includes one live video clip and six spoof video clips under different types of attacks. Six different photo attacks are included in this database: flat/warped printed photos where different regions are cut from the printed face.

5. EVALUATION METRICS

Anjos et al. [24] proposed in 2011 to use Half Total Error Rate (HTER) as an evaluation metric for face anti-spoofing. HTER is defined as the average of False Rejection Rate (FRR) and False Acceptance Rate (FAR) as follows:

$$HTER = \frac{FAR + FRR}{2} \quad (1)$$

Where FAR and FRR are defined as:

$$FAR = \frac{FP}{FP + FN} \quad (2)$$

$$FRR = \frac{FN}{FN + TP} \quad (3)$$

The numbers of True Positives, False Positives, True Negatives and False Negatives are TP, FP, TN and FN respectively. True Positive, False Positive, True Negative and False Negatives are estimated by the model parameters achieving Equal Error Rate (EER) on the validation set (parameters for which FRR=FAR).

However, performance is most frequently documented using the metrics described in the standardised ISO/IEC 30107-3 metrics [30] since 2017. Two assessment metrics are the Attack Presentation Classification Error Rate (APCER) and the Bona Fide Classification Error Rate (BPCER), also known as the Regular Presentation Classification Error Rate (NPCER These two metrics refer to the False Acceptance Rate (FAR and the False Rejection Rate (FRR) respectively, but the FAR is independently calculated for each type of attack to achieve APCER, and APCER is specified as the highest FAR (i.e. the FAR of the most effective type of attack). The Average Classification Error Rate (ACER) is then defined as the mean of APCER and BPCER using the EER on the validation set, similar to HTER.

The Receiver Operating Characteristic (ROC) curve and the Area Under the Curve (AUC) are often widely used to determine the output of the PAD system. The HTER and ACER have the advantage as they can provide a global assessment of the efficiency of the model over various parameter set values.

6. CONCLUSION

The increasing demand for efficient face based biometric technology has recently led to research work in the area of face spoofing that presents an issue of face recognition. The researchers focus to identifying false and authentic face samples in the last two decades. However, the suggested algorithms of detection for liveness and replay attack run on common spoof materials. Therefore, for unseen and uncertain spoofing attacks, generalised algorithms need to be applied. In order to add additional functionality to make the device more stable and computer-efficient for unseen and unexpected spoof attacks, the weakness of features against spoofing attacks must be taken into consideration.

REFERENCES

[1] Galbally, S. Marvel, J Fierrez, “Biometric ant spoofing methods: A survey in face recognition”, IEEE Access, vol.2, pp. 1530 -1552, 2014.

[2] Chingoyska, Ivana, Andre Rabello dos Anjos. “On the use of client identity information for face ant spoofing” IEEE Transactions on Information Security, vol. 10, no. 4, pp. 787-796, 2015.

[3] Hadid, Abdenour, Nicholas Evans, Sébastien Marcel, and Julian Fierrez. "Biometrics systems under spoofing attack: an evaluation methodology and lessons learned." IEEE Signal Processing Magazine, vol. 32, no. 5 pp. 20-30, 2015.

[4] Xiaoyang Tan, Yi Li, Jun Liu, and Lin Jiang, Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model.Springer, 2010.

[5] Jukka Mtitittti, Abdenour Hadid, Matti Pietiktiinen, Face Spoofing Detection from Single Images Using Micro-Texture Analysis, IEEE,2011.

[6] Neslihan Kose, Jean-Luc Dugelay, Reflectance Analysis Based Countermeasure Technique to Detect Face Mask Attacks, IEEE, 2013.

[7] Tiago de Freitas Pereira, Andre Anjos, Jose Mario De Martino1, and Sebastien Marcel, LBP – TOP Based Countermeasure against Face Spoofing Attacks, Springer, 2013.

[8] Di Wen, Member, Hu Han and Anil K. Jain. Face Spoof Detection with Image Distortion Analysis, IEEE Transactions on Information Forensics and Security, 2015.

[9] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. Ho, “Detection of face spoofing using visual dynamics,” IEEE transactions on information forensics and security, vol. 10, no. 4, pp. 762–777, 2015.

[10] Zinelabidine Boulkenafet, Jukka Komulainen, Abdenour Hadid. Face Anti-Spoofing Based on Color Texture Analysis, pages 1–8. IEEE, 2015.

[11] Allan Pinto, Helio Pedrini, William Robson Schwartz, and Anderson Rocha: Face Spoofing Detection through Visual Codebooks of Spectral Temporal Cubes. IEEE Transactions on Image Processing, 2015.

[12] Litong Feng, Lai-Man Po, Yuming Li, Xuyuan Xu, Fang Yuan, Terence Chun-Ho Cheung, Kwok-Wai Cheung. Integration of image quality and motion cues for face anti-spoofing: A neural network approach. Elsevier, 2016.

[13] Lei Li, Xiaoyi Feng, Zinelabidine Boulkenafet, Zhaoqiang Xia, Mingming Li, and Abdenour Hadid. An Original Face Anti-Spoofing Approach using Partial Convolutional Neural Network. IEEE, 2016.

[14] Azim Zaliha Abd Aziz, Hong Wei, James Ferryman. Face Anti-spoofing Countermeasure: Efficient 2D Materials Classification Using Polarization Imaging, IEEE, 2016.

[15] Xiaochao Zhao, Yaping Lin, and Janne Heikkil: Dynamic Texture Recognition Using Volume Local Binary Count Patterns with an Application to 2D Face Spoofing Detection.IEEE, 2017.

[16] Yousef Atoum, Yaojie Liu, Amin Jourabloo, Xiaoming Liu. Face Anti-Spoofing Using Patch and Depth-Based CNNs. In Proceedings of the IEEE joint conference on Biometrics. IEEE, 2017.

[17] Arti Mahore, Meenakshi Tripathi: Detection of 3D Mask in 2D Face Recognition System Using DWT and LBP. In Proceedings of the 3rd International Conference on Communication and Information Systems, IEEE, 2018.

[18] Mayank Yadav, Kunal Gupta: Novel Technique for Face Spoof Detection in Image Processing. Proceedings of the Second International Conference on Intelligent Computing and Control Systems. IEEE, 2018.

[19] Taiamiti Edmunds and Alice Caplier, Face spoofing detection based on colour distortions, Special Issue: Face Recognition and Spoofing Attacks IET, 2018.

[20] Shilpa S, Sajeena A. Hybrid Deep Learning Approach for Face Spoofing Detection. Proceedings of the

International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE, 2019.

[21] Peng Zhang, Fuhao Zou1, Zhiwen Wu, Nengli Dai Skarpness Mark, Michael Fu, Juan Zhao, Kai Li. FeatherNets: Convolutional Neural Networks as Light as Feather for Face Anti-spoofing. In 2019 International Conference on Computer Vision and Pattern Recognition Workshops.Pages 1574 - 1583. IEEE, 2019.

[22] Haonan Chen, Chen, Xiang Tiang, a Cascade Face Spoofing Detector Based on Face Anti-Spoofing R-CNN and Improved Retinex LBP, IEEE, 2019.

[23] Wang, Zitong Yu, Deep Spatial Gradient and Temporal Depth Learning for Face Anti-spoofing, IEEE, 2020.

[24] André Anjos and Sébastien Marcel. Counter-measures to photo attacks in face recognition: a public database and a baseline. In 2011 international joint conference on Biometrics (IJCB), pages 1–7. IEEE, 2011.

[25] Zhiwei Zhang, Junjie Yan, and et al. A face anti spoofing database with diverse attacks. In International Conference on Biometrics, pages 26–31. IEEE, 2012.

[26] Nesli Erdogmus and Sébastien Marcel. Spoofing 2d face recognition systems with 3d masks. In 2013 International Conference of the BIOSIG Special Interest Group (BIOSIG), pages 1–8. IEEE, 2013.

[27] Keyurkumar Patel, Hu Han, Anil K Jain, and Greg Ott. Live face video vs. spoof face video: Use of moiré patterns to detect replay video attacks. In 2015 International Conference on Biometrics (ICB), pages 98–105. IEEE, 2015.

[28] Zinelabinde Boulkenafet, Jukka Komulainen, and et al. Oulu-npu: A mobile face presentation attack database with real-world variations. In International Conference on Automatic Face & Gesture Recognition, pages 612–618. IEEE, 2017.

[29] Yaojie Liu, Amin Jourabloo, and X. Liu. Learning deep models for face anti-spoofing: Binary or auxiliary supervision. 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, pages 389–398, 2018.

[30] Iso/iec jtc 1/sc 37 biometrics. Information technology – biometric presentation attack detection – part 1: Framework. International Organization for Standardization, 2016.