Machine Learning Method for Face Spoofing: A Review

*** Mr. Arpit Neema**
Research Scholar, Computer Science,
Oriental University, Indore
Email- : arpitneema@gmail.com

**** Dr. (Lt.) Sanjeev Kumar Sharma**
Professor (CSE) and Dean Student Welfare
Oriental Institute of Science and Technology, Bhopal
Email- : spd50020@gmail.com

***** Dr. Deepak Sukheja**
Associate Professor, Department of Computer Science and Engineering
VNR Vignanajyothi Institute of Engineering & TechnologyGovt Engineering College, Hyderabad, Telangana, India
Email- : deepak_s@vnrvjiet.in

Abstract

Digital data has always been the most worthless asset of human beings. In modern years, it has gain large importance. With the initiation of technologies that use data, safety has become a major anxiety. Nearly all biometric systems use face detection. The industry around facial recognition technology is rapidly maturing due to advances in AI, ML and deep learning technologies. Facial recognition is a technology that is capable of recognizing a person based on their face. It employs machine learning algorithms which find, capture, store and analyse facial features in order to match them with images of individuals in a pre-existing database. These systems are unguarded against spoofing attacks due to lack of face liveness detection facilities. This paper gives a brief overview of various face anti-spoofing techniques. This paper also covers different methodologies for face spoofing detection, description of the experimentation databases available for face spoofing detection and aims to provide new research direction in this field.

Keyword: Biometrics, face liveness detection, face anti-spoofing, feature extraction, fusio*n.*

I. INTRODUCTION

In the last 10 years the term Machine Learning is penetrating in every sector like in Digital Assistant, Public and Online Transportation Networks, Web Medium Services, Videos Inspection, Face Recognition, Email Spamming Filtering, Search Engine outcome Refining, Online Support for any kind of Customer, Merchandise Recommendation, Web Fraud Detection etc.

In recent years Face identification techniques through machine learning has gain significant attention of the huge mass. Face spoofing is the latest form of spoof. It is a attack in which user can subvert or attack a **face** recognition system. Face spoofing term has come with lots of the extension of deep learning machinery and it has enhanced the precision of face identification [1] and created more appliances of face-oriented systems [2]. Every human face has its own privacy and individual identity. As a result, attackers are paying more attention to create spoof faces which breaks the identity original face.

With the moving of face recognition concept the subsequently step is to move in to new era that is “Face Spoof Detection System”. Face Spoofing Technique is most usable and latest trend for stopping frauds. Therefore, face spoofing attack detection (anti-spoofing) is becoming most important topic for research [3]. Many researchers have different approach to think spoofing attacks. Spoof detection is also called Bluff attack detection (BAD) which is a challenging target for search community.

Therefore, the Objective of the study is to analyse and investigate various existing methods explore various dataset for improving the prediction of Face Spoofing System.

II. LITERATURE SURVEY

A. Motion Analysis based Methods

Motion primarily based techniques goal at extracting liveness records which can distinguish the genuine face from the spoofed one thru eye blinking, lips movement, and head rotation.In [4], the planar object actions were detected as cues for translation, in-aircraft rotation, panning and out-of-plane rotation. In [5][6], the diffused movements of different facial parts had been extracted as essential features below the assumption that the real and spoofed faces may be distinguished through the movement cues.

Face motion-based Eye-blinking is a typical face motion cue wildly utilized in early work [7]. A human face is a non-rigid 3D object, exhibiting different optical flow trajectories compared with a 2D photo face.Kollreider et al. [8] assumed that the correlation between different facial components' motions is discriminant between real faces and photography faces. Bao et al. [9] proposed a motion model to describe the optical flow field of planar objects, and a divergence from this mode was assumed to exist in a real face's motion. Bharadwaj et al. [10] utilized Eulerian motion magnification to amplify subtle facial motions in a specialized frequency band. Macro- and micro-facial expressions presented by real faces can

Scene motion-based The motion correlation between the user and background can indicate the presence of a spoofing attack. Kim et al. [11] supposed that the face and body region has low consistency with the background and the extracted background should not change in a preset authentication environment. Anjos et al. [12] utilized optical flow correlation between the user head and the background scene to detect photo face spoofing attacks, and a HTER of 1.49% was achieved on the PHOTO-ATTACK database. In practice, varying scenarios will be presented to face authentication systems, especially with mobile internet apps. One pre-defined face motion-based or scene motion-based model is not suitable for a wide variety of authentication environments.

B. Texture Analysis based Methods

The idea of facial texture and distortion analysis originates from the assumption that the spoofed medium is likely to lack high-frequency information, due to the face media reproduction process. By analyzing the texture artifacts left behind during an attack, we can extract useful information such that the genuine and spoofed faces can be properly distinguished.

In it [13] author conducted research based on the study of contrast and dynamic texture features of both seized and spoofed photos. A modified version of the DoG filtering method, and local binary pattern variance (LBPV) based technique, which is invariant to rotation, were used. Support vector machine (SVM) is used when feature vectors are extracted for further analysis. The publicly available NUAA photo-imposter database is adapted to test the system, which includes facial images with different illumination and area. The accuracy of the method can be assessed using the False Acceptance Rate (FAR) and False Rejection Rate (FRR).

In [14] author has proposed a novel face anti-spoofing technique that uses two different color spaces Y*Cr*Cb and CIE*L*U*V. Six histograms are calculated each corresponding to one plane of these two-color spaces and they are combined into a single feature vector for a particular face image. Further, these feature vectorsare provided to an ExtraTreeClassifier for face spoofing detection. Though this method performs best, more number of color spaces need to be explored by the author.

In it [15] author exploit the joint colour-texture information from the luminance and the chrominance channels by extracting complementary low-level feature descriptions from different colour spaces. More specifically, the feature histograms are computed over each image band separately. Extensive experiments on the three most challenging benchmark data sets, namely, the CASIA face anti-spoofing database, the replay-attack database, and the MSU mobile face spoof database, showed excellent results compared with the state of the art.

C. Sensor based Methods

In addition to motion analysis and texture analysis methods, additional sensors can also be leveraged for face spoofing detection. One example is to leverage the infrared (IR) sensor which can help to reduce the influence of diverse illumination [16][17][18]. Another example is to utilize a specific LED and photodiodes with difference wavelengths [19][20] which can measure the reflectance information as the discriminative feature for face spoofing detection. We can also leverage other sensors which were already proved to be effective for face recognition task, including facial vein detection sensor [21], 3D face acquisition sensor [22–24] and thermal imaging sensor [25][26].

D. Deep Learning based Methods

Deep learning based methods have also been proved to be effective for biometric spoofing detection tasks. Yang et al. [27] first proposed to use Convolutional Neural Network (CNN) for face spoofing detection. In [28], CNN has been proved to be effective for face, fingerprint and iris spoofing detection. More recently, Atoum et al. [29] proposed depth-based CNN for face spoofing detection to extract depth information based on RGB face images. Wu et al. [30] proposed a pre-processing algorithm based on consecutive face video frames and further extracted discriminative feature with CNN. However, due to the lack of large-scale training data based on face anti-spoofing problem, these methods are lack of generalization capability.

Two CNN architectures namely Depth-based CNN & Patch-based CNN are proposed by the author in [31]. Random patches of an input image are fed to patch-based CNN to obtain patch scores while the entire image is supplied to Depth based CNN to obtain depth features that are in turn passed to SVM. Finally, the facespoofing detection is carried out by considering the output of SVM & patch spoof scores. In order to avoid overfitting, image patches are used by the proposed method for one of the CNN streams. In [32] the author proposes a novel CNN architecture called DeepColorFASD. After the color space conversion, each plane of the three color spaces (RGB, YCrCb, HSV) is passed to the DeepFASD network in order to obtain a corresponding color space score from the softmax layer. These scores are used by a fusion-based voting method for face liveness detection. Inter-database testing should be carried out to observe the robustness of this method. Approach based on Transfer Learning is applied in [33] by using ResNet-50 along with Long Short Term Memory (LSTM) to classify the images. LSTM units were used to extract temporal features. This method makes effective use of pre-trained CNN architecture called ResNet50.

III. DATABASE

A. NUAA Database

The database [34] is developed by Nanjing University of Aeronautics and Astronautics. It consists of both Real face images & forged face images of 15 candidates that are captured by generic webcam purchased from the local market. Each face image is having a size of 640 × 480 pixels. For performing photo attacks, each face image is printed on two types of papers: i) Photographic paper of size 6.8cm × 10.2cm for small and 8.9cm × 12.7cm for bigger resp. ii) A4 paper of 70g with a HP color printer. Dataset contains 5105 real and 7509 fake face images which are separated as a training set and testing set. The database is public.

Link: http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html

B. REPLAY-ATTACK Database

The database [35] is provided by IDIAP Research Institute. It is a superset of PRINT-ATTACK dataset. It includes 1300 videos of 50 clients. The dataset is divided into 4 sets: training, development set contains 60 real & 300 attack videos each, testing set contains 80 real & 400 attack videos and enrollment set which includes 100 real access videos. The frame rate for each video is about 25 Hz. Both the real as well as fake access videos are captured in different illumination conditions: adverse & controlled. Depending on the type of device used to produce an attack, the dataset can be divided into 6 different protocols which are: High-definition (tablet), Photo, Video, Mobile (phone), Print and Grandtest.

Link: https://www.idiap.ch/dataset/replayattack

C. CASIA-FASD Database

CASIA-Face Anti-Spoofing database [36] is created by the Chinese Academy of Sciences Center. The database consists of real & spoof attempts of 50 subjects which are segregated into training and testing sets. Face images are captured by using the following resolutions: low resolution (640 × 480 webcam), normal resolution (480 × 640 webcam) and high resolution (1920 × 1080 Sony HD NEX-5 camera). Warped photo, Cut photo and Video attacks are considered in the database.

TABLE-I
STATISTICS OF CASIA-IRISV3

Subset Characteristics	CASIA-Iris-Interval	CASIA-Iris-Lamp	CASIA-Iris-Twins
Sensor	CASIA close-up iris camera	OKI IRISPASS-h	OKI IRISPASS-h
Environment	Indoor	Indoor with lamp on/off	Outdoor
Session	Two sessions for most iris images	One	One
Attributes of subjects	Most are graduate students of CASIA	Most are graduate students of CASIA	Most are children participating Beijing Twins Festival
No. of subjects	249	411	200
No. of classes	395	819	400
No. of images	2,639	16,212	3,183
Resolution	320*280	640*480	640*480
Features	Cross-session iris images with extremely clear iris texture details	Nonlinear deformation due to variations of visible illumination	The first publicly available iris image dataset of twins
Total	A total of 22,034 iris images from more than 700 subjects and 1500 eyes		

Source: http://www.cbsr.ia.ac.cn/english/IrisDatabase.asp

D. OULU-NPU Database

The database [37] is created by the University of Oulu. Videos for this database are recorded through front cameras of 6 different mobile phones. The Oulu-NPU face presentation attack detection database consists of 4950 real access and attack videos. These videos were recorded using the front cameras of six mobile devices in three sessions with different illumination conditions and background scenes. The presentation attack types considered in the OULU-NPU database are print and video-replay. The attacks were created using two printers and two display devices.

TABLE-II

	Users	Real access	Print attacks	Video attacks	Total
Training	20	360	720	720	1800
Development	15	270	540	540	1350
Test	20	360	720	720	1800

Source: https://sites.google.com/site/oulunpudatabase/

IV. RESULT AND DISCUSSION

The paper discusses the research work performed in the field of Face spoofing method during previous year. From above we can say most popular anti-spoofing state-of-the-art solutions include Motion study which include Face liveness detection which is a mechanism based on an analysis of how ‘alive’ a test face is. This is usually done by checking eye movement, such as blinking and face motion. Other type of motion study is Contextual information techniques in which investigation of the surroundings of the image can be done. While in Texture analysis small texture parts of the input image are probed in order to find patterns in spoofed and real images. In Sensor based method Infra red, voice and 3D depth can be used. While in Deep learning method use of CNN technique is common.

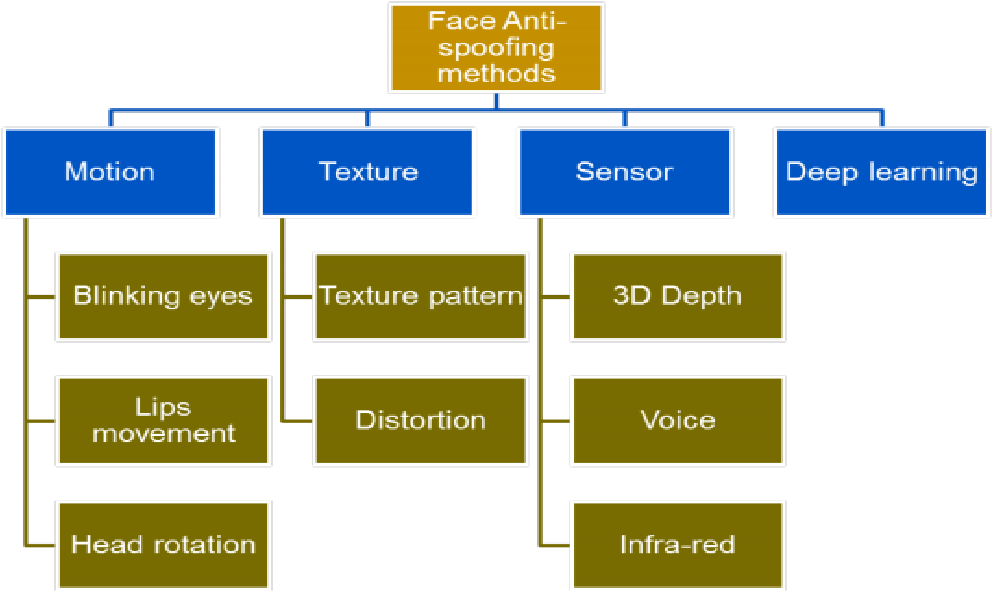

Figure. 1 Face Anti-Spoofing Methods

This paper also throw light on various database like NUAA Database**,** OULU-NPU DatabaseREPLAY-ATTACK and CASIA-FASD Database discusses various data set in which the data is split into generally in 3 sub-groups consist of training, development and Test Data. Training data, to be used for training anti-spoof classifier; Development data, to be used for threshold estimation and Test data is used to report error figures.

V CONCLUSION

This paper presents a brief study of various face anti-spoofing method which can be used as a quick reference by an expert as well as by the novice. Though the researchers focus to identifying false and authentic face samples in the last two decades. the spoofing attacks are also becoming mature gradually. A lot of sophisticated face spoofing methods has evolved so far. Available public databases are useful for study of face spoofing attacks, but the face anti-spoofing methods built by making use of them may not perform best in a few scenarios. In the future, there are many problems that need to be solved in order to tackle various faces spoofing attacks and making biometric systems more reliable as well as robust.

REFERENCES

[1] F. Schroff, D. Kalenichenko, J. Philbin", Facenet: A unified embedding for face recognition and clustering," Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 815-823, 2015.

[2] M. Chihaoui, A. Elkefi, W. Bellil, & C. Ben Amar", A survey of 2D face recognition techniques", Computers, vol. 5, no. 4, pp. 21, Dec-2016.

[3] L. Omar, I. Ivrissimtzis", Evaluating the resilience of face recognition systems against malicious attacks," BMVA Press, 2015

[4] G. Pan, L. Sun, Z. Wu, & S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera", IEEE 11th International Conference on Computer Vision , pp. 1-8, Oct-2007.

[5] X. Song, Q. Wu, D. Yu, G. Hu & X. Wu, "Face Anti-Spoofing Detection Using Least Square Weight Fusion of Channel-Based Feature Classifiers", EasyChair, Feb-2020.

[6] Y. Ma, L. Wu, Z. Li and F. liu, "A Novel Face Presentation Attack Detection Scheme Based on Multi-Regional Convolutional Neural Networks", Pattern Recognition Letters, vol. 131, pp. 261-267 Jan-2020.

[7] Y. LeCun, Y. Bengio and G. Hinton, “Deep learning”, Nature 521, pp. 436-444, May- 2015.

[8] Elloumi, W., Chetouani, A., Charrada, T. B., & Fourati, E., “Anti-Spoofing in Face Recognition: Deep Learning and Image Quality Assessment-Based Approaches,” In Deep Biometrics, Springer, Cham pp. 51-

69, 2020.

[9] Ma, Y., Wu, L., & Li, Z., “A novel face presentation attack detection scheme based on multi-regional Convolutional Neural Networks,” Pattern Recognition Letters, 131, pp. 261-267, 2020.

[10] Bharadwaj, S., Dhamecha, T.I., Vatsa, M., et al.,: ‘Face anti-spoofing via motion magnification and multifeature videolet aggregation’

[11] Kim, J.H. Yoo, K. Choi, A motion and similarity-based fake detection method for biometric face recognition systems, IEEE Trans. Consumer Electron. 57 (2) (2011) 756–762.

[12] A. Anjos, M.M. Chakka, S. Marcel, Motion-based counter-measures to photoattacks in face recognition, IET Biomet. 3 (3) (2014) 147–158.

[13] Hasan, Md Rezwan & Mahmud, S & Li, Xiang. (2019). Face Anti-Spoofing Using Texture-Based Techniques and Filtering Methods. Journal of Physics: Conference Series. 1229. 012044. 10.1088/1742-6596/1229/1/012044.

[14] Valter Costa, Armando Sousa, and Ana Reis, “Image-Based Object Spoofing Detection”, 19th International Workshop on Combinatorial Image Analysis, Porto, Portugal, (2018) November 22-24.

[15] Z. Boulkenafet, J. Komulainen and A. Hadid, "Face Spoofing Detection Using Colour Texture Analysis," in *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1818-1830, Aug. 2016, doi: 10.1109/TIFS2016.2555286.

[16] K. Jain, R. Bolle, and S. Pankanti, Biometrics: personal identification in networked society. Springer Science & Business Media, 2006, vol. 479.

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

[18] X. Sun, L. Huang, and C. Liu, “Context based face spoofing detection using active near-infrared images,” in Pattern Recognition (ICPR), 2016 23rd International Conference on. IEEE, 2016, pp. 4262–4267.

[19] Y. Kim et al., “Masked fake face detection using radiance.

[20] Z. Zhang et al., “Face liveness detection by learning multispectral reflectancedistributions,” in IEEE International Conference on Automatic Face & Gesture Recognition and Workshops, 2011, pp. 436–441.

[21] A. Seal et al., “Automated thermal face recognition based on minutiae extraction,” International Journal of Computational Intelligence Studies, vol. 2, no. 2, pp.133–156, 2013.

[22] K. W. Bowyer, K. Chang, and P. Flynn, “A survey of approaches and challenges in 3d and multi-modal 3d+ 2d face recognition,” Computer vision and image understanding, vol. 101, no. 1, pp. 1–15, 2006.

[23] X. Xie et al., “One-snapshot face anti-spoofing using a light field camera,” in Chinese Conference on Biometric Recognition. Springer, 2017, pp. 108–117.

[24] N. Kose and J.-L. Dugelay, “Reflectance analysis based countermeasure technique to detect face mask attacks,” in Digital Signal Processing (DSP), 2013 18th International Conference on. IEEE, 2013, pp. 1–6.

[25] P. Buddharaju et al., “Physiology-based face recognition in the thermal infrared spectrum,” IEEE transactions on pattern analysis and machine intelligence, vol. 29, no. 4, pp. 613–626, 2007.

[26] G. Hermosilla et al., “A comparative study of thermal face recognition methods in unconstrained environments,” Pattern Recognition, vol. 45, no. 7, pp. 2445–2459, 2012.

[27] J. Yang, Z. Lei, and S. Z. Li, “Learn convolutional neural network for face antispoofing,” arXiv preprint arXiv:1408.5601, 2014.

[28] D. Menotti et al., “Deep representations for iris, face, and fingerprintspoofing detection,” IEEE Transactions on Information Forensics and Security, vol. 10,no. 4, pp. 864–879, Apr 2015.

[29] Y. Atoum et al., “Face anti-spoofing using patch and depth-based cnns,” in In Proceeding of International Joint Solution Using a Multi Channeled Color Spaces CNN”, IEEEConference on Biometrics, Denver, CO, October2017Anti Spoofing.

[30] L. Wu et al., “Motion analysis based cross-database voting for face spoofing detection,” in Chinese Conference on Biometric Recognition. Springer, 2017, pp. 528–536.

[31] Yousef Atoum, Yaojie Liu, Amin Jourabloo and Xiaoming Liu, “Face Anti-Spoofing Using Patch and Depth-Based CNNs”, The International Joint Conference on Biometrics (IJCB 017), Denver, Colorado, United States, (2017), October 1-4.

[32] KaoutharLarbi, WaelOuarda, HassenDrira, Booulbaba Ben Amor, and Chokri Ben Amar, “DeepColorFASD:FaceInternational Conference on Systems, Man, andCybernetics (SMC), Miyazaki, Japan, (2018) October, pp. 4011-4016.

[33] Fang, “Ultra-deep Neural Network for Face Anti-spoofing”, Book Neural Information Processing: 24th International Conference on Neural Information Processing, Guangzhou, China, vol. 10635, (2017), pp. 686-695.

[34] X.Tan, Y.Li, J.Liu and L.Jiang, “Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model”, 11th European Conference on Computer Vision (ECCV'10), Crete, Greece, (2010), September 2010 5-11.

[35] Ivana Chingovska, Andre Anjos and Sebastien Marcel, “On the Effectiveness of Local Binary Patterns in Face Anti-spoofing”, Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG), January (2012), Darmstadt, pp. 1-7.

[36] Junjie Yan, Sifei Liu, Zhen Lei and Zhiwei Zhang, “A face antispoofing database with diverse attacks”, 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, (2012), March 29 – April 1.

[37] ZinelabidineBoulkenafet, JukkaKomulainen, Lei li, Xiaoyi Feng and AbdenourHadid, “OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations”, 12th IEEE International Conference on Automatic Face and Gesture Recognition (FG), Washington, DC, (2017), May 30 – June 3.