ISSN No:-2456-2165

Anti Spoofing Face Detection with Convolutional Neural Networks Classifier

Akash Chaudhary, AnkitaSingh, Km.Yachana
Department of Computer Science and Engineering (CSE)
Galgotia's College of Engineering and
Technology (GCET) Greater Noida, India

Ritu Dewan
Galgotia's College of Engineering andTechnology (GCET)
Greater Noida, India

Abstract:- The ability to detect spoofed faces has become a critical concern in various applications, such as face recognition systems, banking, and security measures. Thisresearchpresentsa simple system that can detect whether a facein video stream is spoofed or real using pre-trained models for face detection and anti-spoofing. The system uses a continuous loop to read each frame of the video stream, to assess whether a face image is real or spoof, first detect faces using the pre-trained face detection model, then crop and resize the face image. If the model predicts that the face is fake, the system draws a red rectangle around the face and displays the label "spoof." If the model predicts that the face is real, the system draws a green rectangle around the face and displays the label "real." The proposed system achieved a high accuracy rate in detecting spoofed faces, making it suitable for real-world applications.

Keywords:- *Facebiometric, liveness detection, Anti-spoofing, Fraud prevention, Face Spoofing detection, Convolutional neural networks.*

I. INTRODUCTION

The face is the mostly use biometrics technology in software, the identification of an individual is done by comparing the captured images with the stored images of that person in real time. These recognition systems are in the rapid development phase and are accumulated with a new strong algorithm that improves the system day by day. However, these systems are facing many security issues as frauds are increasing on a daily basis.There is a need to upgrade these systems to make them more secure, reliable and automatic.Facial recognition systems can be attacked to present faces that are not real. Face spoofing is an attack by presenting a fake face on camera. Simply the face which is provide to a biometric system is not from the real authorized person and someone try to breach the security by providing the photo, video or 3d mask of an authorized person to breach the security system is called spoofing attack.One spoofing attack that stand out among the other for its damage is facial spoofing. Also, a person's face is significantly simpler to get than other biometrics like their fingerprints. Using social media or a person's profile picture, it is simple to find out someone's face.The purpose of face antispoofing detection is to identify original and spoof face images.Face Liveness Detection [1] is a technology in face recognition which checks whether the image from the webcam comes from a live person or not. Face Liveness Detection is a crucial requirement for a system that uses facial recognition.Attacks that refer someone's face might be static or dynamic. Whereas dynamic attacks use video replays [2] or several photographs in a sequence, static 2D demonstration spoofing attacks use photos or masks. Attacks in static 3D demonstrations may make use of 3D sculptures, prints, or even masks, whilst in animated versions, sophisticated robots are used to mimic facial expressions, replete with make-up.Fake and real face images have various material patterns. The reality is that when features are recreated from camera photos [3], the clarity of facial emotions and reflectivity gaps are degraded. Different manipulated theRGB or LBP variations of color texture,have been used in several prior experiments to try and depict the distinction. Similar studies have also employed classification methods like closest neighbors or support vector machines. The reliance on the lighting in the room, on the other hand, is a flaw of this texture analysis method. It may be difficult to distinguish the original face texture of imitations in certain room settings, such as dark rooms.One extremely accurate liveness detection assessment is eyeblink detection. The simple act of natural blinking can reveal whether a visage is alive or not. During a blink, the eyes are closed for about 250–300 milliseconds. The typical individual blinks five to ten times per minute. Eye blink recognition can be used to analyze facial features and determine the surface area of the eyes. However, depending on blinking eye recognition is insufficient because modern technology makes it simple to target video recordings using tools like cellphones or iPads.Requests and responses are yet another effective anti-spoofing [4] strategy. This method makes use of an original action known as a challenge. The device's purpose is to verify challenges that occurred while watching a movie. A challenge-response system relies on a series of tasks to validate an individual's identification [5]. Despite being successful, this process needs more input and could have a negative impact on the user experience.

The goal of the movement recognition method is to identify vital indicators by analyzing [6] each unique facial movement. This movement separates humans from inanimate things like photographs. A change in the way someone looks, blinks their eyes, or moves their lips is one of the most common motion recognition methods. In most cases, motion-based assessment techniques are sufficient to avoid passive representation strikes.A real method of fraud prevention is the real-time inspection of faces, such as eye blinks and lip movements. However, this approach is powerless against video replay attacks.The most reliable method of anti-spoofing would be 3D sensors or photoplethysmography. Since we can distinguish between a visage and a planar object, specific pixel depth guidance may provide high accuracy against demonstration assaults. However, webcams continue to be one of the most reliable face anti-spoofing methods available.

Additionally, few clients have cameras on their PCs despite having access to them, and it is unsuitable for use with mobile devices like cellphones.Face spoofing detection is becoming increasingly popular. [7],In the literature, many different strategies have been put forth by researchers to stop face spoofing. Face Spoofing detection can be categorized in quality of image, Movement based, reflectance-based and Texture Based detection [8]. These handcrafted characteristics [11] are exclusive to particular counterfeit versions., scene conditions and fake devices [12], It limits how generalizable they can be. The efficiency of anti-spoofing approaches has recently been enhanced by convolutional neural networks which is based on deep learning methods, which develop sensitive end-to-end discriminative representations.Tofind difference between spoof and real faces, thisstudy suggests an enhanced face liveness detection algorithm using CNN. It is simple and most significantly, it can judge real and fake faces through different attack methods. Here is a detailed introduction to the important working process.

Our method can be implemented without the need of additional hardware equipment to be added.Real-time detection and robust capability are both features of our visage anti-spoofing system. In complex real-world interior or outdoor situations, it can manage various spoofing assaults (print, replay, and disguise).Ourrecommended method is completely accurate because it employs CNN and deep transfer learning [6] to identify signals that represent the features of both real and fake faces.

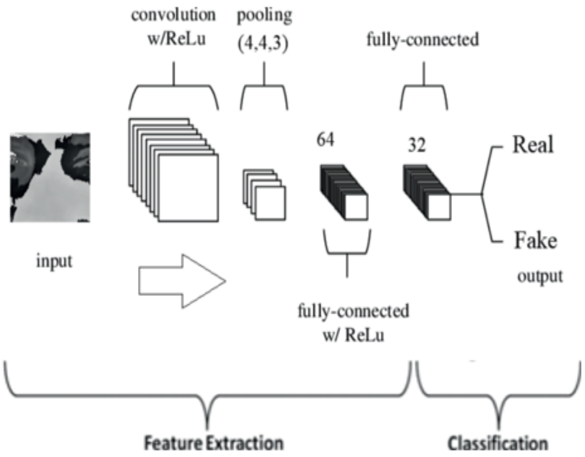

Fig. 1: Convolutional Neural Network Algorithm Model [21]

II. RELATED WORK

There are three of databasesbackground subtraction, data classification, andfeature learning are used to determine whether it produces results that perform better with the state of the art.Cross-type tests are then used to test the technique's ability to manage all properties and attacks from all three databases, and cross-dataset tests are used to compare each data sequence used in the testin order to validatethe approach [1]. Detect if an input is fraudulent or normal by processing the input image to remove image noise for efficient execution and multi-part digital images [2]. By reducing the size of the cheat clues for real-time samples while placing no explicit restrictions on cheat samples, a cheat hint generator mimics cheat hints for closed real-time sample and open cheat sample. The suggested systemstate of the art outperforms on the well-known Red Green Blueface anti-spoofing dataset without any extra depth or temporal information [3].

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 lack in higher frequency components [4]. The Semantic Feature Augmentation module generates paradoxical noise by making real-time and misleading features semantically conscious. As part of face anti-spoofing, SFA takes into account contrasting data categories and model texture bias, improving the attack success rate by almost 40%. But the annotation of facial features and modern networks do not guarantee that the model resists adverse attacks [5]. A technique that enables networks to assess their own domains using middle-layer grouped convolutional feature statistics without identifying the domain as a dataset [7]Modified versions of the Local Binary Pattern Deviation (LBPV)-based (rotation-invariant) DoG filtering method and techniques have been specified for use with support vector machines (SVMs), and the base publicly available NUAA dataset was adapted for the test system, performing better on key metrics compared to other cutting-edge technologies [8].

Fully unique wavelet CNN design for face spoofing detection. convolution and pooling layers in CNNs are replaced with wavelet decomposition of image with auto stack encoder. Output is obtained in accordance with the input image given and the comparison of the trained images [9]. A 3D mask attack detection system in the visible spectrum is proposed through CNN-based presentation attack detection (PAD) and blink detection. The method uses a maximum pooling process to learn the texture proofs for the final convolutional layer of a CNN. Two public tests of the proposed PAD approach have been conducted. Available datasets include paper masks and silicone. There are also YouTube videos featuring 3D latex masks. They get higher accuracy on datasets and YouTube videos [10]. Methods for full extraction of texture features that are hand-crafted or rely solely on deep neural networks [11]. The CNN network by which anti spoofing face detection is based uses texture and color information fromimage of face. Information of texture of colorcombineswithcolor difference channels and luminance, analyze with using descriptors of local binary pattern. The scheme performs better than cutting-edge techniques created in earlier research [12].

This model automatically pay attention to specific regions, and it can analyze network behavior. Thecollectionsolution of data combined with synthesis of data technology which simulate spoofed face attacks which is based on digital media that can easily help to obtain a big amount of training data that reflecting the real scene. and significantly outperform traditional techniques on publicly availabledatasets of face anti-spoofing [13].Fusion-based methods [18] work by merging two complementary images, namely an RGB image and a MSR image. The proposed framework is trained and validated by the standard CASIA_SURF dataset, achieving improved results over existing work [14]. For multimodal strategies a fusion classification with ensemble cascade classifiers are performed [15]. Features are extracted with using LBP or directed gradient histogram, Principal Component Analysis and Linear Discriminant Analysis are used. Only pertinent data should be retained in the feature vector, features are assigned to nearest neighbors with classifiers to detect the fraud. To determine robustness of the methodtesting should be performed with Cross-database [17].

Anti-face spoofing R-CNN and improved retina-based LBP are combined to create a cascade face spoofing detection with different face anti - spoofing datasets used in the method [19]. The stacked vanilla convolutions give detailed discriminative hints such as spatial gradient magnitude characteristics between living and spoofing are refined [20].The visual approach presents the different modalities to visual spectrum face recognition system for spoofing attacks and introduced datasets which is publicly available for the counter measure performance and recognition system vulnerability [22]. The two stream approach of CNN face anti spoofing that extract holistic depth map from face image and local feature of the face image where local feature facilitate CNN to discriminate spoof patches independently of spatial face areas and holistic depth map is to examine the input image whether it have face like depth [23].The face anti spoofing dataset that have pose variation, subject and illumination in a large range is also have depth based feature system to distinguish between spoof and live faces [24]. The approach that learns to detect the structure and dynamic of micro texture of the face that help system to characterize between the spoof and real face which is evaluate on publicly available datasets (CASIA and Reply Attack database) [25].

III. METHODOLOGY

The face spoofing is an attack in which an attacker uses the photo, video or 3d maskof an authorized person face to breach the live security system with the intention of steal its identity. Where anti spoofing face detection is system which help to differentiate between the spoof which is used by attacker and real face of authorized person. The steps and process are performed in order to make a anti spoofing face detection system along with the necessary libraries.

Pre-processing steps captured face photo has better photo quality than a retake face photo; thus, the recovered image contains fewer high-frequency components.By comparing the fake and the real face, this circumstance can be identified.Detecting whether a face in a video stream is spoofed and real. Itusesa trained face detection modelin a video stream to detect featuresof face, then passes the face through a trained anti-spoofing model to determine if it is spoofed or real.

The necessary libraries for image processing, including OpenCV, NumPy, and TensorFlow. It also loads thetrained models required for face detection and anti-spoofing. The program then captures a video stream using the System default camera. It runs a continuous loop to read each frame of the video stream and detect faces using the pre-trained face detection model. For each detected face, the program crops the face image and resizes it to 160x160 pixels before passing it through the anti-spoofing model to determine if it is spoofed or real. If the model predicts that the face is fake (spoof), the program draws a red rectangle around the face and displays the label "spoof" If the model predicts that the face is real, the program draws a green rectangle around the face and displays the label "real". The program then displays the processed video stream on the screen.

IV. IMPLEMENTATION

Our face anti-spoofing system consists of two main components: a pre-trained face detection model and a deep learning anti-spoofing model. The face detection model is used to detect faces in video streams and extract face regions for processing. We used the Haar Cascade classifier for face detection, which is a popular and effective method for detecting faces in real-time video streams. A deep learning model that has trained to discriminate between spoofed and real faces is the anti-spoofing face detection model. For the anti-spoofing model, we apply a convolutional neural network architecture, which has previously produced encouraging results. The cropped face image from the face identification model is the input for our anti-spoofing model, and outputs a probability score indicating whether the face is real or fake.We trained our anti-spoofing model on available datasets.A binary cross-entropy loss and accuracy combination as the training objective andAdam optimizer is use to trained the model. The cascade classifier based on Haar features given by OpenCV is used in the algorithm's face detection section. our anti-spoofing model achieves high accuracy across the dataset.

To extract high-level features from photo of faceConvolutional neural networks is used. A CNN is made up of numerous convolution and pooling layers that figure out how to represent the input image hierarchically. A fully linked network is then fed the CNN's output for categorization. Multiple dense layers make up a fully connected network, which learns to map input features to output labels. A dataset of actual and fake facial photos was used to train and test the system. The dataset contains 2102 images of real faces and 2118 images of fake faces generated from printed photos or video playbacks. There are 4220 face images in total. The test dataset contains 477 images of real faces and 474 images of fake faces. There are 951 face images in total.

Table 1: Datasets items

TRAINING DATASETS		TESTING DATASETS	
REAL	2102	REAL	477
SPOOF	2118	SPOOF	474
TOTAL	4220	TOTAL	951

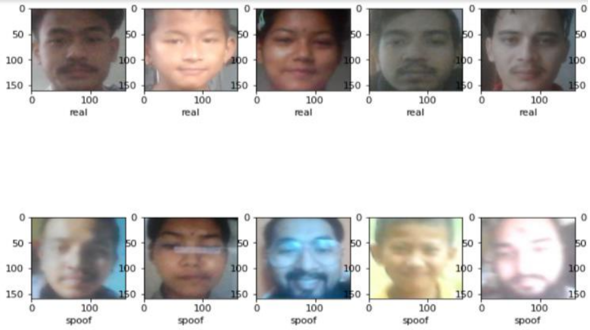

Fig. 2: Sample image from the dataset

The set of data is split in two. The test setandtraining set in an 80:20 ratio. Using backpropagation and gradient descent, the training set is utilised to optimise the training of CNNs and fully connected networks.

The test set is employed to gauge system effectiveness.

- **Input Image -** Facial Image A digital image of the face with sufficient resolution and image quality for automatic biometric matching. Further development of sensor-captured images for facial spoofing detection.
- **Pre-processing -** Preliminary processing of data for initial processing or further analysis. The term can apply to any first processing step or preliminary step when multiple steps are required to prepare the data for the user. Pixel brightness conversion/brightness correction. geometric transformation. Image filtering and segmentation.
- **Feature extraction-** A universal term for techniques for creating variables combinationsthat get around these issues while accurate represent the data. Most machine learning experts think that the secret of best model development has optimised feature extraction.
- **A matcher-** uses a search distance method to search matching features in two photos. In order to detect or infer features from the source image and transferred them to the target image, one of the images is referred to as the as the target image and the othersource image.
- **Image Database-** An organized collection of digital images designed to efficiently manage and process queries on that image collection. Datasets are compiled datasets for machine learning projects. Image datasets contain digital images compiled to test, train, and evaluate the performance of machine learning and artificial intelligence (AI) algorithms, typically computer vision algorithms.
- **Spoofed/real -** This is the result of the face spoofing algorithm, which is trained to differentiate if the input image is spoofedor real.

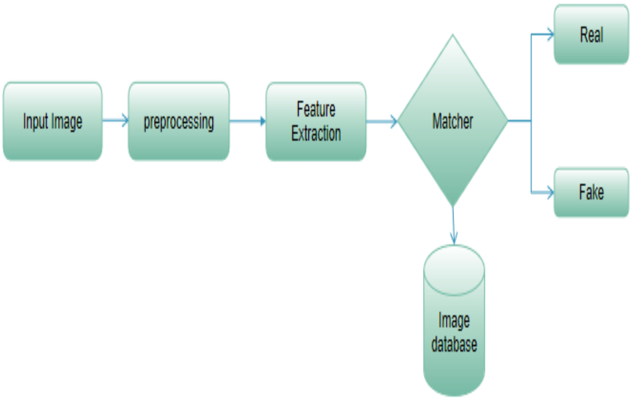

Fig. 3: Working model ofFace spoofing detection

V. RESULT

For the test set, the suggested face anti-spoofing system is light weight and compact for low computational devices like mobile devices that is very efficient and achieves a high accuracy of over 97.37%. Low rates of false negatives and false positives allowed the system to better discern between actual faces and artificial faces. The system has also proven to be resistant to other face spoofing face assaults, including those using video playbackandprinted pictures.

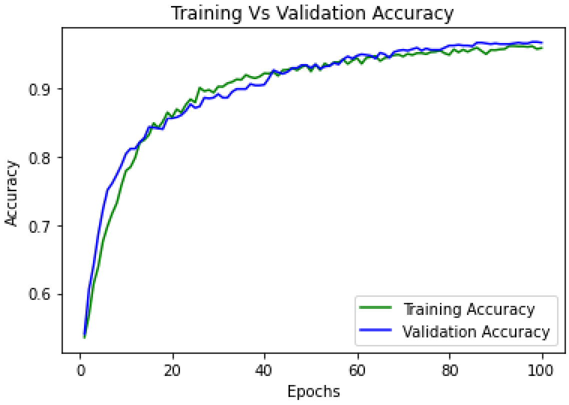

Fig. 4: Training accuracy and validation accuracy of system

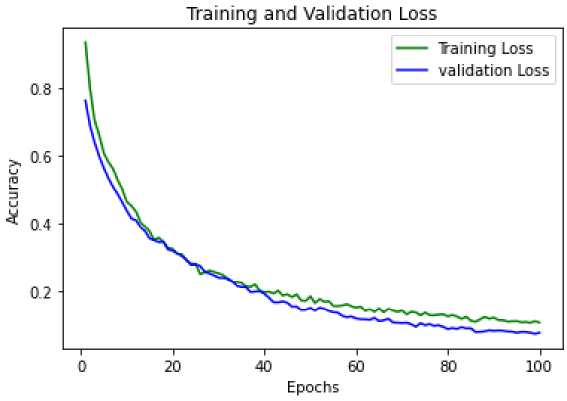

Fig. 5: Training loss and validation loss of system

The above figures show the validation and training accuracy along with the validation and training loss of the introduced system.

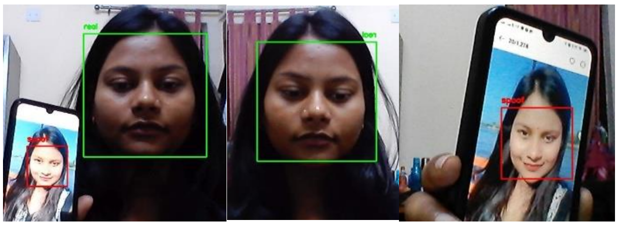

Fig. 6: Spoofing detection with our introduce system

The introduced system that we present perform good in different spoofing attacks. System needs very low computational cost in order to differentiate between spoofed and real faces.

The present system having different types of hardware component in order to differentiate between spoofed and real face this hardware include advanced camera like lidar camera or 3d camera which make system more costly and heavy which can not be implement by everyone. so, in order to make a system which can overcome the different type of spoofing attack and use less computational cost and hardware requirement we present a system that use low computation and need no hardware to prevent spoofing attacks.

VI. FUTURE WORK

Overall, anti-face spoofing systems have the potential to be valuable tools for improving the security and reliability of facial authentication systems. Ongoing research and development help improve the system's accuracy, robustness, and privacy, making it anefficient solution for real-world applications.

VII. CONCLUSION

This paper that we propose is an implementation of a deep learning-based face anti-spoofing system that can distinguish between spoofed and real faces. The system is highlyaccurate and compact which require less computational power to perform that make this an efficient system for the mobile or low computational power devices. This proposed system can be used as a reliable and efficient method for face anti-spoofing in various applications such as security, surveillance and biometric authentication.

REFERENCES

[1.] Benlamoudi, A.; Bekhouche, S.E.; Korichi, M.; Bensid, K.; Ouahabi, A.; Hadid, A.; Taleb-Ahmed, A. Face Spoof Attack Detection using Deep Background Subtraction. Preprints 2022, 2022040033 (doi: 10.20944/preprints202204. 0033.v1).

[2.] A Mittal, P Kaur, Dr. Ashish Oberoi in 2022. Hybrid Algorithm for Face Spoof Detection. International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 10 Issue II Feb 2022.

[3.] Haocheng Feng1, Zhibin Hong1, Haixiao Yue1, Yang Chen2, Keyao Wang1,Junyu Han1, Jingtuo Liu1, and Errui Ding1 . Learning Generalized Spoof Cues (https://doi.org/10.48550/arXiv.2005.03922)for Face Anti-spoofing. 2020.arXiv:2005.03922v1 [cs.CV] 8 May 2020.

[4.] M Yadav, KGupta: Novel Technique for Face Spoof Detection in Image Processing. Proceedings of the Second International Conference onIntelligent Computing and Control Systems. IEEE, 2018.

[5.] Songlin Yang1,2 Wei Wang2 Chenye Xu3 Bo Peng2 , and Jing Dong2 ,Exposing Fine-grained Adversarial Vulnerability of Face Anti-spoofing Models , arXiv:2205.14851 , doi.org/10.48550/arXiv.2205.14851.

[6.] ZitongYu,Yunxiao Qin, XiaobaiLi,Chenxu Zhao, Zhen Lei, and Guoying Zhao in 2022 deep learning based FAS , DOI: 10.1109/TPAMI.2022.3215850.

[7.] Young E Kim and SW Lee 2021,Domain Generalization with Pseudo- Domain Label for Face Anti-Spoofing , doi.org/10.48550/arXiv.2107.06552.

[8.] Md R Hasan, S M Hasan Mahmud and Xiang Yu Li 2019:They introduces a novel and appealing face spoof detection technique , DOI:10.1088/1742-6596/1229/1/012044

[9.] 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, 2019.2

[10.] Noor Al-H T a , TM Hassan b , M A Younis they developed Face Spoofing Detection Using Deep CNN Vol.12 No.13 (2021), 4363-4373

[11.] S K Hashemifard, M Akbari 2021 A Compact Deep Learning Model for Face Spoofing Detection.Wide and Deep Features for Face Presentation Attack Detection. In Proceedings of ACM Woodstock conference (SIGIR 2019).

[12.] Y Moon , 1, IRyoo , 1 and S Kim 2021.Face Anti-spoofing Method Using Color Texture Segmentation on FPGA Received 4 March 2021; Revised 5 April 2021; Accepted 29 April 2021; Published 10 May 2021

[13.] X Yang; W Luo; L Bao; Y Gao; D Gong; SZheng; Zhifeng Li 2019 . Face Anti-Spoofing: Model Matters, so Does Data .Conference: 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR).

[14.] Dr . K Gopalakrishnan 2T.Soundarya, 3S.Santhiya 2022:Face Anti-Spoofing using Deep Learning .Face Anti Spoofing"2022 IEEE/CVF Conference on Computer Vision

[15.] 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.

[16.] Fei Peng, Le Qin and Min Long, "POSTER: Non-intrusive Face Spoofing Detection Based on Guided Filtering and Image Quality Analysis", 12th International Conference, SecureComm 2016, Security and Privacy in Communication Networks, Guangzhou, China, June (2017), pp. 774-777.

[17.] Mina Farmanbar and OnsenToygar, “Spoof detection on face and palmprint biometrics”, Signal, Image and Video Processing, vol. 11, (2017), pp. 1253–1260.

[18.] KLarbi, WOuarda, HDrira, B B Amor, and C B Amar, “DeepColorFASD: Face Anti Spoofing Solution Using a Multi Channeled Color Spaces CNN”, IEEE International Conference on Systems, Man, and Cybernetics (SMC), Miyazaki, Japan, (2018) October, pp. 4011-4016.

[19.] H. Chen, Y. Chen, X. Tian and R. Jiang, "A Cascade Face Spoofing Detector Based on Face Anti-Spoofing R-CNN and Improved Retinex LBP," in IEEE Access, vol. 7, pp. 170116-170133, 2019, doi: 10.1109/ACCESS.2019. 2955383.

[20.] Wang, Z., Yu, Z., Zhao, C., Zhu, X., Qin, Y., Zhou, Q., ... & Lei, Z. (2020). Deep spatial gradient and temporal depth learning for face anti-spoofing. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5042-5051).

[21.] R. B. Hadiprakoso, H. Setiawan and Girinoto, "Face Anti-Spoofing Using CNN Classifier & Face liveness Detection," *2020* 3rd International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, 2020, pp. 143-147, doi: 10.1109/ICOIACT50329.2020.9331977.

[22.] Anjos, André &Komulainen, Jukka & Marcel, Sébastien & Hadid, Abdenour&Pietikäinen, Matti. (2014). Face Anti-spoofing: Visual Approach. 10.1007/978-1-4471-6524-8_4.

[23.] Y. Atoum, Y. Liu, A. Jourabloo and X. Liu, "Face anti-spoofing using patch and depth-based CNNs," 2017 IEEE International Joint Conference on Biometrics (IJCB), Denver, CO, USA, 2017, pp. 319-328, doi: 10.1109/BTAS.2017.8272713.

[24.] Liu, Yaojie&Jourabloo, Amin & Liu, Xiaoming. (2018). Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision. 389-398. 10.1109/CVPR.2018.00048.

[25.] Pereira, Tiago &Komulainen, Jukka & Anjos, André & De Martino, José & Hadid, Abdenour&Pietikäinen, Matti & Marcel, Sébastien. (2014). Face liveness detection using dynamic texture. EURASIP Journal on Image and Video Processing. 2014. 2. 10.1186/1687-5281-2014-2.

[26.] Y. Kim et al., "CloudNet: A LiDAR-Based Face Anti-Spoofing Model That Is Robust Against Light Variation," in IEEE Access, vol. 11, pp. 16984-16993, 2023, doi: 10.1109/ACCESS.2023.3242654.