International Journal Of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704126 |

# Cloudnet A Lidar-Based Face Anti-Spoofing Model Thatrobust against Light Variation

**Dr.T. ARAVIND, RANJITH M, SENTHIL VADIVEL R, POOVARASAN R**

Assistant Professor, Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

**ABSTRACT:** The face recognition system is vulnerable to spoofing attacks by photos or videos of a valid user face. However, edge degradation and texture blurring occur when non-living face images are used to attack the face recognition system. With this in mind, a novel face anti-spoofing method combines the residual network and the channel attention mechanism. In our method, the residual network extracts the texture differences of features between face images. In contrast, the attention mechanism focuses on the differences of shadow and edge features located on nasal and cheek areas between living and non-living face images. The extracted deep color-based features of the face image are used for face spoofing detection in a cloud environment. The proposed method achieves stable results with less training data compared to conventional deep learning methods. This advantage of the proposed approach reduces the time of processing in the training phase and optimizes resource management in storing training data on the cloud. The proposed system was tested and evaluated based on two challenging public access face spoofing databases, namely, Replay-Attack and ROSE-Youtu.

**KEYWORDS**: face anti-spoofing; secondary imaging; residual network; attention mechanism

## I.INTRODUCTION

Nowadays, the Internet of Things (IoT) affects human lives in a wide range of technology from smart homes to smart cities. An enormous number of IoT devices are utilized for collecting and analyzing information for different reasons, such as healthcare, security, and management. According to the estimation of scientifics, around 90% of storing data would be useless [1]. Therefore, the researchers proposed [1] utilizing the edge devices in the architecture of applications or services for cloud computing. In this way, the data can be analyzed and filtered in edge devices and send more enhanced data for processing in the cloud. For example, the deployed sensors for traffic monitoring can be also utilized for fire detection with low-cost and low-performance devices. However, IoT-based systems are faced with different problems such as security threats from the Internet. For instance, let us consider an IoT-based healthcare application which contains critical information such as blood sugar level and blood pressure. The authentication system for data communication through wireless channels should be secured for protecting critical information of clients. Biometric authentication can be utilized for identifying a person in wireless communication. This authentication requires using personal attributes, such as speech, face, fingerprints, palmprint, gait, and iris [2]. This kind of authentication is based on a comparison between the physical aspect of the client that is collected with the help of different sensors and a copy that was stored. The physiological information of clients is more reliable when compared to knowledge-based or token-based methods because this information is unique and not shareable. For this reason, IoT-based cloud computing systems for authentication of clients applied their biometric information.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704126 |

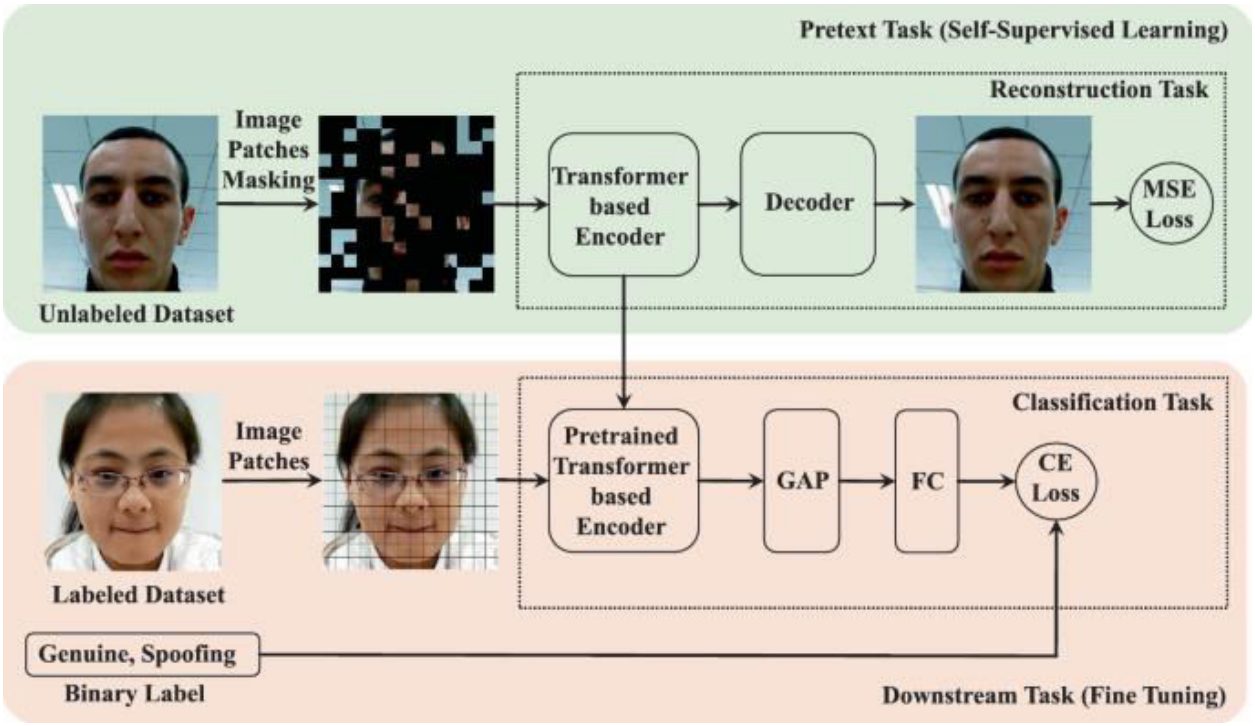


Fig 1: Exploring Masked Image Modeling for Face

For instance, Kumari and Thangaraj [3] proposed a feature selection technique in biometric authentication using a cloud framework. In another similar study, Shakil et al. [4] proposed a biometric authentication system and data management application for security of healthcare data in the cloud. Also, Vidya and Chandra [5] proposed a multimodal biometric authentication system based on entropy-based local binary pattern feature description technique for cloud computing. Additionally, Masud et al. [6] proposed a deep learning-based approach for face recognition in IoT environments. Face recognition systems have achieved significant interest in many applications such as cell phones' and laptops' authentication or registration systems at places such as online exam centers and airports [1]. These kinds of security systems in the Big Data analytics platform are a topic of concern for real-time applications. Consider the scenario when a person is to be recognized in an airport for registration or a student is attending an online exam. In these scenarios and other similar conditions, the camera captures images of the face continuously and sends these data for processing in the cloud environment. Based on meaningful information of face image, a certain person can easily be identified. Nevertheless, these kinds of authentication and registration systems are vulnerable to different types of attacks. For improving the security of biometric authentication systems, various methods and models are proposed.

For example, Ali et al. [1] proposed a multimodal biometric authentication system using an encryption method for protecting the privacy of biometric information in the IoT-based cloud environment. In another study, Gomez-Barrero et al. [2] proposed a framework for the protection of the privacy of multibiometric templates with an encryption method. However, the aforementioned methods are designed for protection based on man-in-the-middle attacks in wireless communication. According to the literature, face spoofing attacks in IoT cloud environments are not discussed and studied yet. The main objective of this study is to present an IoT cloud-based framework for protecting client's information from face spoofing attacks. In a face spoofing attack, the intruder bypasses the authentication system by presenting a fake face of the victim. Due to this threat, robust and stable face Presentation Attack Detection (PAD) methods must be developed and designed. Face spoofing attacks may be classified into four main groups: print, display, replay, and mask attacks [7].

## II.RELATED WORK

Face liveness detection algorithms based on texture analysis usually recognize the effects of illumination limitations of a printer or any other device during display, such as printing failures, blurring, and other effects. The RGB color space, as

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704126 |

discussed in Section 1, cannot clearly present features regarding illumination and chrominance. In this case, a previous study [12] proposed a deep learning system based on the RGB, HSV, and YCbCr color spaces. In the paper, the CompactNet model was proposed as a layer-by-layer progressively generated color space. Additionally, features of spoofing databases are extracted by a pretrained feature extractor model. Researchers [11] proposed a color feature descriptor method based on different color spaces. In this method, information on the luminance and chrominance channels was extracted by a low-level feature descriptor. Due to the impact of a smaller number of databases in face spoofing detection on training deep learning methods and overfitting problems, researchers investigate the extraction of discriminative and deep features. For instance, a study [15] proposed a perturbation layer (low-level deep features) to extract the deep features of a convolutional neural network (CNN) for classification. Another study presented an adaptive fusion of convolutional feature models to learn the features of face images, and a deep autoencoder was utilized for generating a face image to detect spoofing face images. Some authors [7] .

proposed a Spatial Pyramid Coding Microtexture (SPMT) feature extractor with a deep learning system for detection of liveness cues and employed the Single Shot Multibox Detector (SSD) as an end-to-end face spoofing detection model. Besides the aforementioned color-based deep learning methods, some methods presented local binary pattern- (LBP-) based feature descriptors for spoofing detection. For instance, a hybrid method was proposed based on the Chromatic Cooccurrence of Local Binary Pattern (CCoLBP) and Ensemble Learning (EL) algorithms. In the case of reducing the parameters of CNN models and extraction of deep features, an end-to-end learnable LBP network was proposed. A previous study proposed an algorithm by integrating the LBP descriptor with a modified convolution neural network that extracted deep texture. For extraction of discriminative features of presentation attacks, the Extended Local Ternary Corelation Pattern (ELTCP) feature extraction method was proposed. This feature descriptor with extraction of spatial information of an image in multiple directions achieved robust results on presentation attacks. In recent years, with increasing attention to 3D face spoofing attacks, several studies have been devoted to recognizing 3D mask attacks. For instance, the 3D wax face attacks approach is proposed with a convolutional neural network based on the Residual Attention Network (RAN) for 3D face spoofing detection. In another similar study, a multichannel CNN [22] approach with a one-class Gaussian mixture model is proposed for the detection of 2D and 3D attacks. Another study [23] presented a shading-based 3D feature description method to extract discriminative and robust 3D features from the face image. In another study, researchers proposed a face spoofing framework with the help of convolutional autoencoders for the detection of 3D mask attacks. Another study investigated various factors of affection of acquisition conditions and devices with different resolutions on the generalization of color texture features for spoofing detection. In this light, another possibility seems to be analyzing image textures based on deep features from multiple color spaces, which is proposed in this paper. The experimental results show that our proposed algorithm is superior in color texture extraction and classification over state-of-the-art methods.

## III.METHODS

Among texture recognition techniques, motion-based analysis also plays an important role in spoofing detection. For instance, a study [25] proposed a motion-based analysis approach based on rigid and nonrigid facial movements. The proposed system extracted motion cues such as face movement, lip movement, and hand shaking and classified them into natural and fake motions. In another study [8], an undirected conditional random field in video processing was proposed for the detection of eye blinking. Other researchers [26] proposed a dynamic mode decomposition pipeline with SVM and LBP. This algorithm extracted facial dynamic information in videos as an image sequence.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704126 |

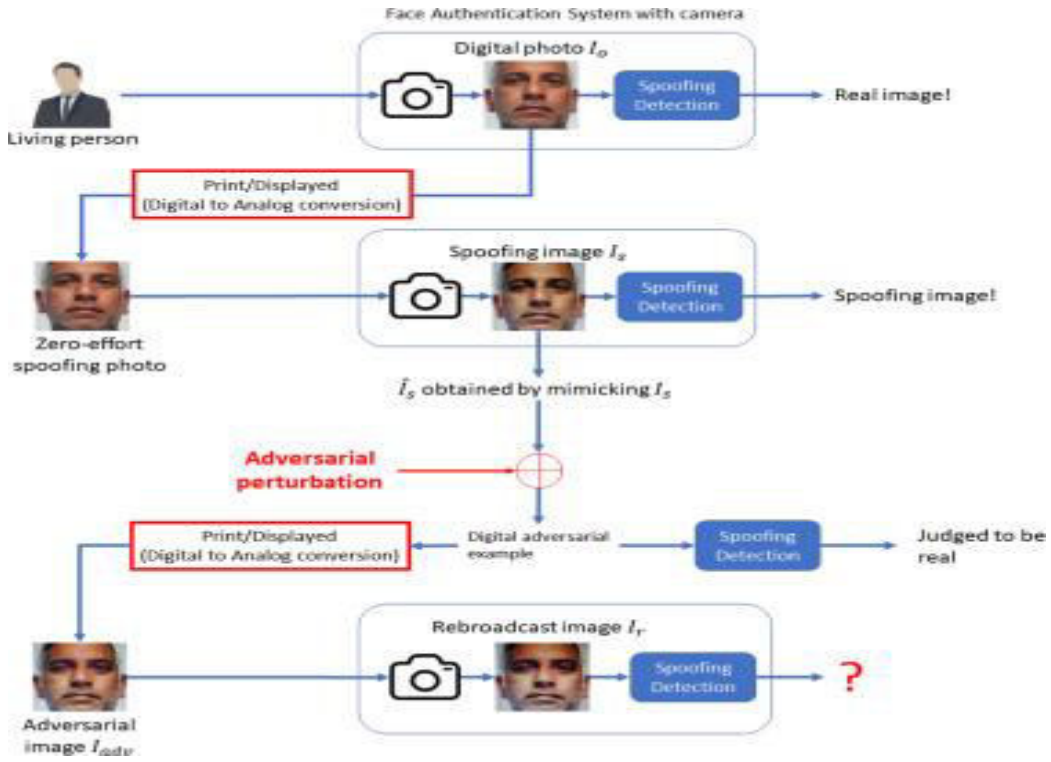


Fig 2: work Flow

Before feeding the face image to the deep model for classification in cloud computing environments, RGB color space is transformed to the HSV and YCbCr color spaces. Three parallel pretrained models are utilized in the proposed deep learning approach. Based on the literature, because of the small number of data and lack of scenarios in controlled environments, it is quite hard to train CNN models from scratch and achieve a stable and high-performance model. In this case, we utilized the VGG-face [33] model in the RGB color space for face spoofing detection [14, 18]. In addition, the transformed images of the HSV and YCbCr color spaces are trained by the VGG16 [34] model individually on the cloud side. After fine-tuning models by a different color space, the features of the last fully connected layer which consists of 4096 features for each deep model are extracted. These features are combined and then selected by employing the Minimum Redundancy Maximum Relevance (mRMR) feature selection algorithm.

## IV.RESULT ANALYSIS

The Replay-Attack database consists of 1300 videos of 2D face attacks under different conditions. This database contains three main subgroups for training, validation, and testing folders with names of training data, development data, and test data. Two main different lighting conditions in this database were named as controlled and adverse.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704126 |

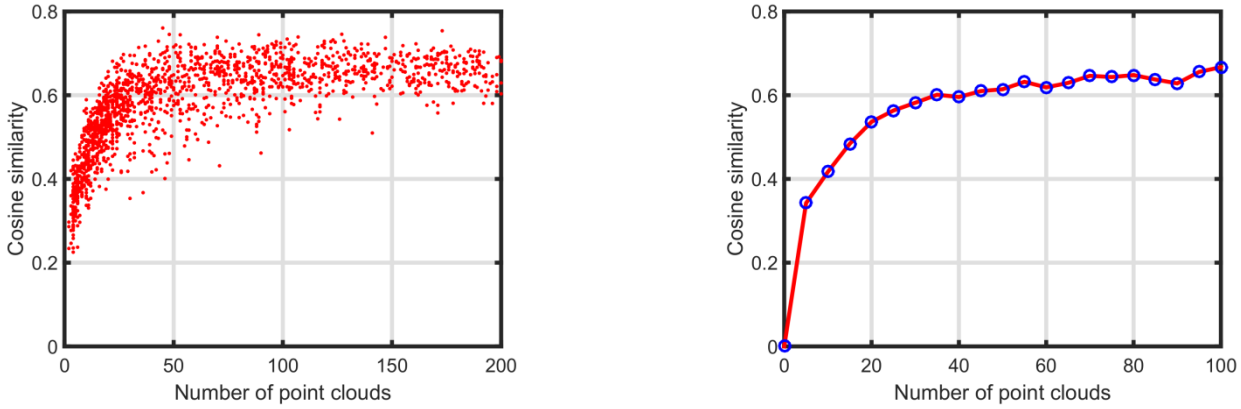


Fig 3: Spoofing Analysis

Learning the different features between live and non-living face images by deep neural network is important for recognition and classification. Scholars generally develop more different feature matrices to improve the accuracy of network recognition by deepening the number of network layers. When the number of layers increases, the network performance does not necessarily improve; rather, the network performance decreases as the number of layers increases. In response to this problem, proposed a deep residual network and applied it to the image recognition task. In the conventional convolution operation, the spatial information and channel information of width and height are fused for superposition calculation. By extracting features globally and ignoring the different relationships between the channels, the features that are useless for the task will also be extracted and become redundant information classification criteria.

## V.CONCLUSIONS

Focusing on the differential features of facial shadows and details between living and non-living face images, this paper used the channel attention mechanism to transform the feature convolution module of the deep residual network, strengthening the network model's ability to extract and represent key differential features in the nose color mutation region and cheek texture region of the face. We embedded a channel attention mechanism module in the residual block in each convolution block with a total number of four. Thus, we proposed a face anti-spoofing method SE-ResNet50. Compared with the original ResNet50 network, SE-ResNet50 has 3.05% and 2.20% higher detection accuracy on Replay-Attack and CASIA-FASD datasets, respectively. Compared with other existing methods, it has a more stable and excellent detection effect on non-living face photo and video attacks. Finally, we can try to fuse other features to enhance our method, such as the face heart feature, to increase the ability to defend against more realistic 3D masked faces.

## REFERENCES

1. Costa-Pazo, A.; Bhattacharjee, S.; Vazquez-Fernandez, E.; Marcel, S. The replay-mobile face presentation-attack database. In Proceedings of the 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 21–23 September 2016; pp. 1–7. [Google Scholar]
2. Chingovska, I.; Anjos, A.; Marcel, S. On the Effectiveness of Local Binary Patterns in Face Anti-spoofing. In Proceedings of the 2012 BIOSIG Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 6–7 September 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 1–7. [Google Scholar]
3. Cai, R.; Chen, C. Learning deep forest with multi-scale local binary pattern features for face anti-spoofing. *arXiv* **2019**, arXiv:1910.03850. [Google Scholar]
4. Freitas Pereira, T.; Anjos, A.; Martino, J.M.D.; Marcel, S. LBP-TOP based countermeasure against face spoofing attacks. In Proceedings of the Asian Conference on Computer Vision, Daejeon, Korea, 5–9 November 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 121–132. [Google Scholar]
5. Kong, Y.; Liu, X.; Xie, X.; Li, F. Face Liveness Detection Method Based on Histogram of Oriented Gradient. *Laser Optoelectron. Prog.* **2018**, *55*, 237–243. [Google Scholar]

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704126 |

6. Boulkenafet, Z.; Komulainen, J.; Hadid, A. Face Spoofing Detection Using Colour Texture Analysis. *IEEE Trans. Inf. Forensics Secur.* **2017**, *11*, 1818–1830. [Google Scholar] [CrossRef]
7. Yang, J.; Lei, Z.; Li, S.Z. Learn Convolutional Neural Network for Face Anti-Spoofing. *Comput. Sci.* **2014**, *9218*, 373–384. [Google Scholar]
8. Lucena, O.; Junior, A.; Moia, V.; Souza, R.; Valle, E.; Lotufo, R. Transfer learning using convolutional neural networks for face anti-spoofing. In Proceedings of the International Conference Image Analysis and Recognition, Montreal, QU, Canada, 5–7 July 2017; Springer: Cham, Switzerland, 2017; pp. 27–34. [Google Scholar]
9. Deng, X.; Wang, H.C. Face liveness detection algorithm based on deep learning and feature fusion. *J. Comput. Appl.* **2020**, *40*, 1009–1015. [Google Scholar]
10. Luan, X.; Li, X.S. Face anti-spoofing algorithm based on multi-feature fusion. *Comput. Sci.* **2021**, *48*, 409–415. [Google Scholar]
11. Yu, Z.; Qin, Y.; Li, X.; Wang, Z.; Zhao, C.; Lei, Z.; Zhao, G. Multi-modal face anti-spoofing based on central difference networks. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, Seattle, WA, USA, 13–19 June 2020; pp. 650–651. [Google Scholar]
12. Cai, P.; Quan, H. Face anti-spoofing algorithm combined with CNN and brightness equalization. *J. Cent. South Univ.* **2021**, *28*, 194–204. [Google Scholar] [CrossRef]
13. Hu, J.; Shen, L.; Sun, G. Squeeze-and-excitation networks. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–23 June 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 7132–7141. [Google Scholar]
14. He, J.; Jiang, D. Fully automatic model based on SE-resnet for bone age assessment. *IEEE Access* **2021**, *9*, 62460–62466. [Google Scholar] [CrossRef]
15. Yoo, J.; Jin, Y.; Ko, B.; Kim, M.S. k-Labelsets Method for Multi-Label ECG Signal Classification Based on SE-ResNet. *Appl. Sci.* **2021**, *11*, 7758. [Google Scholar] [CrossRef]