STM JOURNALS

Recent Trends in
Electronics & Communication Systems

ISSN: 2393-8757
Volume 11, Issue 3, 2024
September–December
DOI (Journal): 10.37591/RTECS

https://journals.stmjournals.com/rtecs

Review RTECS

Comparative Study of Facial Spoofing Detection Using CNN Architecture

Karan Talwalkar[1,*], Aditya Ashok[1], Kshitij Navale[1], Aditya Kasar[2]

Abstract

Facial recognition systems face a high risk of security breach due to various facial spoofing attacks. This challenge was addressed by the study of several deep learning models. This study proposes an idea to detect facial spoofing using deep learning architecture to differentiate live faces form various types of spoofed images/videos using different CNN models. In addition, the study seeks to strengthen security measured in facial recognition system demonstrating that by using deep learning models we can effectively tackle spoofing attack and suggest an efficient and practical framework that can be used in real life scenarios. Systems that use facial recognition have become commonplace for authentication and security reasons. However, they create serious security concerns due to their vulnerability to facial spoofing attacks, which involve tricking the system by presenting images, videos, or 3D masks. Convolutional Neural Networks (CNNs) have become effective tools for identifying such spoofing attempts to counter these attacks. To identify facial spoofing, this study compares and assesses the effectiveness of many CNN architectures in terms of accuracy, computing efficiency, and resilience to different spoofing tactics. This study intends to illustrate the advantages and disadvantages of CNN architecture for improving facial recognition security through an analysis of cutting-edge models.

Keywords: CNN, PCA, AlexNet, GoogleNet, ResNet, liveness detection

INTRODUCTION

There is a rapid rise in the use of facial recognition techniques in recent times and threat of unauthorized users has also increased due to the boom in AI technology (Deep Face). The current technology remains vulnerable to facial spoofing, where the attacker uses various methods to copy the identity of legitimate user. These methods include presenting photographs, videos, or even masks to avoid the recognition system.

This research work determined the application of deep learning models for effective facial spoofing detection/classification among real and spoofed images. Deep learning, the subfield of Artificial Intelligence has developed various disciplines, including computer vision, due to its ability to learn complex patterns from large dataset. By leveraging this ability to learn complex details from complex dataset, we aim to develop a model that can accurately differentiate between live face and spoofing attempts, thereby enhancing the security of facial recognition system.

We search into the specific challenges associated with facial spoofing detection and explore how deep learning offers unique advantages in addressing these challenges. Additionally, this study outlines the proposed deep learning model architecture, training methodology, and evaluation strategy

***Author for Correspondence**
Karan Talwalkar
E-mail: karantalwalkar@gmail.com

[1]Student, Department of Computer Science, SVKM'S (Shri Vile Parle Kelavani Mandal's) Narsee Monjee Institute of Management Studies, Navi Mumbai, Maharashtra, India
[2]Assistant Professor, Department of Computer Science, SVKM'S (Shri Vile Parle Kelavani Mandal's) Narsee Monjee Institute of Management Studies, Navi Mumbai, Maharashtra, India

Received Date: August 07, 2024
Accepted Date: August 12, 2024
Published Date: September 08, 2024

Citation: Karan Talwalkar, Aditya Ashok, Kshitij Navale, Aditya Kasar. Comparative Study of Facial Spoofing Detection Using CNN Architecture. Recent Trends in Electronics & Communication Systems. 2024; 11(3): 9–17p.

employed to assess its effectiveness in identifying spoofing attempts. This research focuses to present the improvement of facial recognition system with the help of deep learning models:

- Demonstrating the capability of deep learning models in facial spoofing detection: We have suggested a strong and effective model for real world applications which can differentiate between the image and can accurately tell which image is spoofed and which is real. It can be effective if someone is trying to gain unauthorized access to confidential information and trying to fool the biometric system with the help of various spoofing techniques like presenting photographs, videos, or masks.
- Contributing in ongoing research to reduce security vulnerabilities related with biometric recognition systems, for e.g. facial recognition technology, we mainly focus on enhancing the facial recognition system which can predict more effectively and accurate spoofing activity and can accurately differentiate between real and spoofed faces.
- For creating these models more efficient in predicting we are going to distribute out dataset into three sets training, testing and validation; our dataset contains the real and spoofed image and is going to use three types of CNN architectures for the prediction. Our generated model will accurately classify between real and spoofed image, and we will also be going to try in our future research to implicate in real time biometric machines to enhance the security of the biometric system.

LITERATURE REVIEW

Facial spoofing detection has grown to be an important field of research because facial recognition systems are now being used in security-sensitive applications. Traditional methods depend on handcrafted features like texture analysis and optical flow that vary with lighting conditions, pose or expression. It is known that deep learning models are efficient in overcoming the limitations of other techniques based on various studies conducted so far.

- Deep feature learning: Deep learning models can learn intricate facial attributes from large datasets and represent subtle nuances in live faces which cannot be easily defined.
- Robustness to variations: These models can learn representations that are robust to variations in lighting, pose, and expression, leading to accurate classification even under challenging conditions.

Our study is focused on facial spoofing detection using different types of deep architectures: Convolution Neural Networks (CNN): CNNs are popular types of networks designed for extracting hierarchical features from images/videos. In previous studies [1, 2], the authors used the pre-trained CNNs such as VGG16 and ResNet and its advantages are included as the other researchers have already done our work on facial spoofing detection, and it can be classified based on different deep learning architecture types:

- Convolution Neural Networks (CNN): These models are commonly employed for their capability to pull out the hierarchy of features from the images/videos provided in input data. In many studies they make use of pre-trained CNNs including VGG16 and ResNet which are fine-tuned for spoof detection.
- Generative Adversarial Networks (GAN): Researchers have also attempted using GAN, where they introduced a generator and a discriminator network that would compete against each other to improve the model's ability to distinguish between real and fake faces [3].
- Recurrent Neural Networks (RNNs): These models are useful in studying sequential data like video frames. Additionally, RNNs were used by Das and Chakraborty to capture temporal dynamics in facial features when trying to detect possible forgery or manipulation [4].
- Attention mechanisms: Attention mechanisms within CNN architectures integrated into studies like by Jasmine *et al*. allow these works to focalize on specific regions of face such as eyes or mouth which play an important role in detecting liveliness [5].
- Lightweight models: Another group is still exploring the development of lightweight models purposely meant for resource scarce devices hence making it possible to conduct real-time mobile platforms based spoofing detection [6].

METHODOLOGY

For this research we have created compression/detection model which can accurately detect between genuine and spoofed faces: (i) Face detection in an image; (ii) Face verification of real or spoof face in an image [7]. We have used complex dataset containing real and spoofed face images to train and testing purpose which can make the model complex and can accurately predict between genuine and spoofed image. The process and our finding for research process in this research work are as followed [8]:

Problem Definition and Scope Clarification

Facial recognition models are vulnerable to presentation attacks [9]. This research concentrates on making the facial spoofing detection model and to enhance its working using various CNN architecture for prediction purpose [10], which can effectively overcome the vulnerability related to facial biometric system and can provide good results regarding facial detection.

Dataset Acquisition and Preprocessing

For this research we have acquired a wide range of data diverse dataset containing the samples of real (genuine) and samples of spoofed facial images from various backgrounds and from different lighting effects [11]. The dataset also includes a variety of presentational attack scenarios images such as printed photos, digital images, and 3D masks. Implemented preprocessing techniques, including normalization, augmentation, and noise injection, to enhance dataset quality which will make dataset more complex will train model effectively due to variety of information present in dataset with all the required aspects for building complex models for complex problems [12].

Gathering of data

- *Real:* Here, we recorded videos of people having different skin tones and in different lighting environments.
- *Spoofed:* We recorded the same video of real one from different device of same person holding mobile showing original image/video which will be considered as fake [13].

We detected each captured frame of faces in dataset and labelled them as real or fake, thereby we have created two folders namely real and fake and stored them respectively in the individual folders thus creating our dataset [14].

Dataset Splitting

The dataset is divided into three sets: training, validation and testing set, ensuring a balanced representation of genuine and spoofed samples in each subset. As our dataset is pre-processed and labelled, data will be provided for the training purpose of the model [15].

Model Architecture Design

- Design a Convolution Neural Network (CNN) based anti-spoofing model that can detect presentation attack.
- Experiment with different convolutional layers, activation function, and model architecture.

You can also consider utilizing transfer learning by using pre-trained CNN models to improve the performance of the model.

We have implemented three architecture models of CNN which are: Alex net (architecture shown in Figure 1), Google net (architecture shown in Figure 2), and Resnet (architecture shown in Figure 3) in which we have compared the output accuracy of all the three models for decision making of the overall model that how accurately the model is predicting between genuine and spoofed image. This approach of using three models for prediction will enhance the accuracy of predictions of the model and it will accurately provide the output of the model [16].

Alex Net CNN Architecture, as shown in the Figure 1, consists of five Convolution layers, three Max pooling layers and three Fully connected layers and SoftMax layers. The data set is divided into three sets: 50% training, 25% testing, and 25% validation [17].

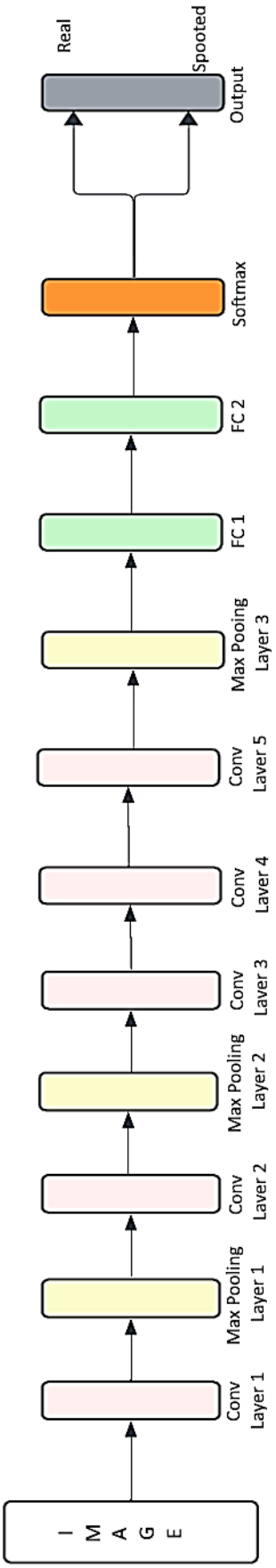

Figure 1. Alex net CNN architecture.

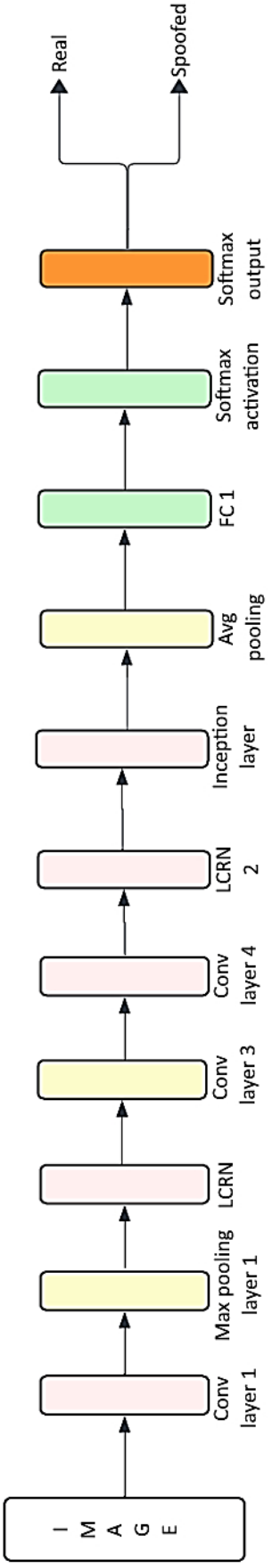

Figure 2. Google net convolution Layer.

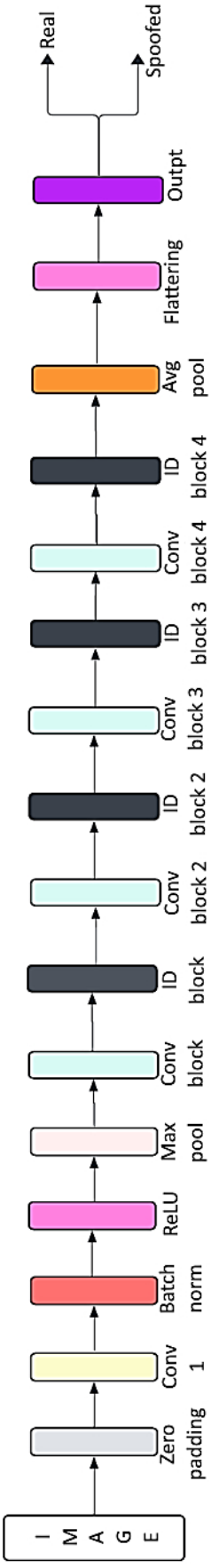

Figure 3. Validation algorithm.

Google net, as shown in Figure 2, consists of three convolution layers, 1 max pooling, 1 Average Pooling, 2 LCRN, 1 Inception 1 Fc, and 2 SoftMax. Validation algorithm is shown in Figure 3.

PROPOSED MODEL

i) Face Feature detection in an image, ii) Face verification of real or spoofed face in an image, as shown in Figure 4.

Training

Training phase contains dataset consisting of both real and spoofed images. The images will be provided as input for all the architectures, as shown in Figures 1–3 [18]. Multiple images will be providing as input to the architecture, as shown in Figure 5, for training purpose [19], we will access our web cam for liveness detection and check whether the model is accurately differentiating between real and spoofed image or not.

RESULT

In this section we are going to present the result which is generated by our research and created model on facial spoofing classification/detection model using deep learning and specifically CNN architecture. The dataset is split into three sets training, validation and testing. We have used vague dataset containing genuine and spoofed facial images. The dataset was pre-processed. We have trained three of the models with the same dataset and recorded the output accuracy of the models and examined which model is providing the highest accuracy among all the used models. From our training and examination, the model which gives highest accuracy is Alex net, which shows the highest accuracy and accurately differentiates between real and spoofed image. We will access our web cam for testing the accuracy of the model if it is working accurately or not. We have used Caffe face detector. The input image for verification is shown in Figures 6 (real) and 7 (spoofed).

To show the model performance and corresponding accuracy we have used serval performance parameters such as precision, recall, F1 score, and area under curve (AUC-ROC), which is essential to have these comprehensive sets of matric to know the performance and accuracy of the respective models as shown in Figure 8. Precision and recall output is shown in Figure 9. By doing this we can get detailed insights into the model's effectiveness in predicting between genuine and spoofed image.

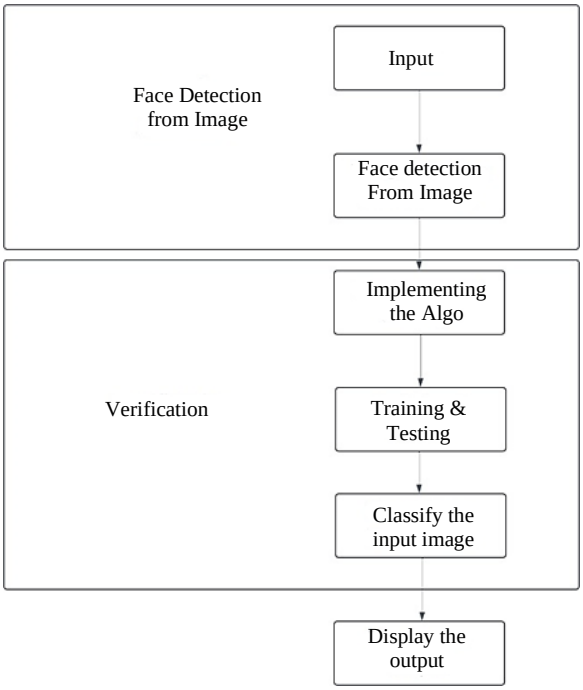

Figure 4. Face verification of Real and spoofed face.

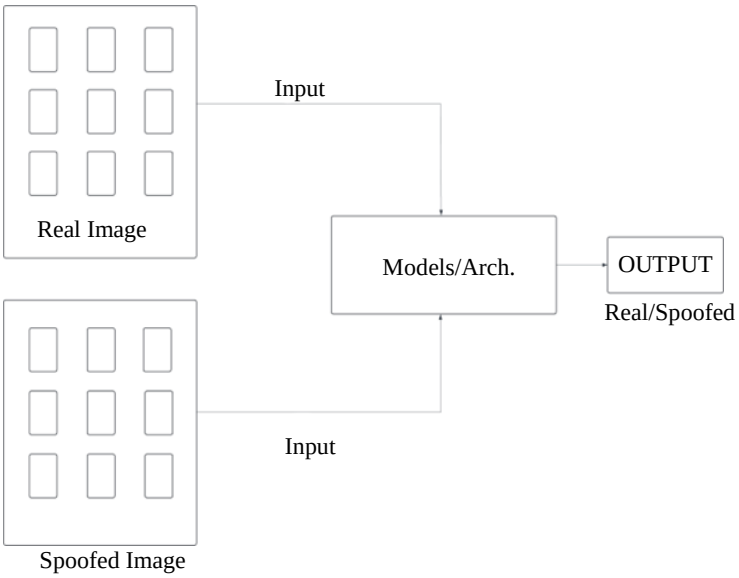

Figure 5. System architecture.

Figure 6. The (a) real and (b) spoofed image in one frame.

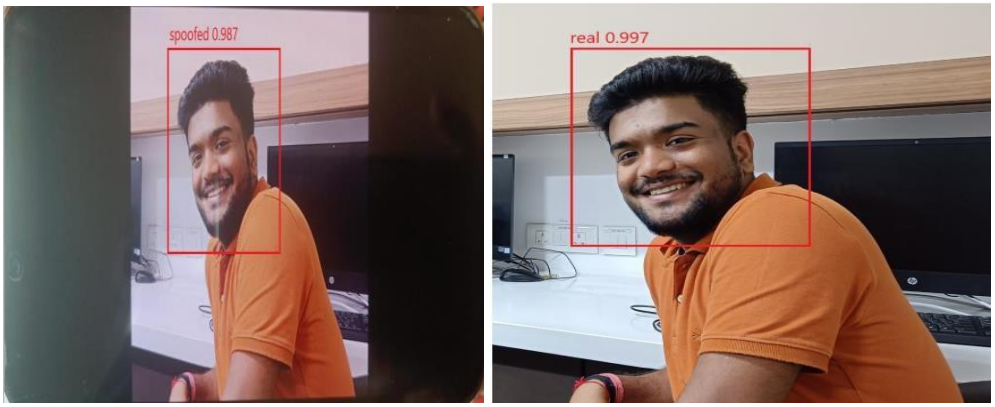

Figure 7. Output result of real and spoofed image.

The F1 score is a metric that combines both precision and recall into a single value. It provides a balanced assessment of a model's performance in binary.

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive+False Negative}} \quad (1)$$

$$\text{Precision} \frac{\text{True Positive}}{\text{rue Positive+False Positive}} \quad (2)$$

$$\text{F1 Score } \frac{2\times\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{3}$$

In the context of a facial spoofing detection model, recall classification tasks, such as facial spoofing detection are discussed. The formula for calculating the F1 score is as shown in Eq. (3). The F1 score ranges from 0 to 1, where a higher value indicates better model performance. The values are shown in Table 1.

Table 1 refers to the ability of the model to correctly identify genuine faces out of all the actual genuine faces present in the dataset. In binary classification terms, where we typically label genuine faces as the positive class and spoofed faces as the negative class, recall can be calculated as in Eq. (1). In facial spoofing detection, precision refers to the ability of the model to correctly identify spoofed faces out of all the instances that the model predicted as spoofed. In binary classification terms, where we typically labelled spoofed faces as the positive class and genuine faces as the negative class, precision can be calculated as shown in Eq. (2).

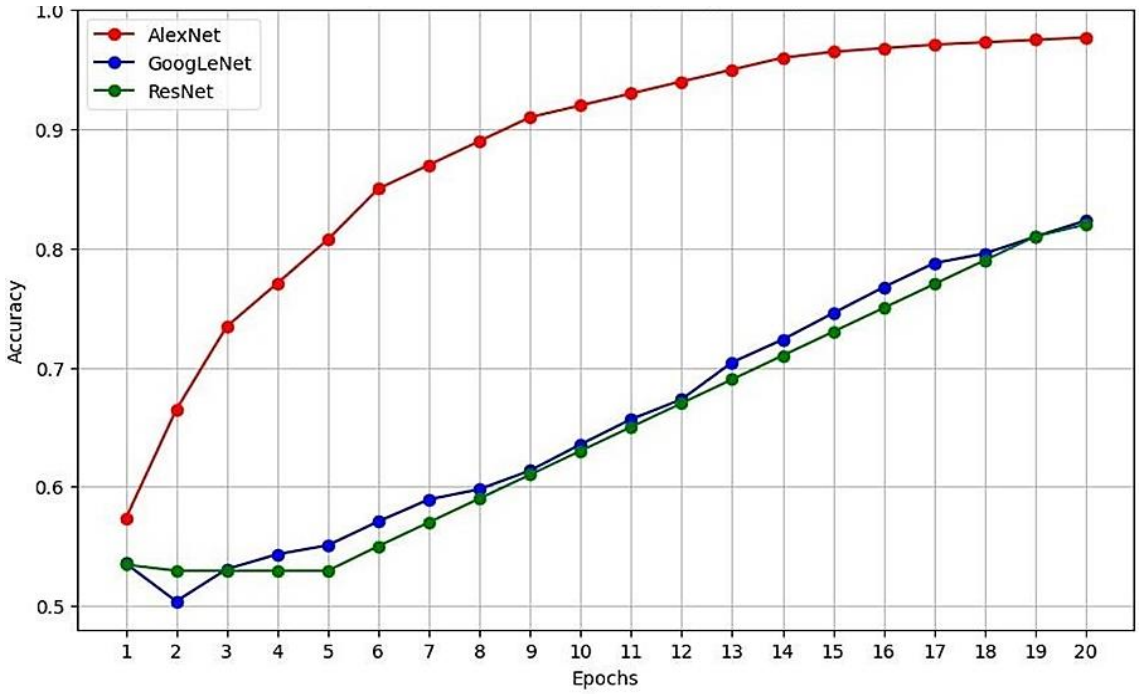

Figure 8. Accuracy Comparison of AlexNet, GoogLeNet, and ResNet.

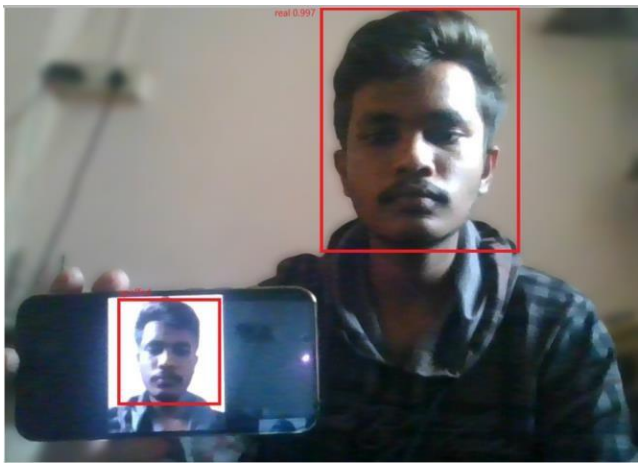

Figure 9. Result of the precision and recall.

Table 1. Genuine Faces versus actual faces of the dataset.

Architecture	F1	Recall	Precision
AlexNet	0.988	0.985	0.992
Resnet	0.898	0.892	0.904
GoogleNet	0.922	0.915	0.930

CONCLUSION

This research work tackled the critical challenges of facial spoofing in biometric authentication systems with the help of deep learning models like Convolution Neural Network (CNN). It presents the categorical based classification of image. Our facial spoofing detection model shows high precision and recall scores for both genuine and spoofed faces, indicating its efficiency in distinguishing between presentation attacks and effectively distributing between real and spoofed faces. The F1-score, showing a harmonized balance between precision and recall, underscored the model's ability to generalize across diverse facial representations. The support metric indicates a well-distributed evaluation across genuine and spoofed examples, contributing to a holistic understanding of the model's performance.

Implications

Our research findings add to the ongoing discussion on detecting facial spoofing. We highlight the significance of customized model architectures and creative preprocessing techniques. Acknowledging the impact of color space transformation opens opportunities for further exploration of multi-modal representations that can enhance spoofing resilience.

Limitations and Future Directions

By acknowledging the limitations of the study, such as dataset constrain sensitivity, in the ever-developing landscape of facial recognition technology, our research contributes a variety of insights, underlining the dynamic relationship between model architectures, preprocessing techniques, and their collective impact on facial spoofing detection.

Future Research

Future research directions may involve:

- Development of generalizable models: Models that can effectively detect a wider range of spoofing techniques, including deep fakes and 3D masks.
- Explainable AI techniques: Techniques to understand the decision-making process of deep learning models to mitigate bias and ensure fairness.
- Integration with other modalities: We can Combine facial features with other modalities like voice, gait, finger, and iris analysis for multi-modal spoofing detection.

REFERENCES

1. Kong Y, Li X, Hao G, Liu C. Face Anti-Spoofing Method Based on Residual Network with Channel Attention Mechanism. Electronics. 2022; 11(19): 3056. https://doi.org/10.3390/electronics11193056
2. Li Y, et al. Deep learning for face anti-spoofing: Artery segmentation and micro-texture analysis. 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018). 2018.
3. Muradkhanli Leyla G, Namazli Parviz A. Face spoof detection using convolutional neural network. Probl Inf Soc. 2023; 14(2): 40–46. http://doi.org/10.25045/jpis.v14.i2.05
4. Das D, Chakraborty S. Face liveness detection based on frequency and micro-texture analysis. 2014 International Conference on Advances in Engineering & Technology Research (ICAETR-2014), Unnao, India. 2014; 1–4. doi: 10.1109/ICAETR.2014.7012923.
5. Jasmine Pemeena Priyadarsini M, Ramya K, Shabareesh Parlakota, Naveen Kumar Reddy Tadi, Jabeena A, Rajini GK. Face Anti-Spoofing and Liveness Detection Using Deep Learning Architectures. Journal of Engineering Science and Technology (Special Issue on IEC2022). 2022 Nov; 217–227.

6. Lucena O, Junior A, Moia V, Souza R, Valle E, Lotufo R. Transfer Learning Using Convolutional Neural Networks for Face Anti-spoofing. In: Karray F, Campilho A, Cheriet F, editors. Image Analysis and Recognition. ICIAR 2017. Lecture Notes in Computer Science. Vol. 10317. Cham: Springer; 2017. https://doi.org/10.1007/978-3-319-59876-5_4
7. Erdogmus N, Marcel S. Spoofing in 2D face recognition with 3D masks and anti-spoofing with Kinect. 2013 IEEE 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS), Arlington, VA, USA. 2013; 1–6. doi: 10.1109/BTAS.2013.6712688.
8. Boulkenafet Z, et al. Face anti-spoofing based on color texture analysis. In Proceedings of the IEEE International Conference on Computer Vision Workshops (ICCVW). 2017; 464–472.
9. Kong Seong G, Jingu Heo, Abidi Besma R, Joonki Paik, Abidi Mongi A. Recent advances in visual and infrared face recognition—a review. Comput Vis Image Understand. 2005 Jan; 97(1): 103–135.
10. Zhang S, et al. A Dataset and Benchmark for Large-Scale Multi-Modal Face Anti-Spoofing. 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Long Beach, CA, USA. 2019; 919–928. doi: 10.1109/CVPR.2019.00101.
11. LeCun Y, Bengio Y, Hinton G. Deep learning. Nature. 2015; 521(7553): 436–444. https://doi.org/10.1038/nature14539
12. He K, Zhang X, Ren S, Sun J. Deep Residual Learning for Image Recognition. 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA. 2016; 770–778. doi: 10.1109/CVPR.2016.90.
13. Rui Huang, Xin Wang. Face anti-spoofing using feature distilling and global attention learning. Pattern Recognit. 2023 Mar; 135: 109147.
14. Meepaganithage A, Rath S, Nicolescu M, Nicolescu M, Sengupta S. Image Forgery Detection Using Convolutional Neural Networks. 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA. 2024; 1–6. doi: 10.1109/ISDFS60797.2024.10527268.
15. Yasar Abbas Ur Rehman, Lai-Man Po, Mengyang Liu, Zijie Zou, Weifeng Ou, Yuzhi Zhao. Face liveness detection using convolutional-features fusion of real and deep network generated face images. J Vis Commun Image Represent. 2019 Feb; 59: 574–582. https://doi.org/10.1016/j.jvcir.2019.02.014
16. George A, Mostaani Z, Geissenbuhler D, Nikisins O, Anjos A, Marcel S. Biometric face presentation attack detection with multi-channel convolutional neural network. IEEE Trans Inf Forensics Secur. 2019 May 14; 15: 42–55.
17. Jiawei Chen, Xiao Yang, Heng Yin, Mingzhi Ma, Bihui Chen, Jianteng Peng, Yandong Guo, Zhaoxia Yin, Hang Su. AdvFAS: A robust face anti-spoofing framework against adversarial examples. Comput Vis Image Underst. 2023 Oct; 235: 103779. https://doi.org/10.1016/j.cviu.2023.103779
18. Zitong Yu, Yunxiao Qin, Xiaobai Li, Chenxu Zhao, Zhen Lei, Guoying Zhao. Deep Learning for Face Anti-Spoofing: A Survey. IEEE Trans Pattern Anal Mach Intell. 2023 May; 45(5): 5609–5631. 10.1109/TPAMI.2022.3215850
19. Nogueira RF, de Alencar Lotufo R. Campos Machado R. Fingerprint Liveness Detection Using Convolutional Neural Networks. IEEE Trans Inf Forensics Secur. 2016 Jun; 11(6): 1206–1213. doi: 10.1109/TIFS.2016.2520880.

