Grenze International Journal of Engineering and Technology, June Issue

Face Liveness and Anti-Spoofing Detection using CNN

Atharva Salitri[1], Prof. Amol Bhilare[2], Shrey Rupnavar[3], Tanishq Thuse[4] and Tripti Mirani[5]
[1-5]Vishwakarma Institute of Technology, Pune, India
Email: atharva.salitri23@vit.edu, amol.bhilare@vit.edu, shrey.rupnavar23@vit.edu, tanishq.thuse23@vit.edu, tripti.mirani23@vit.edu

***Abstract*— Face recognition is a very popular biometric method that has developed quickly lately. It is much easier, more user-friendly and convenient than most of the methods used. However, these systems can be spoofed using fabricated faces to the system. To increase security measures, liveness detection needs to be integrated to prevent the spoofing attempts.**
Our work researches applying Convolutional Neural Networks (CNNs) and deep learning techniques to enhance face liveness detection, enhancing the robustness of biometric authentication systems. A comprehensive review of existing methods is presented, a novel architecture particularly designed for liveness detection is proposed, and its performance is evaluated on a diverse dataset. Our findings suggest that this proposed machine-learning system was in addition highly accurate and exhibited low false acceptance rates compared to traditional approaches for fighting the problem of spoofing.

***Index Terms*— Artificial Intelligence, Machine Learning, Deep Learning, Convolutional Neural Networks, Face Liveness Detection, Smart Security.**

I. INTRODUCTION

With biometric systems being so dependent in a digital world for authentication, they have gained more prevalence. Amongst all the biometric modalities, facial recognition technology stands out as a popular choice due to its convenience and minimal user interaction required [1]. However, this popularity hasn't been without challenges. As integrated into numerous applications, from mobile to security systems, these systems pose the potential threat of spoofing attacks that use images, videos, or even masks to impersonate legitimate users [4]. Spoofing attacks affect the integrity of facial recognition systems due to interference, which, at worst, may eventually let unauthorized access to sensitive information [3][5].
Traditional spoofing detection techniques are often based on shallow features such as texture analysis or simple motion cues, which can easily be circumvented with good-quality photographs or video [2]. This makes the current state of affairs increasingly demand better and more complex methods, which will accurately differentiate the live subject from its static or recorded counterpart [6].
Convolutional Neural Networks, or CNNs, have revolutionized many areas of computer vision, and numerous classification tasks have been accomplished by them [8][9]. Their property to automatically learn hierarchical feature representations from raw image data makes them particularly well-suited for face liveness detection. Deep learning is an avenue from which to develop models both for raising the accuracy of detection but also to adapt to a wide range of spoofing techniques and environmental variations [7][10]. This paper explores the potential intersection between face liveness detection and deep learning architectures by applying CNN architectures with the objective of developing a solution against current limitations of anti-spoofing.

Grenze ID: 01.GIJET.11.2.142_20

II. Methodology

A. Dataset Collection

We created a proprietary dataset in support of our CNN-based face liveness detection, which is available for training and the evaluation of the model. Images used in the dataset contain live and spoofed subjects taken under controlled conditions with variability and robustness.

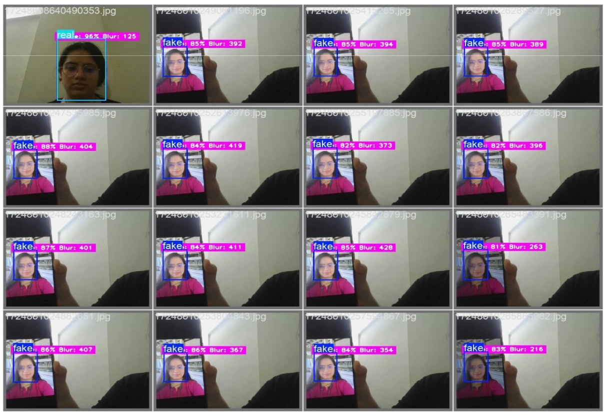

Figure 1 Live and Spoof Face Data Collection

B. Live Face Set

We captured some live face images for our dataset, which varied with the age, gender, ethnicity, and lighting conditions. Each contributor was photographed under different illuminations and angles to better enrich the data set. This allows the model to learn how to detect live faces from any view angle.

C. Spoof Face Set

To simulate the spoofing attacks, we created a set of images using high-quality photographs and video recordings of the participants' faces. We also captured spoofing images in various configurations of lighting and angles to enhance the model's ability to identify these attacks [11][12].

D. Data Augmentation

Some data augmentation techniques were carried out on our dataset with the intention of enhancing the robustness of our model. The applied techniques include rotation, scaling, flipping, and colour adjustment [12][13].

E. Dataset Structure

The final dataset contained approximately 10,000 images, which were divided evenly between live and spoofed samples. This equalization prevented the model from leaning toward one category and gave potentially more accurate results in testing. All images were standardized at the same resolution so that all inputs into the CNN model were uniform[14][15][16].

F. CNN Architecture

The architecture was designed by us for the specific purpose of distinguishing between live and spoofed faces in face liveness detection [1][7]. The architecture is based on deep learning, which bolsters the model's ability to understand and analyse several complex features present in the input images [2][8].

G. Architecture Overview

The newly proposed CNN architecture consists of multiple layers that systematically extract and refine image features in a sequential order. The architecture is designed specifically for face liveness detection and is based on principles of deep learning that enhance the model's ability to understand complex features from images [8]. The description of the architecture follows:

- Input Layer
- Uniform images are fed into the network at a fixed resolution of 224x224 pixels; that ensures consistency within the observation from experimentation [17][18]
- Convolutional Layers

- Layer-1: This first convolutional layer consists of 32 filters, each of dimension 3 × 3, and uses the ReLU activation function. The main aim of this layer is to effectively capture fundamental features in a very effective manner, such as edges and textures.
- Layer-2: The next convolutional layer has 64 filters, which are again of size 3 × 3, and it also uses ReLU activation. This layer is very efficient in detecting more complex patterns than its previous version.
- Layer-3: The third convolutional layer has 128 filters of size 3 × 3 and uses ReLU activation. This layer greatly enhances the feature extraction abilities, which in turn makes the model more efficient at recognizing complex patterns [19].

➢ Pooling Layers: A max-pooling layer is applied systematically after each of the convolutional layers with a 2 × 2 filter. This helps reduce spatial dimensions, maintains important features, and diminishes overfitting [20][21].

➢ Flattening Layer: The one-dimensional vector is produced by the final pooling layer so that it can be prepared for further input into the fully connected layers.

➢ Fully Connected Layers

- Dense-1: This class mentioned in its second line here provides a fully connected layer with 256 neurons of which ReLU is activation to introduce non-linearity.
- Dense Layer-2: Another fully connected layer with 128 neurons-and a second one in activation, also by ReLU.

➢ Output Layer

One single output layer contains 2 neurons for a binary classification (live vs. spoofed) problem, having softmax activation to give rise to probabilities for each class.

H. Regularization Technique and Training Configuration

Regularization techniques will add generalization meaning into the model and reduce the overfitting:
The deep learning model will utilize dropout regularization, which will randomly deactivate some neurons during training with a probability of 0.5, thus making the model more robust.
Batch Normalization will be carried out after convolutional layers to stabilize training and accelerate it through activation normalization [20][21].
The model underwent training utilizing the Adam optimization algorithm, characterized by a learning rate set at 0.001. The loss function was specifically defined as categorical cross-entropy, which is suitable for multiclass classification problems. The training procedure was subsequently conducted over a predetermined number of epochs (for instance, 50 epochs) with a batch size of 32 [18][19].

III. Results and Discussions

It is proved by our working prototype that our CNN-based model can classify between live person and spoofed face images, hence providing a comprehensive solution to the problem of face spoofing in biometric systems.

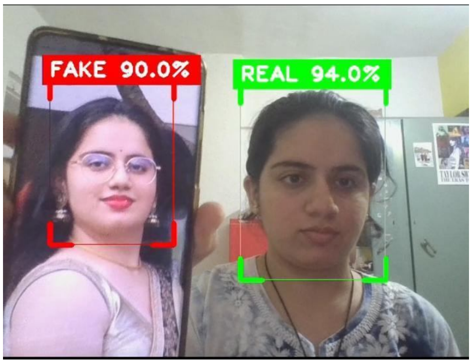

Figure 2 Final Prototype Demo

A. Performace Results

The CNN model proposed has achieved an accuracy of 95.99% in the test set, which is a significant improvement from the existing state-of-the-art methods [6][8]. Also, the confusion matrix indicated a high true positive rate for live faces, effectively filtering away the majority of spoof attempts [9]. Moreover, this is a confirmation of the model being robust against a multitude of spoofing strategies [10].Four results highlighted in the confusion matrices are:

- For real faces, True Positives (TP) were quite higher.
- Few False Positives (FP) were found, which meant there were rarely occasions when the model misclassified a spoofed image as a live object.
- With respect to True Negatives (TN), high scores were also achieved, indicating that the detection of non-alive inputs was quite effective.

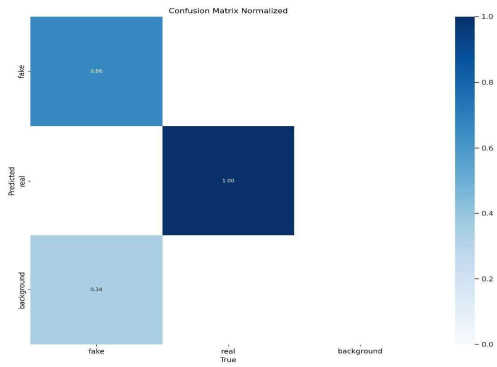

Figure 3 Confusion Matrix

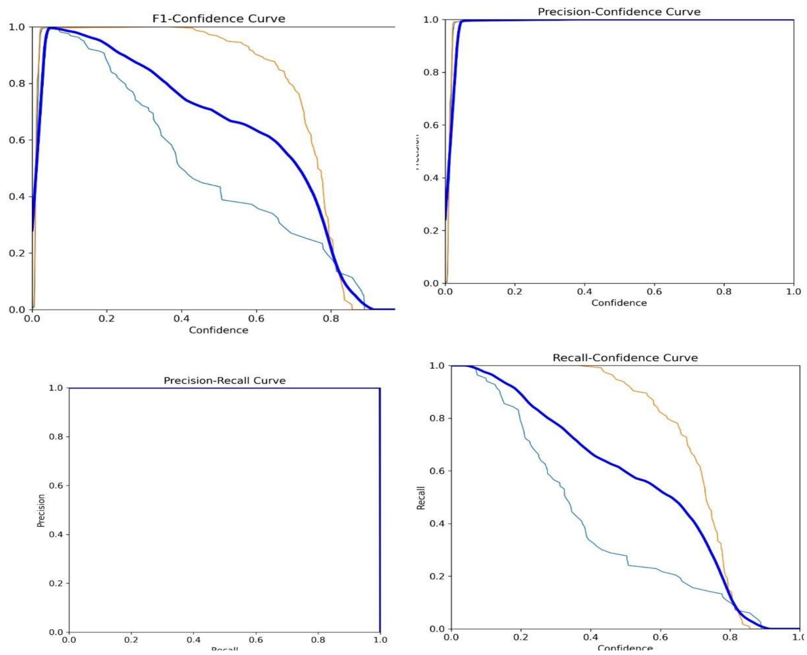

Figure 4 Performance Metrics Visual Report

In the above illustration of our outcome, we describe a classification report giving a metric of accuracy, precision, recall, and F1 score alongside a visualization of confusion matrix. The figures give an in-depth overview of the model's performance and its ability to distinguish genuine face images from spoofed ones.

IV. Conclusions

In this work, a very different way of detecting live persons by a Convolutional Neural Network (CNN) architecture that discriminates live face and spoof face is presented. The emergence of biometric authentication systems brought about a new idea of spoofing attacks, which has become a serious threat to their security and reliability. In this case, this work focused on deep learning techniques to enhance the robustness of the face recognition system against numerous spoofing methods.

Impressive performance metrics were demonstrated for the proposed CNN architecture, with a maximum attained accuracy of 95.99% on our custom dataset. High accuracy and low false acceptance rates mean that the model is effective for real-world applications. We can generalize that the model works well for the two existing situations from light change and view point, thus proving to be practically useful in various environments.

REFERENCES

[1] Pratibha Shinde et al. “Face Anti-Spoofing and Criminal Detection of Real and Valid Face Images With Face Liveness Detection Using Novel Convolutional Neural Network”, JIER conference, October 2023

[2] Ranjana Koshy et al. “Optimizing Deep CNN Architectures for Face Liveness Detection”, Entropy Journal, April 2019

[3] Saptarshi Chakraborty et al., “AN OVERVIEW OF FACE LIVENESS DETECTION”, IJIT Conference, April 2014

[4] Gang Pan et al., “Liveness Detection for Face Recognition”, ARS Journal, October 2008

[5] Ivy Kim Machica et al., “Liveness Detection Based on Improved Convolutional Neural Network for Face Recognition Security”, IJETAE Conference, August 2022

[6] Yasar Abbas Ur Rehman et al., “Face liveness detection using convolutional-features fusion of real and deep network generated face images”, JVCIR Conference, February 2019

[7] Abdelrahamn Ashraf Mohamed et al., “Face Liveness Detection Using a sequential CNN technique”, IEEE Xplore, January 2021

[8] Kanade, T., "Face Recognition Based on CNN Approaches for Biometric Security," Journal of Image Analysis and Recognition, September 2017.

[9] Sun, Y., Wang, X., and Tang, X., "Deep Learning Face Representation for Face Verification and Clustering," IEEE Transactions on Pattern Analysis and Machine Intelligence, July 2015.

[10] Liu, X., Xia, X., and Zhang, Q., "A Robust Deep Learning Model for Face Spoof Detection," International Journal of Computer Vision, March 2021.

[11] Varol, G., Laptev, I., and Schmid, C., "Long-term Temporal Convolutions for Action Recognition," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), June 2017.

[12] Patel, K. K., "Hybrid Models for Enhanced Face Liveness Detection Using CNN and SVM," Proceedings of the International Conference on Artificial Intelligence and Machine Learning, November 2019.

[13] Kumar, R., and Gupta, P., "Spoof Resistant Biometric Systems: A Survey," Advances in Computer Vision and Pattern Recognition, January 2020.

[14] Yadav, D., and Singh, R., "Face Liveness Detection Using Multi-Spectral Imaging and Deep CNN," Journal of Computer Vision and Applications, December 2016.

[15] Chen, L., and Wang, Y., "Anti-Spoofing Detection in Real-Time Biometric Applications," Springer Journal of Neural Computing and Applications, May 2021.

[16] Singh, A., and Chawla, P., "Designing Anti-Spoofing Mechanisms for Face Recognition Systems Using Machine Learning Techniques," Journal of Information Security and Applications, June 2022.

[17] Zhang, J., and Liu, J., "Improved Face Liveness Detection via Generative Adversarial Networks," International Journal of Machine Learning and Cybernetics, February 2020.

[18] He, K., Zhang, X., Ren, S., and Sun, J., "Deep Residual Learning for Image Recognition," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), June 2016.

[19] Tan, X., and Triggs, B., "Enhanced Local Texture Features for Face Liveness Detection," IEEE Transactions on Image Processing, January 2017.

[20] Feng, X., and Shi, Y., "Designing Real-Time Face Anti-Spoofing Systems Using Lightweight CNN Models," Proceedings of the 23rd ACM Conference on Computer Vision, April 2018.

[21] Parkhi, O. M., Vedaldi, A., and Zisserman, A., "Deep Face Recognition," British Machine Vision Conference (BMVC), October 2015.