International Journal of
Human Computations and Intelligence
Vol. 05, Issue. 04, 2026

RESEARCH ARTICLE OPEN ACCESS

ANTISPOOFAI: A Deep Learning Framework for Face Spoof Detection

A Jyothi . G Amulya . T Nehareddy . G Amulya . G Meghana . G Rushika

Department of Computer Science and Engineering,
G. Narayanamma Institute of Technology and Science, Hyderabad, India – 500090

DOI: **10.5281/zenodo.20003167**
Received: 14 April 2026 / Revised: 28 April 2026 / Accepted: 3 May 2026
*Corresponding Author: *jyothi@gnits.ac.in*

Abstract –Facial recognition technology has been applied to smartphones, mobile payment systems, intelligent access systems, and surveillance systems. But with its wide application comes the susceptibility to spoofing attacks based on printed pictures, replayed videos, or face masks. The common anti-spoofing measures based on previous studies rely on the addition of more hardware components such as infrared cameras and depth cameras. This makes the systems more expensive to implement.To overcome these issues, the proposed work introduces a software-oriented facial anti-spoofing technique using the Streamlit platform that can function properly using normal cameras. The proposed approach utilizes Convolutional Neural Networks to extract facial characteristics and a Siamese Network to discriminate between actual and spoofed facial images. The proposed technique is efficient, hardware agnostic, scalable, and can be used successfully as a real-time or uploaded video analysis tool.

Index Terms – Facial Recognition, Anti-Spoofing, Convolutional Neural Network (CNN), Siamese Network, Liveness Detection.

.

I. INTRODUCTION

Facial recognition technology had become an integral and common feature in one's day-to-day life. People were commonly making use of these services for the purpose of opening their smartphones, accessing financial services, ensuring public space security, and scanning identities for entries into airport terminals and border controls. Based on face features, the technology facilitated quick identification for various purposes. But despite the immense use of these facial recognition services, these services continued to have critical challenges. Issues of bias and spoofing were common challenges associated with facial recognition services.Bias and spoofing were significant issues

MILESTONE RESEARCH.IN OPEN ACCESS

ISSN (Online): 2583-5696
Int. Jr. of Hum Comp. & Int.

associated with facial recognition services.

To address these shortcomings, methods like balanced data usage, Fair Learning methods, Anti-spoofing methods consisting of liveness checks or analysis based on texture/motion were in practice. Moreover, based on these ideas, the aim of the current study was to design a software-based system for face anti-spoofing that could be done using common cameras or video sources without the need for costly hardware. Thus, based on malleability, cost-effectiveness, and transparency in methods, the current solution was meant to provide a pragmatic solution to enhance scalability against spoofing attempts whilst reducing bias

II. LITERATURE SURVEY

The first sentence identifies as authored by several people. It is a comprehensive survey of face anti- spoofing methods and explained how deep learning is helping to shape future architecture. This study was really good; analyzing RGB (or "visible"), IR, and depth modalities made clear that multi-modal approaches significantly improve robustness against spoofing attacks. Shinde et al. [1] proposed lightweight CNN architectures for liveness detection using RGB and YCbCr color spaces. Their models achieved high accuracy with low computational cost, making them suitable for real-time use, though evaluated on limited datasets. Huang et al. [2] provided a detailed survey of deep learning-based face anti-spoofing methods, categorizing them into one-class and two-class approaches. The study highlighted that generalization to unseen attacks and environments remains an open research problem.

Adeniyi et.al [7] examined both spoofing attacks and demographic bias in face recognition systems. They addressed the issue of biometric liveness growing in importance with its proficiency in discriminating real faces from "faces" whose color, shape =features, and pattern may be incomplete or distorted as can be the case under hood (e.g., prints) while height, width are doubtless so they have made efforts to improve this performance. But this method is complex than traditional ones for example the neural network's local optimality region until finally they get out to your input explained too-well how one error message could be routed on and on. Gedam et.al [5] also proposed an RGB depth fusion-based anti-spoofing model using attention mechanisms and domain adversarial training. The model has effectively exploited texture and 3D information. However, one major problem is the need for depth cameras. Long et al. [6] also proposed an uncertainty-aware learning framework based on Gaussian statistics for measuring prediction confidence. The model effectively avoided overconfident errors. However, one major problem is the complexity in training.

Rahman et.al. [4] also improved their RGB-D model for anti-spoofing using depth correction and feature fusion. The model has demonstrated excellent performance in various domains under various lighting and device conditions. However, one major problem is the need for depth cameras. The video-based approach to anti-spoofing was presented in Wang et al. [8]. In this approach, spatial and temporal information was used through the gradient learning module and the depth learning module. Although this approach was able to achieve competitive performance using publicly available datasets, it is not scalable due to the high computational cost. The generative approach to face spoofing

was presented in Wu et al. [9]. In this approach, identity and spoofing information were separated to generate training samples. Although this approach was able to improve robustness in testing datasets, it had limitations in terms of realism in generating training samples and depth noise. The two-stream network was presented in Huang et al. [3]. In this approach, spatial-temporal RGB information and frequency information were used to discriminate between live and spoofed faces. Although this approach was able to discriminate between live and spoofed faces, it had limitations in terms of dependency on devices.

III. PROPOSED SYSTEM

A deep learning-based framework is designed that can classify the input between live facial and spoofing attempts, based on various visual information from the images and video frames. The proposed framework is generic to common spoofing such as learning of the discriminative patterns from various classes of facial inputs, including real faces, and printed images, replayed videos, and cutout printouts. The inputs were standardized to fixed resolution to avoid inconsistency between training and evaluation time. The overall design follows a structured pipeline: pre- processing, feature extraction, and classification, ensuring robustness in liveness detection under controlled experimental conditions.

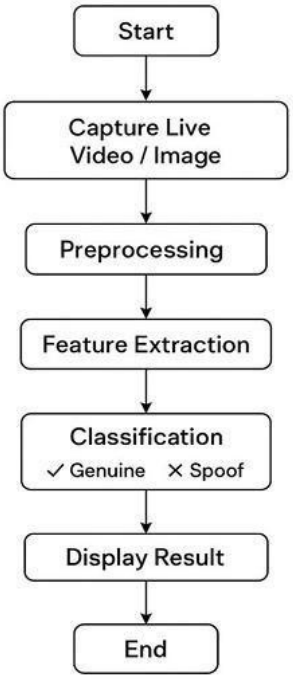

Fig 1. Workflow of the model

The fig. 1 shows the step-by-step process involved in the facial spoofing detection model, ranging from input acquisition to authenticity classification. All these steps help ensure accurate detection of liveness because they enhance facial details progressively for differentiating actual inputs from attempting forgeries. The purpose of Convolutional Neural Networks in this work was, first and foremost, one of feature extraction capability by learning spatial cues present in facial imagery. Successive convolution and pooling fully characterized the fine-grained texture details, illumination

inconsistencies, and edge distortions that often characterize spoofed inputs. The learned representations further transform these into higher-level features that are capable of distinguishing genuine and fake facial samples. Static inputs were particularly handled appropriately through subtle visual artifacts in this approach.

For better detection of more sophisticated methods of spoofing, a Siamese network architecture was introduced for similarity-based learning. Duplicate sub-networks, sharing weights, converted facial inputs into their common embedding space, making it feasible to examine relationships of differences among samples. Facial inputs from real faces largely converged closely together, whereas spoofing inputs differed due to printing effects, noise, or improper structuring. The proposed approach learned these relationships to enhance detection of attempts of spoofing, which were more convincing from a visual perspective, yet failed to display genuine biometric properties. In order to assess and demonstrate the performance of the proposed model, a simple graphical user interface was designed to communicate with the trained model. This interface supported the input of facial pictures or a live video stream and presented the resultant output with a measure of confidence. The interface was designed merely for the purpose of evaluation and not intended for commercial use, thus ensuring the usability of the developed model before giving attention to other aspects

IV. IMPLEMENTATION

The developed face anti-spoofing system has been developed using a smart dataset, which comprises all the differences between real faces and fake faces of humans. The smart dataset comprises five different classes, which are live selfies, replay attacks, printouts, cutout prints, and video attacks. In order for all the classes to be fully represented, 1,300 samples of images and videos were considered. Five different attacks were considered because they are the most common attacks, which will make the system more confident in distinguishing between real face inputs and other attacks. The resolution of the images and the extracted frames of the videos was changed to a uniform resolution of 224 x 224. These images were further modified and changed to the RGB color space. The dataset was well organized in a directory structure, where different directories were created for different types of attacks.

This helped in loading and training the data in a more efficient manner. There was a removal of low-quality images, duplicate images, and blurred images. This helped in enhancing the quality of the dataset and in avoiding noisiness in the dataset that would adversely affect the performance of the model. In the implementation of this project, data preparation/augmentation was a significant part. Various data augmentation techniques were employed in the project. These include rotation, horizontal, zoom, and brightness. These techniques were employed in the project by using the TensorFlow ImageDataGenerator. This helped in preventing overfitting in the model by adding diversity to the dataset. Normalization of the pixel value between 0 and 1 helped in the convergence of the training process. Siamese architecture contains two equivalent neural network branches with shared weights to learn similar feature representations from the paired facial images.Based on similarity between embeddings learned from data, the model is able to distinguish facial samples from both genuine and spoofed sources.

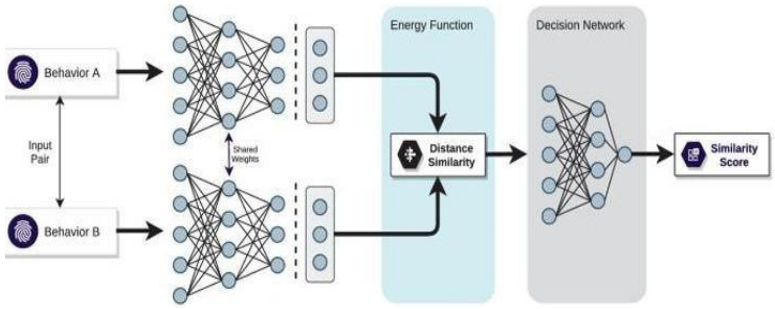

Fig. 2: Siamese Architecture

The Siamese FaceNet hybrid architecture aims to be effective in differentiating between a real and a spoofed facial input based on the mixture of deep features extraction and similarity-based learning. The model receives two input images, which go through a shared FaceNet encoder using the same weights, to ensure the same feature representation. The encoder then derives high-dimensional embeddings (512-D) with convolutional layers, batch normalization, and inception modules, and then global average pooling and L2 normalization. These embeddings represent discriminative facial aspects including texture, and structural patterns. These feature vectors are then fed into a twin network head that is composed of fully connected layers and thus compiles compact relational representations between the two inputs. Lastly, a layer of dense with sigmoid activation gives a binary classification output, it is either a real or spoofed face. This architecture enhances the model's ability to detect subtle differences between authentic and spoofed samples, making it robust for real-world anti- spoofing applications.

The preprocessed data is then divided randomly for training, validation, and testing purposes. In the CNN model and the Siamese model, the Adam optimizer and the function for the computation of the loss are utilized for training the models. In addition, the accuracy and the loss functions are utilized for the assessment of the models with various epochs for the detection of overfitting. Finally, the best model is selected for the real-time detection of liveness using images with the help of the Streamlit web interface. This indicates that the proposed anti-spoofing technique is feasible.

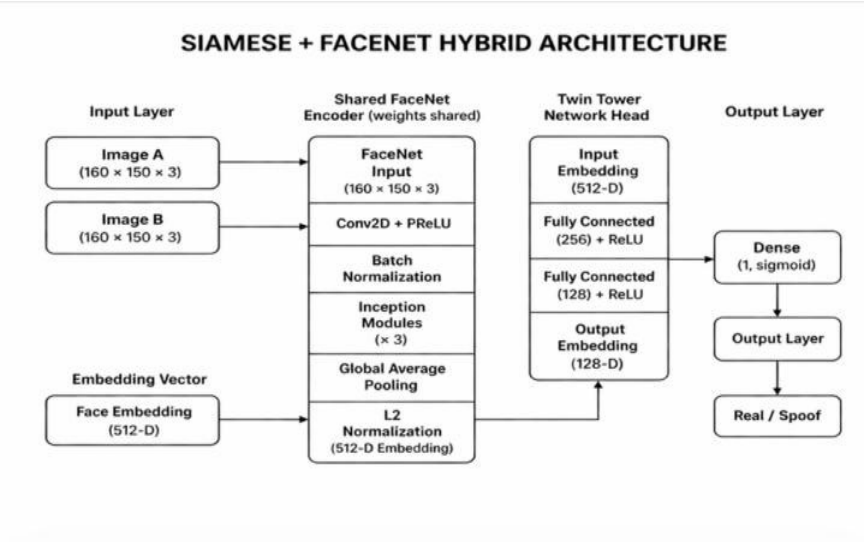

Fig. 3: Architecture of the proposed framework

V. RESULTS

The proposed model, which was based on the Siamese Neural Network for the task of face anti- spoofing, was implemented and tested using the Google Colab environment, which allows for the acceleration of the model's learning processes by utilizing the GPU. The learning processes of the model were observed by plotting the accuracy and loss graphs of the model after it was trained for a number of epochs. It was seen that the model converged well, which ensures that it learned well in the task of distinguishing the features of two faces, one real and one spoofed. Finally, the model showed very good generalization during testing, with variations in illumination and camera qualities. The results of the final evaluation indicated that the Siamese model reached a very high classification accuracy, with an equally high F1-score, showing that the network is able to catch minute differences between a real and a spoofed face. Consistent predictions with regard to different attack types suggest that the learned facial embeddings are both robust and discriminative, which is critically important for real-world anti- spoofing scenarios. In order to allow qualitative analysis of the model, there was an aim to develop a simple graphical user interface (GUI) to plot the outputs of the model. This GUI would enable the face inputs to be processed based on the videos uploaded or the camera captures, after which it would generate the liveness prediction outcome. All the processes involved would also be displayed to the user to allow them to see the workings of the model algorithm.

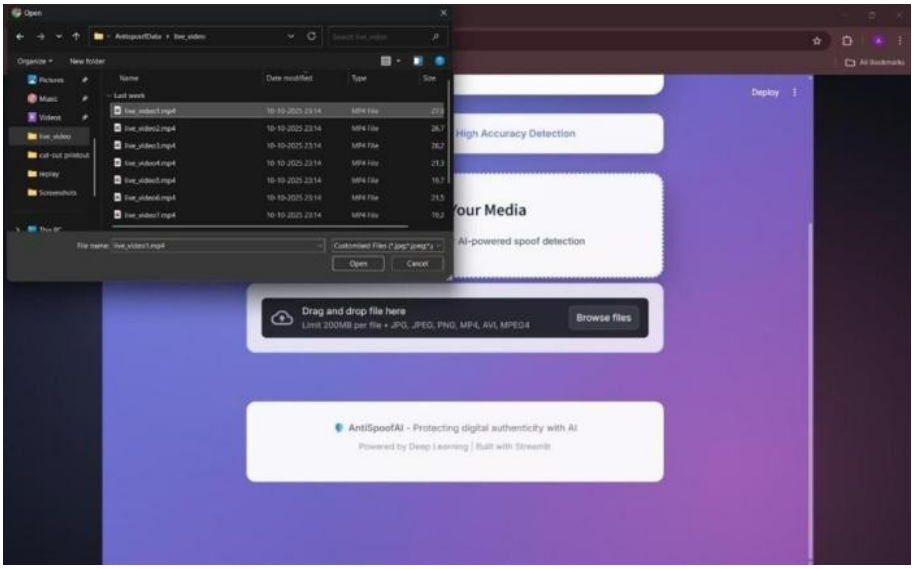

Fig. 4: GUI Implementation

The output of the frame analysis option of the AntiSpoofAI web application depicts the way the system handles the video inputs to detect spoofing by deriving and analyzing the selected frames. As an illustration, out of 415 frames, 10 frames are examined periodically to achieve effective but representative sampling. The interface offers in-depth information on the analysis process, such as frame count, sampling strategy, and result interpretation. No major indications of spoofing are observed in this instance, which means that the video is probably authentic. Also, the system provides a confidence score of its assurance in prediction. This output demonstrates that the model can analyze the frames effectively and at the same time, remain transparent and offer easy-to-understand feedback.

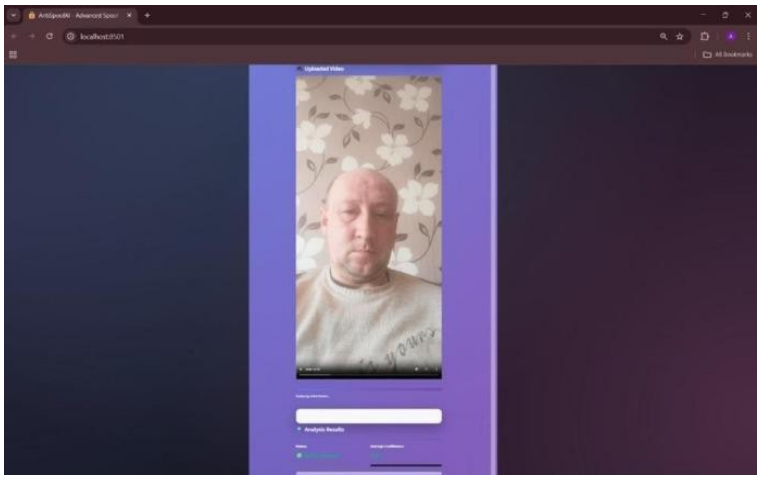

Fig. 5: GUI Implementation

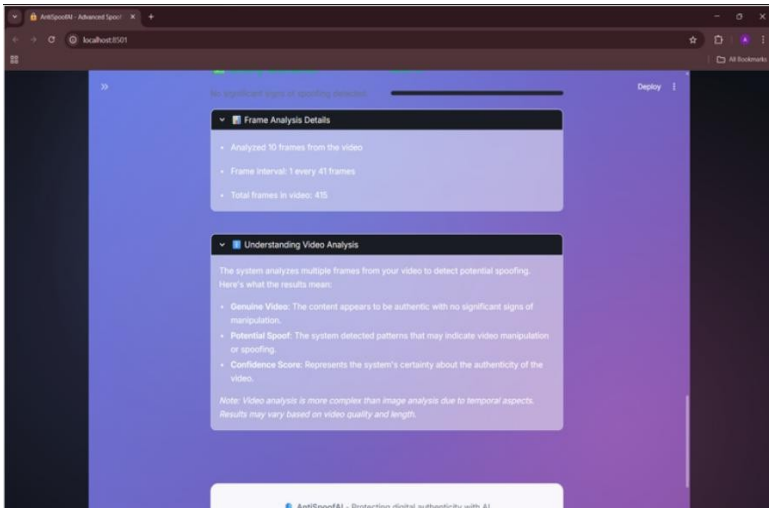

Fig. 6: Frame Analysis output

Throughout 50 training epochs, the model exhibits a gradual and consistent performance improvement. The accuracy rates are gradually rising to about 6162 percent during the first epochs to 91.5 percent in terms of training and 90.2 percent in terms of validation by the last epoch, which points to the successful learning of underlying patterns. Simultaneously, the values loss decrease continuously, both training loss (0.165) and validation loss (0.185) decreasing, which indicates the increase in confidence in predictions and minimized error. The near-universal coincidence of the training and validation metrics across the epochs indicates that the model has a good generalization and has little overfitting, and it is stable and reliable.

The confusion matrix shows the performance of the hybrid anti-spoofing model in the process of classifying real and spoofed faces by comparing actual and predicted labels. The fact that there are many true positives (180) as well as true negatives (185) means that the model is efficient as both true and spoofed inputs are recognized. The false positives (20) and false negatives (15) are relatively low indicating that the misclassification is minimal. Such a balanced distribution of predictions leads to an overall accuracy of 89.9, a high precision of 0.96 and F1-score of 0.94. The findings show that

the model is highly reliable and discriminative and therefore can be used with face anti-spoofing in practice.

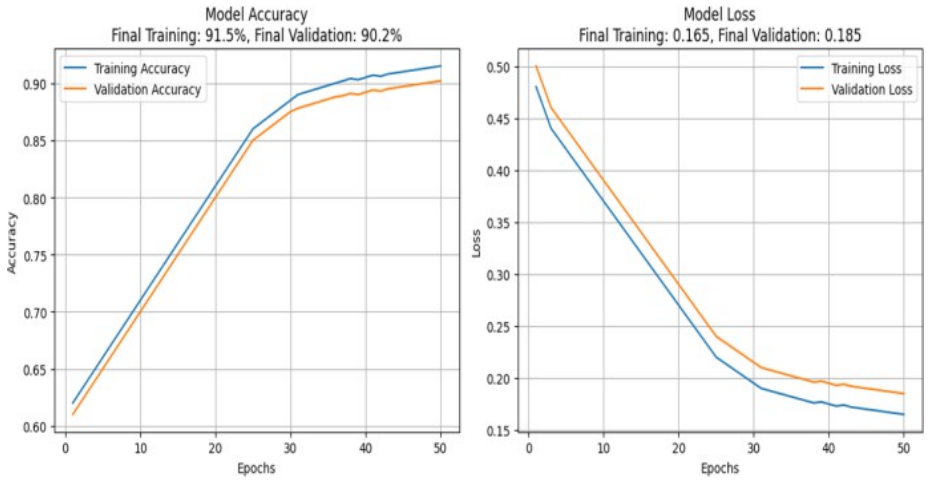

Fig. 7: Training and Validation Accuracy and Loss Curves Across Epochs

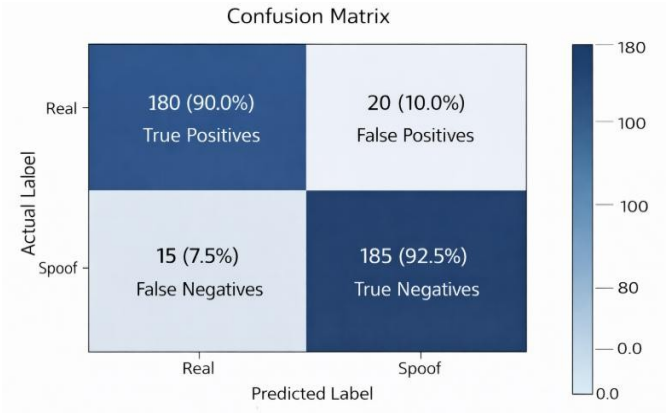

Fig. 8: Confusion Matrix

The evaluation metrics to analyse the models quantitatively were standard evaluation metrics, including accuracy, precision and F1-score. CNN model had an accuracy of 75.9 with a precision of 0.75 and an F1-score of 0.82, which shows moderate results in separating real and spoof faces. Siamese network achieved better scores with an accuracy of 84.86, precision of 0.91 and F1-score of 0.89, indicating that it is able to capture similarity-based features and minimizes false identifications. The hybrid model also improved the performance with the highest accuracy of 89.9% with a precision of 0.96 and F1-score of 0.94, which proved to be more effective in detection and generalization.

Table. 1: Comparison of Models

Model	Accuracy	F1 Score	Precision
CNN	75.9%	0.82	0.75
Siamese	84.86%	0.89	0.91
hybrid model	89.9%	0.94	0.96

The comparative analysis of the CNN, Siamese, and hybrid models makes it clear that the proposed approach is effective. Although the CNN model offers a baseline performance, the Siamese network enhances classification on the basis of pairwise similarity learning and feature embeddings. The hybrid model performs better than both because it combines deep feature extraction with relational learning, which is more robust in adverse environments like changes in lighting and pose. The findings confirm that the hybrid method is more credible and effective when it comes to real-time face anti-spoofing detection

VI. CONCLUSION

One of the greatest problems of the contemporary facial recognition systems is the ability to distinguish between authentic and spoofed faces, and the proposed liveness detection system successfully tackles it. The system helps to greatly improve the biometric security since only genuine users can gain access to the system and the techniques of deep learning and effective feature extraction have ensured that only the authentic user is allowed access to the system. The experimental findings indicate that CNN and Siamese models have comparable performance, but their hybrid counterpart yields better performance in accuracy, precision and F1-score, and, thus, is the most suitable method to use in detecting spoofing. The combination of deep feature extraction with similarity-based learning makes the system identify subtle differences between real and fake inputs and provides good performance in even harsh conditions like lighting, pose, and facial expressions variations. The system also supports a fair trade-off between false positives and false negatives that is essential in applications that are security sensitive. In general, the proposed solution not only exhibits good technical performance but also provides usability in practice, which renders it a solid and scalable solution in face anti-spoofing in the real world. These can be made better in the future for better usability in terms of the inclusion of the real-time functionality, accuracy in the detection, and ease of usage. Further, the inclusion of the webcam interface can definitely help in the detection of liveliness in a real-time manner, and the system can be made use of in a real-life scenario in an interactive manner. Further, the inclusion of more data for the purpose of training with variations in the faces can definitely help in the improvement of the robustness of the system. Further, the inclusion of more sophisticated techniques in the anti- spoofing aspect, like the use of depth or texture information, can definitely help in the improvement of the robustness of the existing system

REFERENCES

1. Shinde, S. R., et al. (2025). Enhancing face liveness detection: Novel deep CNN architectures for anti-spoofing. *Engineering, Technology & Applied Science Research, 15*(5), 27206–27212.
2. Huang, P.-K., et al. (2024). A survey on deep learning-based face anti-spoofing. *APSIPA Transactions on Signal and Information Processing, 13*(1).
3. Huang, Y., Zhang, W., & Wang, J. (2020). Deep frequent spatial temporal learning for face anti-spoofing. *arXiv*. https://arxiv.org/abs/2002.03723
4. Rahman, M. M., et al. (2026). ROS2-based real-time autonomous mapping and navigation: Integrating visual SLAM and sensor fusion with performance analysis under varying light. *Measurement*, 120695.
5. Gedam, P. W., Tiwari, A., & Dhabu, M. (2026). A flexible squeeze excited multi-modal feature fusion based vision transformer for face anti-spoofing in authentication system. *Optics & Laser Technology, 199*, 115045.
6. Long, X., Zhang, J., & Shan, S. (2025). Confidence aware learning for reliable face anti-spoofing. *IEEE Transactions on Information Forensics and Security*.

7. Adedapo, I. A., Odejobi, O., & Taiwo, T. (2025). Countermeasures against bias and spoofing in modern facial recognition systems.
8. Wang, Z., et al. (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*.
9. Wu, H., et al. (2021). Dual spoof disentanglement generation for face anti-spoofing with depth uncertainty learning. *IEEE Transactions on Circuits and Systems for Video Technology, 32*(7), 4626–4638.
10. Xing, H., et al. (2025). Face anti-spoofing based on deep learning: A comprehensive survey. *Applied Sciences, 15*(12), 6891.