International Journal of Computer Techniques–IJCT Volume 13 Issue 2, March-April - 2026

Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

FACIAL RECOGNITION SYSTEM WITH ANTI SPOOFING MACHANISM

S. Hariprakash Reddy #1, Shaik. Mahaboob Basha #2, V. Vijay Simha Reddy #3, Mr.C.Ramachandran #4

#123 UG Students, Department of Computer Science and Engineering, School of Engineering & Technology, Dhanalakshmi Srinivasan University, Trichy-621112, Tamil Nadu

Email: siddehariprakashreddy@gmail.com, mahaboobbashashaik9907@gmail.com, vsimha2005@gmail.com

#4 Assistant Professor, Department of Computer Science and Engineering, Dhanalakshmi Srinivasan University, Trichy-621112- Tamil Nadu

Email: ramachandranc.set@dsuniversity.ac.in

----------**********----------

Abstract:

Facial recognition has become one of the most common techniques of biometric authentication which is highly accurate and convenient. Nonetheless, it is still highly vulnerable to the presentation attacks like photo and video spoofing or mask-based spoofing that may undermine the security of the system. The paper proposes a Facial Recognition System with an Anti- spoofing Mechanism using the MobileNetV3 which is a lightweight convolutional neural network that allows it to be used on a mobile and a device where it has high performance. The suggested system combines the element of a facial extraction and the detection of spoof in a single deep learning architecture. The system works well to differentiate authentic attempts and fake attempts in real time by training the model on real and spoof face datasets. Trial performances prove the idea that MobileNetV3 offers an optimal trade-off conclusions in respect to accuracy, computations, and velocity, therefore, it is most appropriate to be utilized on a practical setting in terms of mobile authentication, access control, and surveillance. This method maximizes the effectiveness of facial recognition as well as providing a high level of protection against a spoofing attack.

Keywords — Anti-Spoofing, Liveness Detection, Deep Learning, Presentation Attack Detection, Facial Recognition, and Convolutional Neural Network. Anti- Spoofing, Liveness Detection, Deep Learning, Presentation Attack Detection, Facial Recognition, and Convolutional Neural Network.

----------**********----------

I. INTRODUCTION

Facial recognition technology has turned out to be one of the most noticeable and widespread biometric authentication systems in the recent years. It is not a contact device, easy to implement, and it is quick in recognizing an individual that makes it suitable in mobile authentication, access control, tracking of attendance, banking, as well as surveillance systems. Facial recognition in contrast to the old-fashioned techniques of security like passwords or PINs is based on the use of specific aspects of a face that cannot be duplicated easily. Nevertheless, in spite of its increasing usage, the technology has great security issues, particularly through spoofing or presentation attacks, whereby, ill-intentioned users seek to deceive the system with printed photographs, digital videos, or 3D face masks.

Spoofing attack is an attack in which an intruder enters a biometric sample- a photo, some video replayed- to access something inaccessible. The traditional recognition models which simply consider only the static features can easily be deceived by such attacks. Thus, anti-spoofing mechanisms have become an essential part of the contemporary facial recognition systems. The purpose of these mechanisms is to identify whether the face shown is real (live) or fake (spoof) and therefore increase the strength and accuracy.

In this regard, to overcome this weakness, scholars have come up with multiple methods of face liveness detection, which include the use of texture-based, motion-based, depth estimation, and deep learning- based methods. Deep learning has demonstrated impressive performance among them because of its capability to automatically learn complex patterns and features on data. The CNNs have been particularly useful in the differentiation between actual faces and the spoofed ones where there are small differences in text.

Nevertheless, the cost of computation is one of the biggest hurdles to deploy anti-spoofing systems that are based on deep learning. The high-performance CNNs are reliable but tend to be resource-intensive and can not be used in real-time or mobile mode.In order to conquer this, MobileNetV3 has been introduced as an effective deep neural network that computes light-weight without losing accuracy. MobileNetV3 is a mixture of depth wise separable convolutions, squeezeand excitation (SE) modules, and hard-swish activation, making it faster, smaller, and significantly more powerefficient than its counterpart, MobileNetV1.

The proposed In this study is a Facial Recognition System, embedded with an Anti-Spoofing Mechanism based on MobileNetV3. The system does the face recognition and simultaneously the spoof detection through a single deep learning system. It is configured with real and spoof samples by sets and is trained to classify input images as either real or spoof, in the process of authentication. MobileNetV3 is also lightweight, which provides it with the capability to perform in real-time without compromising accuracy, which makes it suitable to be used in real-life applications such as smartphones, internet of things, and low-power security devices.

The significant contributions of this paper are as follows:

Embarkation of a two-step recognition system that incorporates facial recognition and anti-spoofing. Application of MobileNetV3 architecture to obtain the best accuracy at minimum computational needs.

Measurement of system performance on benchmark real- vsspoof datasets, with the ability to be robust and generalize to different types of attacks.

Professionally, demonstration of the model as a viable platform to deploy in real-time and on the edges to show how practical and feasible the model can be when used in security systems today.

In general, the purpose of this study is to fill the gap between the accuracy and the efficiency of the facial recognition systems. The proposed system is capable of improving the security of biometric authentication through an efficient antispoofing system that is being driven by the MobileNetV3 and keeping the speed and computational efficiency of the system. It can be concluded that the findings of the research show that lightweight deep learning models can be used as a substantial defense against the threat of a spoofing attack against realtime facial recognition systems, which may secure and more trustworthy human-machine interaction in the future.

II. LITERATURE REVIEW

The evolution of the face anti-spoofing techniques in the past few years shows that the old manual features are steadily being substituted by the lightweight deep learning models that are trained to work in real-time. Purva Mhasakar et al. [1] provided the idea of multi-stream CNN relying on the color space analysis of face anti- spoofing in the journal Computer Vision and Image Processing (CVIP). They used the RGB and HSV feature stream-based approach to detect presentation attacks and achieved good results intradataset. The model was however problematic when it comes to generalizing its results to datasets and had failed to support real time mobile testing thereby restricting its use.

The article by TZ-Chia Tseng and others [2] explored antispoofing in live face authentication of mobile phones through the assistance of the texture and dynamic features. This was suitable at the time when it was employed in lowpower machines though it had low accuracy when the illumination was low as well as in different spoof attacks. Similarly, Sagar M S and Saravanan C [3] came up with a spoof detection method which made use of image processing method as opposed to basic handcrafted features. They were effective in 2D spoofing and not successful in 3D mask and change of environment which justifies the need of deep feature extraction models. Face spoof detection is suggested as a classification model in the article by Abhishek Dwivedi and Shekhar Verma [4], with the notions of deep learning (The Scientific Temper journal). The system proved to be more precise at identifying objects in controlled data, but seemed to falter on real-time detection and the flexibility of datasets which required medical researchers to have dynamic and lightweight models. Pawar A.H. et al. [5] proposed a deep learning-based antispoofing system in IJSRED in which the attention was directed to the texture analysis offered by CNNs. The model was successful, and it lacked any specifics of implementation and performance measures that can be replicated, so it is difficult to compare. Meanwhile, T. Naveen Prasad and B. Anuradha [6] applied Mobile Net + Haar Cascade to increase speed and detection in mobile device. Despite its good efficiency, it failed to work effectively with various illuminations and in multifaceted spoofing that prompted the necessity to have well developed adjustable architectures. R. Kumar et al. [7] proposed a hybrid EfficientNet-B0 and Vision Transformer (ViT) model that was anticipated to form a greater degree of accuracy in the detection of spoofing. A hybrid setup was more efficient in extracting features, but was significantly more complicated to calculate and could not run in real time mobile application. This demonstrates the trade- off between the power of high features and portability. The Face Recognition Attendance System presented in the article by Dr. Shabeena Sayed et al. [8] was created with Anti- Spoofing Detection. Their system also brought together attendance automation with liveness verification but suffered performance issues in low hardware and low-light environments, which demonstrates the need to have faster and lighter deep learning models to execute in other environments. Gap Identified Inter-Studies.

Most of the models lack cross dataset generalization and are susceptible to novel forms of spoofing. Computational efficiency is also an issue that especially imposes on mobile or embedded systems. With many studies, there is no information on how the implementation was made and even the validation of the performance in real time was not provided. Models that fulfil the requirements of accuracy and speed in a challenging illumination and pose are found not in great numbers.

The manner in which the Proposed Work Fills These Gaps. The limitations that the proposed Facial Recognition System with an Anti-spoofing Mechanism based on MobileNetV3 would address through application of lightweight yet effective CNN that can be applied in real-time in a mobile application. The effectiveness of MobileNetV3 is that it offers accurate detection of spoofing attacks with a low latency and resources expenditure simultaneously. This has been employed to harmonize the disparities among power, scalability and practical applicability and is therefore the most appropriate to the next generation biometric authentication systems.

III. PROPOSED METHODOLOGY

It is possible to say that, based on the proposed Facial Recognition System and Anti Spoofing Mechanism, it is selective in distinguishing the true (live) and spoofed (fake) facial images in the real world of application. It uses the system exploiting MobileNetV3 as one of the most effective convolutional neural networks optimized to use embedded and mobile devices. The time and cost of executing the algorithm will involve five processes, including data preprocessing, model architecture, training strategy, evaluation, and deployment. Each of the stages is applied differently to provide a balance between the accuracy, computability and feasibility of the real world.

A. Description and Preprocessing of the dataset.

The experiment involves CASIA Face Anti-Spoofing Dataset (CASIA-FASD) which are real face videos and spoof face videos captured under various conditions of lighting, angle, and devices. The dataset (printed photo attacks, replay attacks and cut-photo attacks) shares three major attacks of spoofing that would form a challenging baseline to test the model.

All video frames were deleted and transformed into still pictures. The dataset was divided into three subsets above, i.e., training, validation and testing ones 80 percent and 10 percent respectively. All images were reduced and resized to the size of 224x224x3 pixels, the input size of MobileNetV3.

The scaling of the pixel values into the range of 0 to 1, which was done as a normalization, was to guarantee quicker convergence during training. The data augmentation was done to improve the generalization and avoid overfitting by feeding the Image Data Generator application in Keras with data. The augmentations included:

- Random rotations (+-20deg)
- Horizontal flips
- Zoom movements and movements
- Brightness variation

This ensured that the model had a variety of visual conditions during training which simulated the changes in light in the real world plus changes in pose. The processed data were then stored so that the data would save time in the redundant processing.

B. Model Architecture

MobileNetV3Small is an architecture that can be used in features extraction due to its high accuracy-efficient trade off. It consists of depth wise convoluted Squeeze-and- Excitation (SE) blockswhich reduce the size of the parameters and the representational capacity.

To take advantage of transfer learning, the base model was MobileNetV3 with pretrained weights trained on ImageNet. Adjustment of the upper most layers was sufficient to fit some characteristics of real and spoof faces. Final network structure includes layers that are as follows: Base Model: MobileNetV3Small (frozen base layers). Global Average Pooling Layer: Minimisation of spatial dimensions and feature map pooling.
Dense Layer (128 units, ReLU activation): This layer is trained under the influence of high-level discriminating details.
Dropout Layer (rate = 0.4): It is an algorithm that prevents overfitting with the implementation of random selection of neurons to drop out. Output Layer (1 unit, Sigmoid activation): This is binary (live (0) or spoof (1)).

The model was generated with the Adam optimizer and a learning rate of 1e-4 that has an adaptive momentum and converges quickly. The loss value that was used was binary cross-entropy and Accuracy, Precision, Recall, and AUC (Area Under the ROC Curve) were employed to analyze the performance of the loss.

C. Training Strategy

The training was done in a number of stages in an attempt to maximize efficiency and accuracy. In the initial experiment the MobileNetV3 base frozen custom dense layers were initially trained. This allowed this model to be task-specific to the face features yet not cause interference on the already pretrained filters. In the second step, MobileNetV3 finetuning upper-layers were selected and unfreezing was taken.

The training was carried out In a batch of 32 and a maximum of 100 epochs. Two key callbacks were used:
Early Stopping: The loss of validation is checked and the training is terminated once again when no longer increasing gains.

Reduce LR On Plateau: The learning rate will automatically decrease to a situation in which the validation loss does not reduce any longer.
This was checked in terms of Keras callbacks so as to determine the resilience of the models. The best model weights were saved under the name best model keras and bestmodel.h5, and periodic checkpoints (e.g., ckptepochweights.h5) were saved, which could be used to restart training. It was efficient due to loss prevention when interruption took place and efficiency in experimentation.

D. Evaluation and Analysis

The last procedure was to test the model they had been trained on test data. Accuracy, Precision, Recall, F1-score and AUC were the measures of evaluation. As a Confusion Matrix, the correct and the incorrect classifications were indicated.
In order to find the stability of the model training, the curves of the model training and validation accuracy and loss were plotted. The Receiver Operating Characteristic (ROC) realized the model was sensitive and specific and it is therefore effective in distinguishing between live and spoof faces.

Good performance with the trained model was archived,
where: Accuracy: Above 85.67%
Validation AUC: Close to 0.93
There are small false rejection (FRR) and false acceptance (FAR) rates.
The actions indicate that MobileNetV3 is a light but powerful setup as it is stronger than the traditional CNN and handcrafted feature methods. Another good behaviour of the model was observable in various lighting conditions and pose condition.

E. Real-Time Deployment Accuracy

To facilitate real time applications in mobile and edge applications, the trained model was disclosed to TensorFlow Lite (TFLite). There has not been any trade off of size or latency (due to model quantization) which has been applied to reduce model size. This allowed making a straightforward inference to devices with lower computing capabilities such as smartphones and Raspberry Pi.
Precision 85.76% 83%

Recall 87%
F1-Score 85%
AUC 0.93
The Introduced software also works with live camera feed and provides the result to TFLite model in real-time. Based on the likelihood of prediction, there will be the display of the words LIVE FACE DETected or SPOOF FACE
DETected.

This kind of system could be integrated into the security systems, attendance schemes and digital authentication systems and even low resource conditions will provide the correct identity check in such an environment. Operating within real time setting and highly reliable and fast would be efficient.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed Facial Recognition System and anti-spoofing System implemented using MobileNetV3 were created on the basis of the windows 11 and i7 Intel processor and 16GB RAM heed by using the TensorFlow and Keras programs. The model was trained and tested on CASIA Face Anti Spoofing Dataset which contained real and spoof face samples at varying illumination, angle and the device settings.

A. Experimental Setup

The data used in experimentation has been divided in the healthy ratio of 80:10:10 training, validation and testing respectively. The training images were made more diverse through normalization and augmentation of the training images. The model will be acquired after 100 epochs using a batch size of 32 and the Adam optimizer (learning rate = 1e4) and binary cross-entropy loss. Early termination and schedule of learning rate came in handy in avoiding overfitting and provide a stable convergence.
I applied accuracy and loss graphs to observe the training process of the training stage and training stage validation. The checkpoints mechanism was switched such that automatically, the best weights with which the test should be done and deployed were saved.

B. Performance Evaluation

The traditional measures of the model analysis were Accuracy, Precision, Recall, F1-score and AUC (Area Under the Curve). The results were obtained on the test dataset and they were as follows:

Metric	Value
Accuracy	85.76%
Precision	83%
Recall	87%
F1-Score	85%
AUC	0.93

The obtained accuracy demonstrates that the model can distinguish between live face and spoofed faces in most of the test sample. The value of the AUC at 0.95 means that the model has great classification ability i.e. It is able to distinguish real and counterfeit images with high accuracy regardless of other situations.

C. *Confusion Matrix Analysis*

The performance of classification was depicted by drawing Confusion Matrix. It shows four categories:

True Positives (TP): Live faces are identified rightly.
True Negatives (TN): These are faces that are rightly reported to be spoof.

False Positives (FP): False alarms?

False Negatives (FN): Live faces were as spoof.

The analysis of the matrices has shown that the number of errors in classifications was minimal which serves as evidence of the effectiveness of the process of MobileNetV3 feature extraction. The circumstances of low-resolution spoof samples and low light were major mistakes.

D. *AUC Interpretation and ROC Curve.*

The ROC curve that was previously plotted between the True Positive Rate (TPR) and the False Positive Rate (FPR) presented the sharp growth up to the upper left corner and this implied the existence of a high discriminating power. The fact that the AUC is 0.95 is indicator of the fact that this model can be used effectively in discriminating between real and spoofed faces.
Having the value of the AUC higher means that the classifier is highly sensitive (finds the true faces) and specific (rejects the spoof faces) hence, it is applicable in the biometric authentication system.

E. *Result Visualization*

A webcam interface was applied whereby the image of face was fed into the model in the process of real time testing. The system was able to recognize that each of the faces is a Live or a Spoof based on the probability level of prediction (>0.6 = Spoof,<0.6=Live).

Sample results:
Live Input Image 1: Live – Predicted: Live (0.18 Probability
Input Image 2: Spoof – Output: Spoof (0.72 Probability)

Image 3: Face on Paper – Prediction: Spoof (0.87 Probability)

The system had the capability to provide consistency in prediction under different light and angle conditions which confirmed the consistency under real world testing conditions.

F. *Comparative Analysis*

The suggested MobileNetV3 was determined to achieve the competitive inference speed and comparable accuracy within a reduced computational load level than the previous researches on the conventional CNN and Efficient Net models. Other advanced systems that had state-of-the-art high accuracy of 90-93% recorded high parameters and expensive GPUs. The proposed approach achieved its accuracy rate of 85.76 percent with a small amount of resource; that is why it is applicable according to mobile and embedded platforms.

G. Discussion

The experiment results prove that Mobile Net V3 is a tradeoff that can be effectively used when it comes to performance and efficiency. Its small size allows it to be implemented in real time without loss of accuracy of classification. The value of AUC of 0.95 indicates that the model possesses enormous abilities of responding to spoofing attacks such as photo and replay attacks and also a mask based fake. However, there were few instances of misclassification in cases of low illumination and radical face angles. These problems can be resolved in future work by incorporating the time factor or incorporation of the depth maps and eye- blink detector to make it more resistant to a more advanced high tech spoofing attack.

V. CONCLUSION AND FUTURE WORK

This paper has created and assessed a Facial Recognition System using Anti-Spoofing Mechanism based on MobileNetV3 on CASIA Face Anti-Spoofing Dataset. The model was developed to effectively differentiate between live and spoof faces using deep learning methods thus reaching an astounding accuracy of 85.76% and an AUC of 0.95. The findings also suggest that MobileNetV3 due to its lightness architecture and high representational efficiency is effective to be used in real-time applications with low computational capability.

This model was very effective to distinguish between real and spoofed images since it learnt more complex patterns of facial texture and fine variations in illumination and depth- related clues. Improved generalization and robustness were helped by the data augmentation, class balancing and adaptive schedule of learning rate. The suggested technique can be simply embedded into the existing biometric authentication system to augment the security level in face- based access control systems, Internet verifications, and surveillance systems. In spite of good performance witnessed with the proposed system, some restrictions were realized when poor light occurs, side poses, and motion blur. Such instances sometimes resulted in inaccurate classification of a case because of a lack of time information in one-frame classification. Because MobileNetV3 is more geared towards spatial features, the model cannot easily capture motion features, which can be crucial to the application of detecting dynamic instances of spoofing like video replay or 3D mask spoofing. Future Work

To improve it in the future, real-time face anti-spoofing with the use of a hybrid deep learning model that integrates MobileNetV3 and a Temporal Shift Module (TSM) may be developed based on the system. By implementing TSM, the model will be able to describe the inter-frame differences in time and movement, which will make it possible to differentiate between natural scenarios of facial movements (eye-blink, lips wrapping and moving) and non-moving spoof patterns.
This combination will probably have a great impact in enhancing the accuracy and hence lowering false positives in actual practice. The implementation of the real-time version will also feature live-detection using webcams and optimized inference using TensorFlow Lite (TFLite) so as to deploy it in edge and mobile hardware.

In addition, future employment can be dedicated to: Increased dataset comprising of multi-ethnic faces and various spoofing (print, video and 3D mask).

A way to enhance the model transferability to different camera devices is by using domain adaptation techniques.
Integrating depth estimation, infrared sensing, or eye-blink detection into the auxiliary inputs to enhance the spoofing power.

Training a real-time interface that is easy to use to predict live as well as receiving feedback and retraining the model with dynamic samples. To conclude, the suggested MobileNet V3 face recognition and anti-spoofing system is a good basis of a secure and efficient face authentication. Adding the feature of temporal learning (MobileNetV3 + TSM) to the future, the system has a chance to perform real-time, highly-accurate, and lowlatency which makes it a promising system in the next generation of biometric security systems.

REFERENCE & BIBLIOGRAPHY

1.A. H. Pawar, N. Kadam, Y. Dadas, S. Kakade, and K. Kamble, "Face Anti-Spoofing Using Deep Learning Approach," International Journal of Scientific Research And Engineering Development (IJSRED), vol. 6, no. 11, pp. 1– 3, 2023.

2.M. S. Sagar and C. Saravanan, "Face Spoof Detection Using Image Processing," International Journal of Creative Research Thoughts (IJCRT), vol. 9, no. 6, pp. 478–481, 2021.

3.T.-C. Tseng, T.-F. Shih, and C.-S. Fuh, "Anti-Spoofing of Live Face Authentication on Smartphones," Journal of Information Science and Engineering, vol. 37, no. 3, pp. 605– 616, 2021.

4.S. Sayed, S. Fatima, Q. A. Kader, M. Ebrahim, and S. M. Ibrahim, "Face Recognition Attendance System with AntiSpoofing Detection," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 5, no. 11, pp. 230–238, 2025.

5.A. Dwivedi and S. Verma, "SCNN-Based Classification Technique for Face Spoof Detection Using Deep Learning Concept," The Scientific Temper, vol. 13, no. 2, pp. 165– 172, 2022.

6.P. Mhasakar, S. Mandal, and S. K. Mitra, "Multi-stream CNN for Face Anti-Spoofing Using Color Space Analysis," Computer Vision and Image Processing (CVIP), vol. 2, no. 1, pp. 45–53, 2020.

7.T. N. Prasad and B. Anuradha, "Face Anti-Spoofing and Liveness Detection Using MobileNet and Haar Cascade Algorithm," International Journal of Scientific Research in Science and Technology (IJSRST), vol. 10, no. 2, pp. 34– 39, 2023.

8.R. Kumar, A. Sharma, and M. Singh, "Hybrid EfficientNetB0 and Vision Transformer Model for Face Spoof Detection," Springer Nature Computer Science, vol. 5, no. 3, pp. 215– 227, 2024.

9.J. Patel and N. Mehta, "Lightweight CNNs for Real-Time Face Liveness Detection," IEEE Transactions on Information Forensics and Security, vol. 15, no. 4, pp. 1021–1030, 2020.

10.Y. Zhang, Y. Liu, J. Wan, and G. Guo, "CASIA-SURF: A Benchmark for Face Anti-Spoofing," in Proc. IEEE CVPR Workshops, pp. 1000–1008, 2020.

11.X. Li, H. Wang, and T. Zhang, "Generalized Face Presentation Attack Detection with Cross-Domain Learning," Pattern Recognition Letters, vol. 152, no. 2, pp. 76–85, 2021.

12.J. Kim and S. Park, "MobileNetV3-Based Lightweight Architecture for Real-Time Face AntiSpoofing," Sensors, vol. 22, no. 5, pp. 2101–2112, 2022.

13.T. Nguyen, H. Le, and P. Tran, "Temporal Shift Module for Face Anti-Spoofing in Videos," IEEE Access, vol. 10, pp. 78112–78123, 2022.

14. H. Gao, X. Ren, and L. Liu, "Depth and RGB Fusion for Face Spoofing Detection," Neural Computing and Applications, vol. 35, no. 4, pp. 3251–3265, 2023.

15. R. Zhao and K. Liu, "Transformer-Based Framework for Face Presentation Attack Detection," in Proc. IEEE CVPR Workshops, pp. 540–548, 2023.

16.C. Luo, Y. Chen, and F. Zhang, "Enhancing Spoof Detection Under Low Illumination Using Adaptive Feature Enhancement," Pattern Analysis and Applications, vol. 26, no. 6, pp. 489–500, 2023.