# A TWO-STAGE HYBRID METHODOLOGY FOR FORGERY DETECTION AND PALMPRINT AUTHENTICATION

Vatsal Aggarwal and Yash Saini

## Introduction

Many biometric systems have been successfully developed which use palmprint as their basis of authentication. However, these systems are prone to various spoofing attacks (majorly print and digital) which ought to be detected.

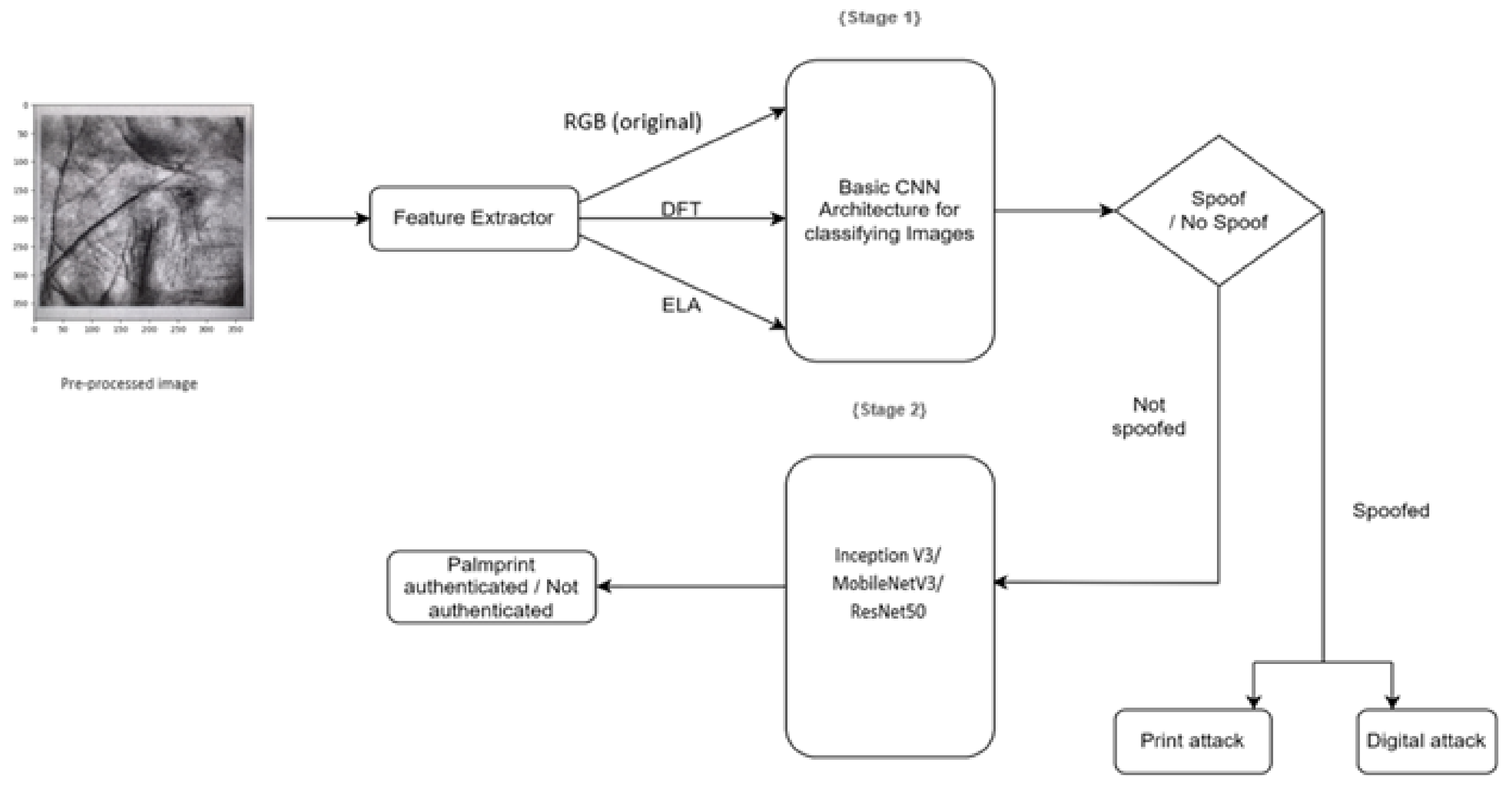
## Methods

### Stage 1

- Acts a defense mechanism to detect print/digital spoofing.
- Features are extracted after which DFT (Discrete Fourier Transform), ELA (Error Level Analysis) and original images are passed to the basic CNN model with 63000 trainable parameters. 3 models were separately trained on these features (original, digital and print attack images for each technique).
- The best results are seen with the DFT features as it eliminates 99% of forged images.

### Stage 2

- Acts as a palmprint recognizer/authenticator.
- Inception V3, ResNet-50 and MobileNetV3 were trained on the original image data. These are used to determine as to which of the 230 classes (IITD palmprint V1 dataset) the palmprint belongs to.



*A two-stage forging detection and palmprint authentication system architecture*

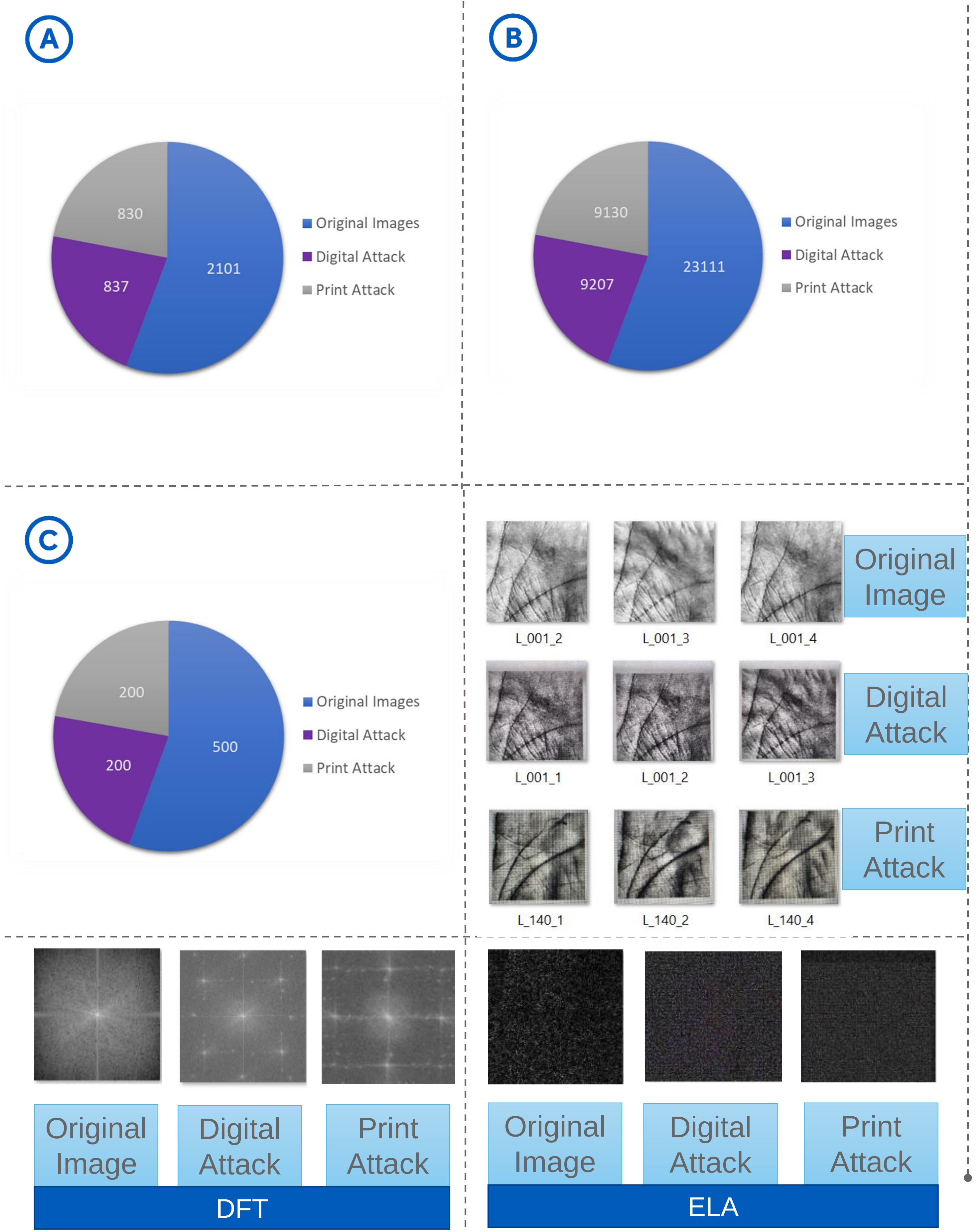
## Data Analysis

The proposed approach uses IITD palmprint V1 dataset which has 1300 segmented images each of left and right palm. Stage 1 data details are described below. For Stage 2 all the three models were trained on approximately 23,000 augmented images of 230 subjects.

A. Stage 1 training dataset before augmentation

B. Stage 1 training dataset after augmentation

C. Final test dataset of unseen images for both stage1 and stage2.

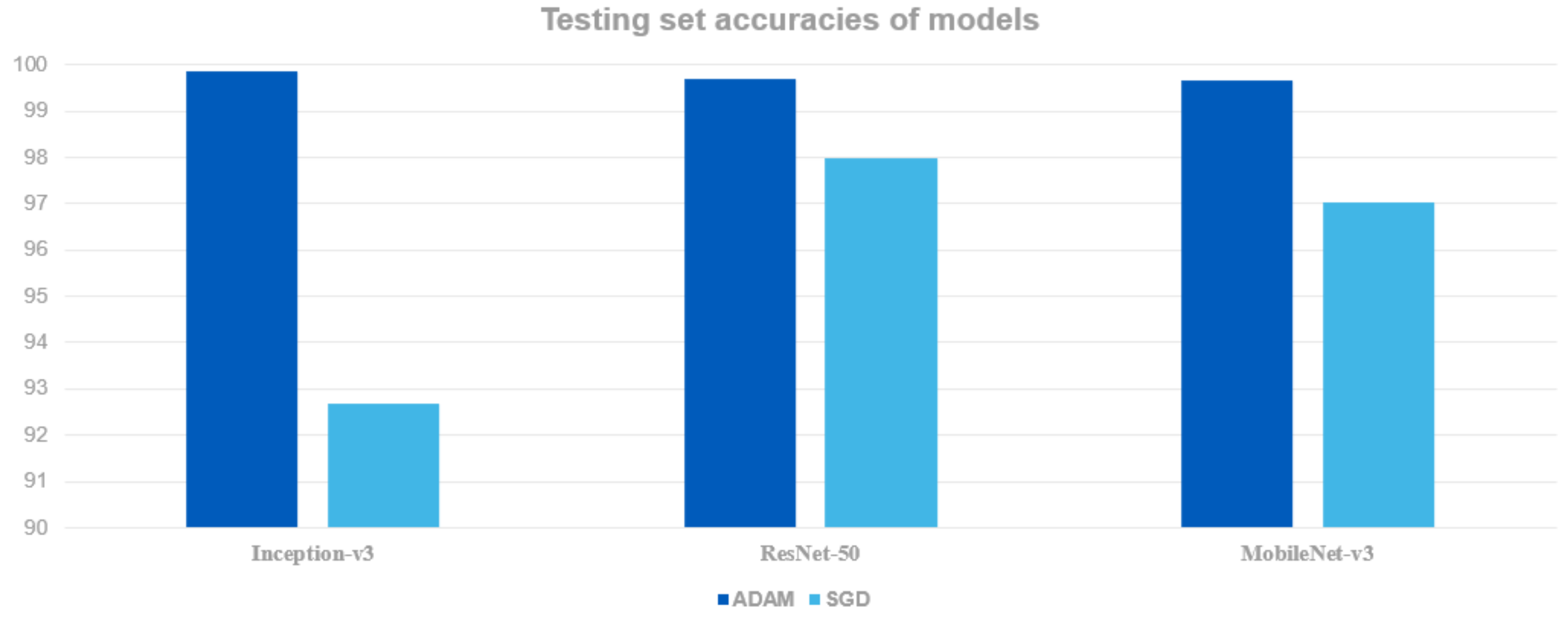


## Results

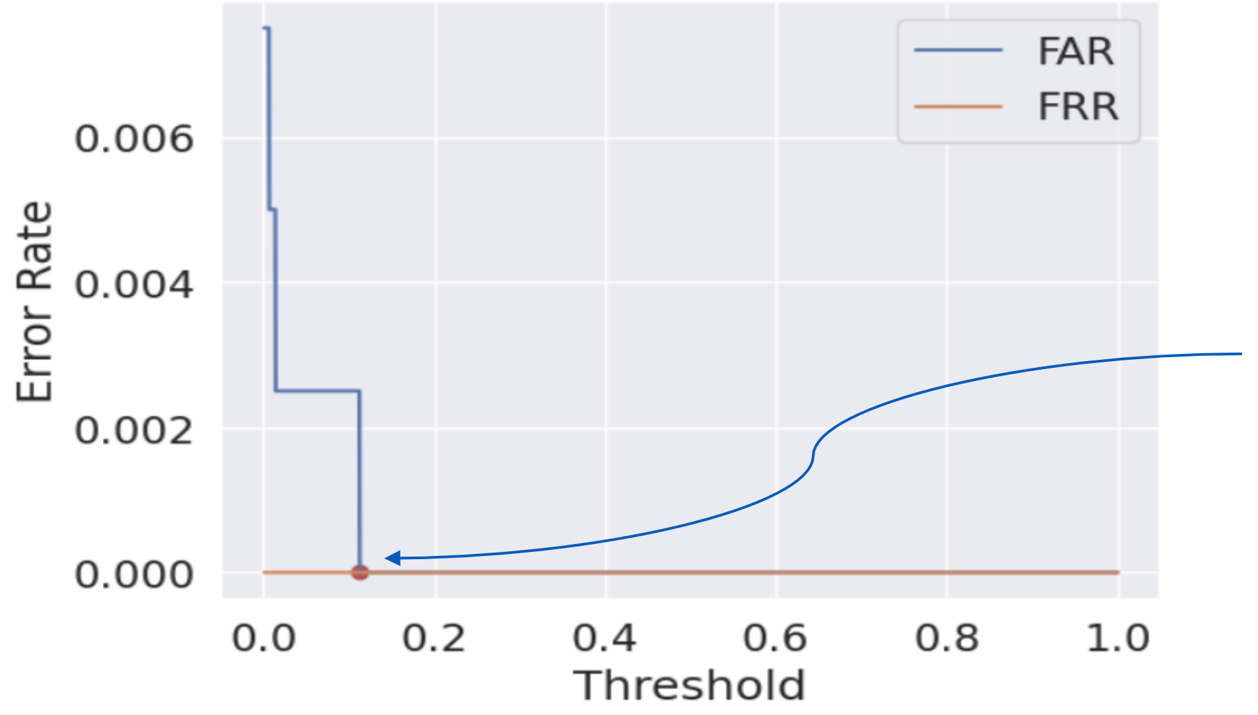
It is observed that DFT performs the best with the accuracies pertaining to 99% for stage 1.

| | Table 1 – Accuracies for DFT/ ELA and RGB | |
|---|---|---|
| For Epoch 25 | Training Accuracy | Testing Accuracy |
| DFT | 99.701 | 99.651 |
| ELA | 56.003 | 54.795 |
| RGB (Original Image) | 89.819 | 89.591 |

For stage 2, when the three models (Inception-v3, ResNet-50 and MobileNet-v3) are tested with Adam and Sgd optimizers, it is observed that Inception-v3 with Adam optimizer gives an accuracy of 99.87% as shown in the figure below.

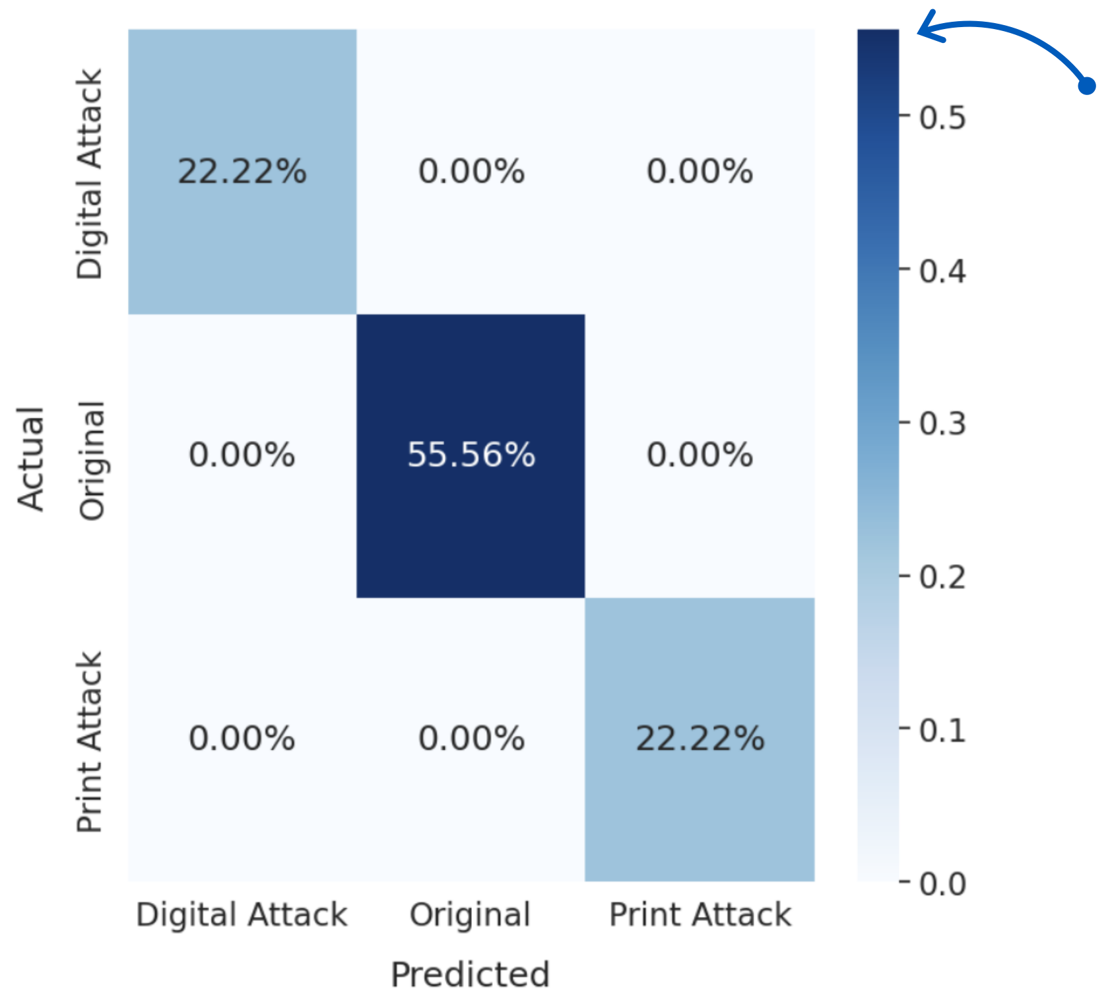


For the final pipeline stage, the image after being evaluated from stage 1 moves to stage 2, the anti-spoofing metrics for the final process are given below. It has been observed that with DFT features, F1-score of 1 on test data was obtained.



The figure represents FAR and FRR for DFT features on test set.

**Equal Error Rate**



The figure represents confusion matrix of DFT on test set.

## Conclusion

Forgery detection in palmprint authentication systems is the need of the hour. The 2-stage technique presented here, successfully detects the print and digital attacks introduced in the otherwise original dataset. Some consolidated results are concluded below:-

- **Stage 1:** DFT features gave a testing accuracy of 99.651%.
- **Stage 2:** It has been observed that Inception-v3 model with Adam optimizer performed the best with a test accuracy of 99.87%.
- **Final pipeline:-** Using DFT features and any of the 3 models, test accuracy of 100% was noted. F1 score of 1 was calculated. Also, for a threshold of 0.1, EER of 0.00 was observed.

## References

1. Farmanbar, M., Toygar, Ö. Spoof detection on face and palmprint biometrics. SIViP 11, 1253–1260 (2017). https://doi.org/10.1007/s11760-017-1082-y

2. H. Shao, D. Zhong, X. Du, S. Du and R. N. J. Veldhuis, "Few-Shot Learning for Palmprint Recognition via Meta-Siamese Network," in IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1-12, 2021, Art no. 5009812, doi: 10.1109/TIM.2021.3076850.

3. E. Thamri, K. Aloui and M. S. Naceur, "New approach to extract palmprint lines," 2018 International Conference on Advanced Systems and Electric Technologies (IC_ASET), Hammamet, Tunisia, 2018, pp. 432-434, doi: 10.1109/ASET.2018.8379895.

University at Buffalo The State University of New York

Department of Computer Science and Engineering,
University at Buffalo

buffalo.edu