UNIVERSITY OF JOHANNESBURG

A Model for Face Anti-Spoofing based on Deep Learning and Ensemble Learning Methods

Mr. S Maphisa
Prof. D Coulter

Introduction

- Despite significant advancements in face recognition, existing systems are subject to spoofing attacks.
- Previously different anti spoofing approaches have been developed to detect whether a living person or an artificial copy is in front of a facial recognition system's camera.
- Yet developing effective protection techniques against this threat has proven to be a difficult challenge The need for an efficient face anti-spoofing system still exists.
- The aim is to implement four different pipelines for face anti spoofing attacks using deep convolutional neural networks.
- The final model combines different pipelines using ensemble learning algorithms.

- **Spoofing Attacks**:
- Face spoofing attack refer to the act of using false biometric identity of a known user by an attacker in the attempt of gaining unauthorized access.
- Types of face spoofing attack include:
  - **Photo attack** : a photo attack consists of displaying a photograph of the attacked identity to the sensor of the face recognition system.
  - **Replay attack** : an attacker could play a video of the legitimate user in any device that reproduces video and then presents it to the sensor/camera.
  - **3D Mask attack** : in this type of attack, the attacker builds a 3D reconstruction of the face and presents it to the sensor/camera.
  - **Other attacks** : makeup, surgery, cuts, etc.

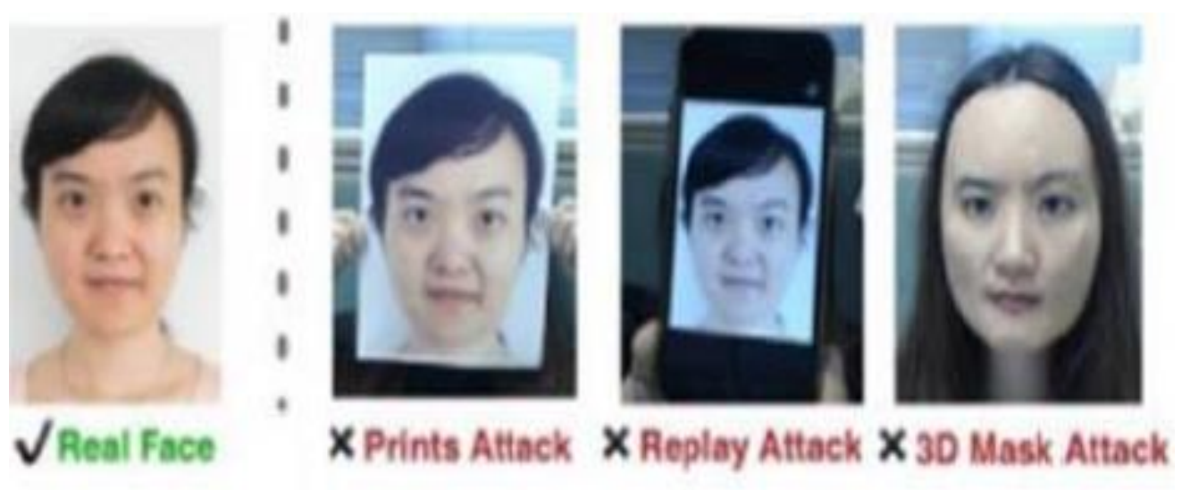


Figure 1: Typical example of Face spoofing attacks.

- **Anti-Spoofing Detection**:
- Face spoofing detection is the countermeasure for face spoofing attacks. Numerous anti spoofing techniques to detect and possibly eliminate such vulnerability exploits have been explored over the year. These anti-spoofing techniques are grouped into the following categories:
  - Face Anti spoofing based on Motion Analysis Methods.
  - Face Anti spoofing based on Texture Analysis Methods.
  - Face Anti spoofing based on General Image Quality Assessment Methods.
  - Face Anti spoofing based on Hardware Methods.

Methodology

- **Proposed Model:**

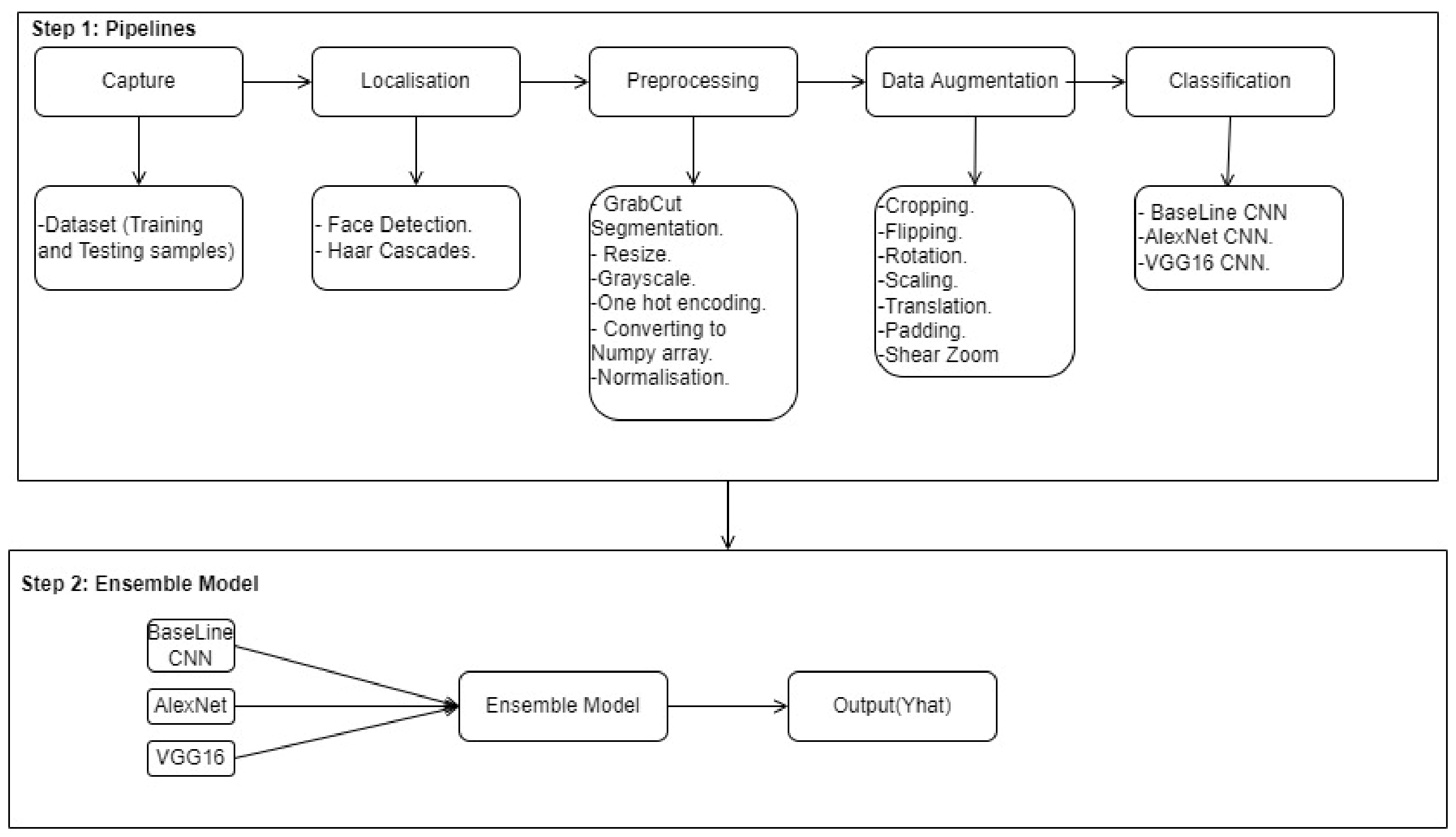


Figure 2: The Proposed Model Architecture.

- The study implements and train deep convolutional neural networks pipelines.
- Then Combine the pipelines using ensemble methods to form the final Anti spoofing model.
- The study then measures the performance of each pipeline during training and testing stage using classification metrics (accuracy, precision, recall, F1 score, ROC, and AUC).

- **Datasets**:
- The study uses two face anti-spoofing dataset: NUAA photo imposter database and CelebA-spoof dataset.
  - **NUAA Photo imposter database**:
    - The NUAA Photograph Imposter Database (Fig 3), which is open to the public, incorporates pictures of each proper customer's right of entry and image assaults.
    - Each person's facial image graph is captured over the route of 3 periods separated using round weeks, with the ambient and light instances various from consultation to consultation. For every subject's recording, there are 500 photos.
    - The pictures within the database have been taken using well-known cameras and feature a decision of 640*480 pixels for 15 subjects.
  - **CelebA- Spoof Dataset:**
    - CelebA-Spoof (Fig 4) has 625,537 images of 10,177 patients, a significant increase over the datasets that are currently available.

Figure 3: Examples of NUAA Photo Imposter Database.

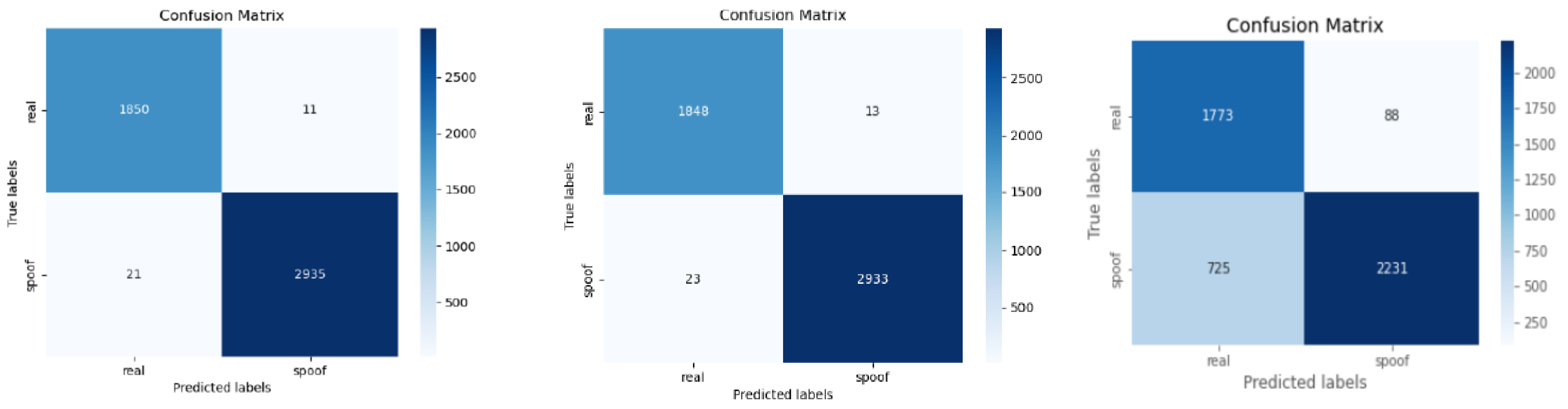
Figure 4: Example of CelebA – Spoof Datasets

Results

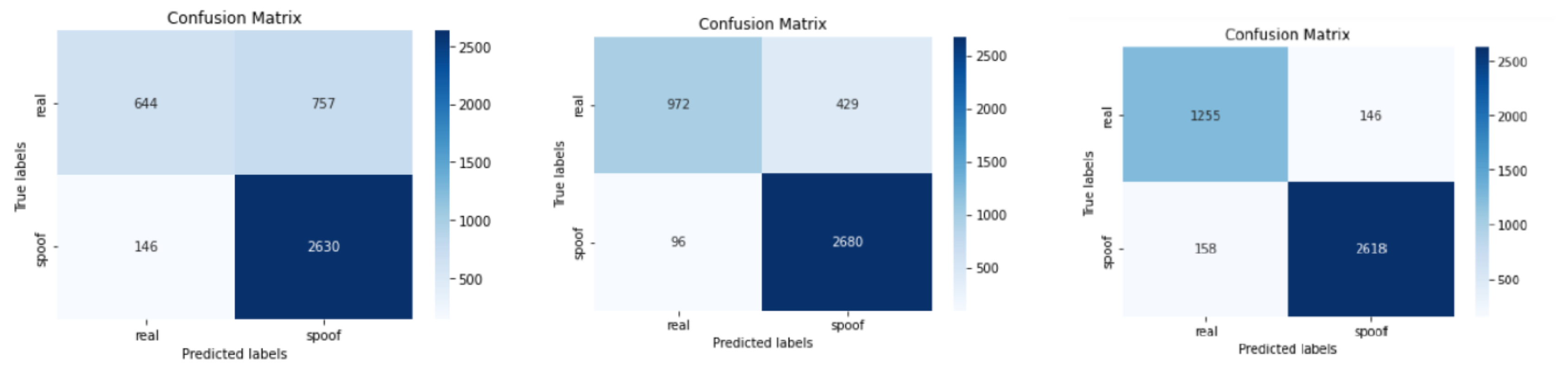
- **Model Performance**:

Dataset	Pipeline	Accuracy (%)	Precision	Recall	F1 score	AUC
NUAA Dataset	Baseline CNN	99,33	0,99	0,99	0,99	1,00
	AlexNet CNN	97,67	0,9745	0,9763	0,9789	1,000
	VGG16 CNN	98,6	0,9832	0,9876	0,9853	0,980
CelebA Dataset	Baseline CNN	78	0,80	0,70	0,72	0,816
	AlexNet CNN	87	0,89	0,83	0,75	0,936
	VGG16 CNN	92,7	0,92	0,92	0,92	0,976

- **Confusion Matrix**:



- **Figure 5**: Confusion matrix using NUAA dataset for Baseline pipeline (left), Alexnet pipeline (center), and VGG16 pipeline .



- **Figure 6**: Confusion matrix using NUAA dataset for Baseline pipeline (left), Alexnet pipeline (center), and VGG16 pipeline .

- **Receiver Operating Curves:**

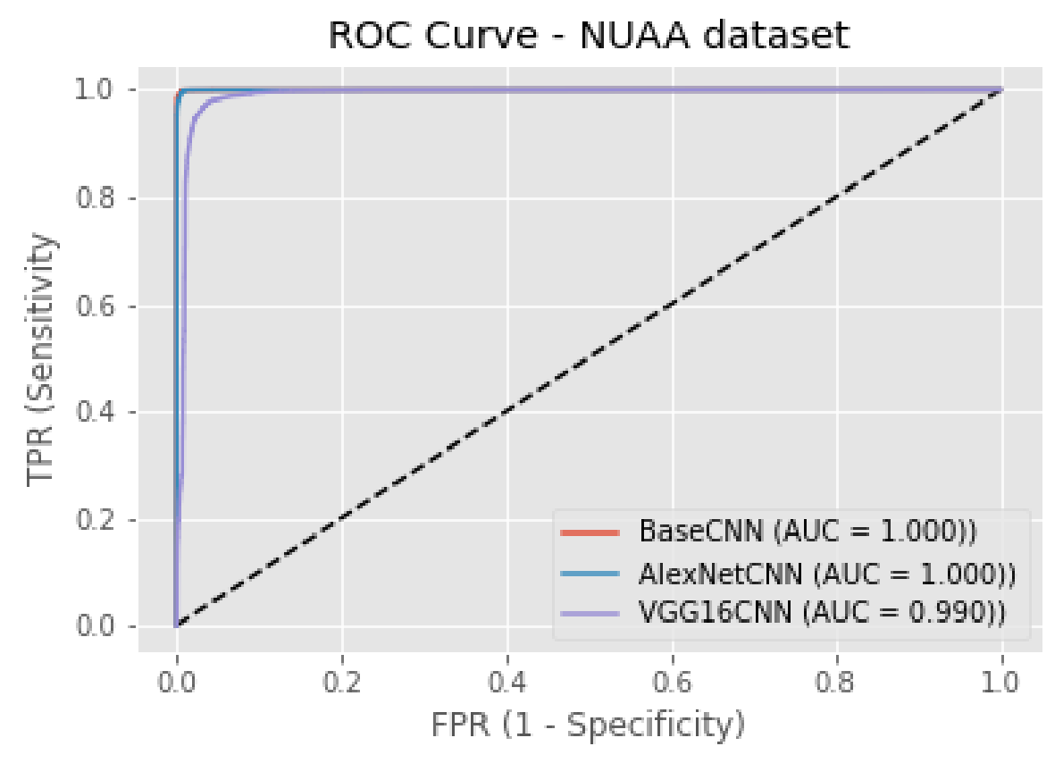


Figure 7: Performance Comparison using ROC for NUAA pipelines.

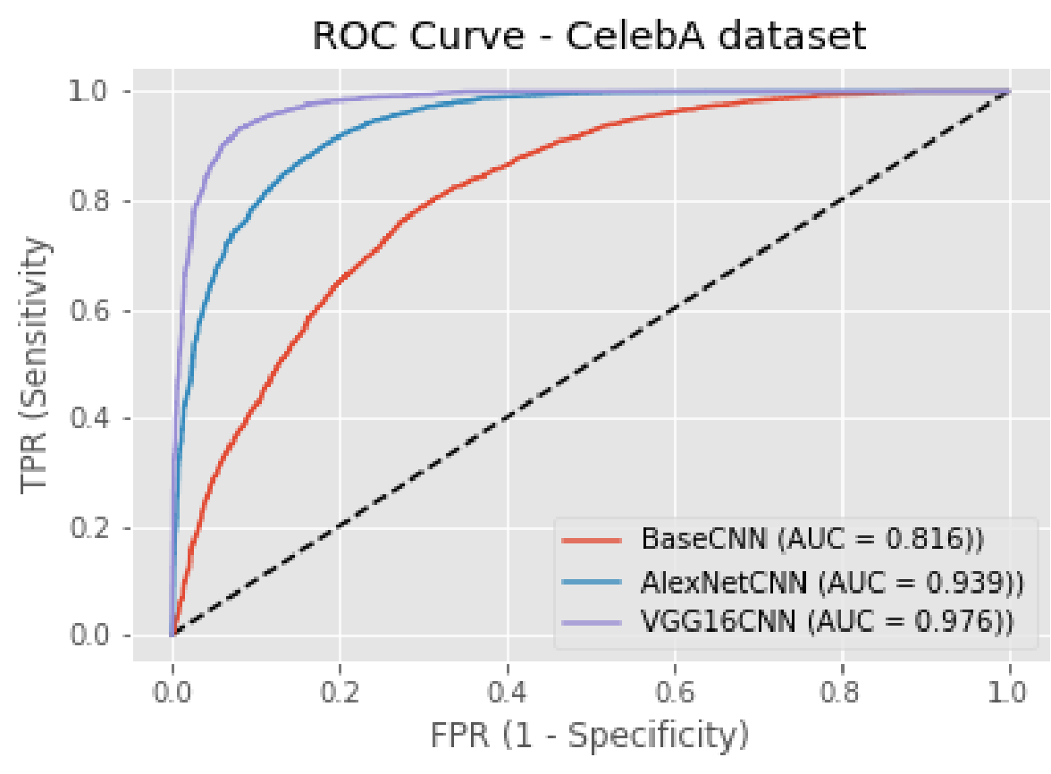


Figure 8: Performance Comparison using ROC for NUAA pipelines

Conclusion

- This study was able to train and compare three different CNN architectures. All the models proved to perform very well using the adopted datasets.
- The study is in progress, parameter study is being performed to the pipelines and results are yet to be available. Looking at the current result, an observation can be made that these pipelines are performing relativeIy well.
- Future Work: The study will architectures) and then add ensemble learning to the optimized pipelines to obtain the final model.

References

Boulkenafet Z Akhtar, Z Feng, X Hadid, A 2016 Face Anti spoofing in Biometric Systems In Biometric Security and Privacy s l Springer, Cham, pp299 321.

Daniel, N Anitha A 2018 A Study on Recent Trends in Face Spoofing Detection Techniques Coimbatore, India, s n.

Galbally J Marcel, S 2014 Face Anti spoofing Based on General Image Quality Assessment Stockholm, Sweden, IEEE.

Thepade S D et al 2020 The Comprehensive Review of Face Anti Spoofing Techniques International Journal of Advanced Science and Technology, 29 5 pp 8196 8205