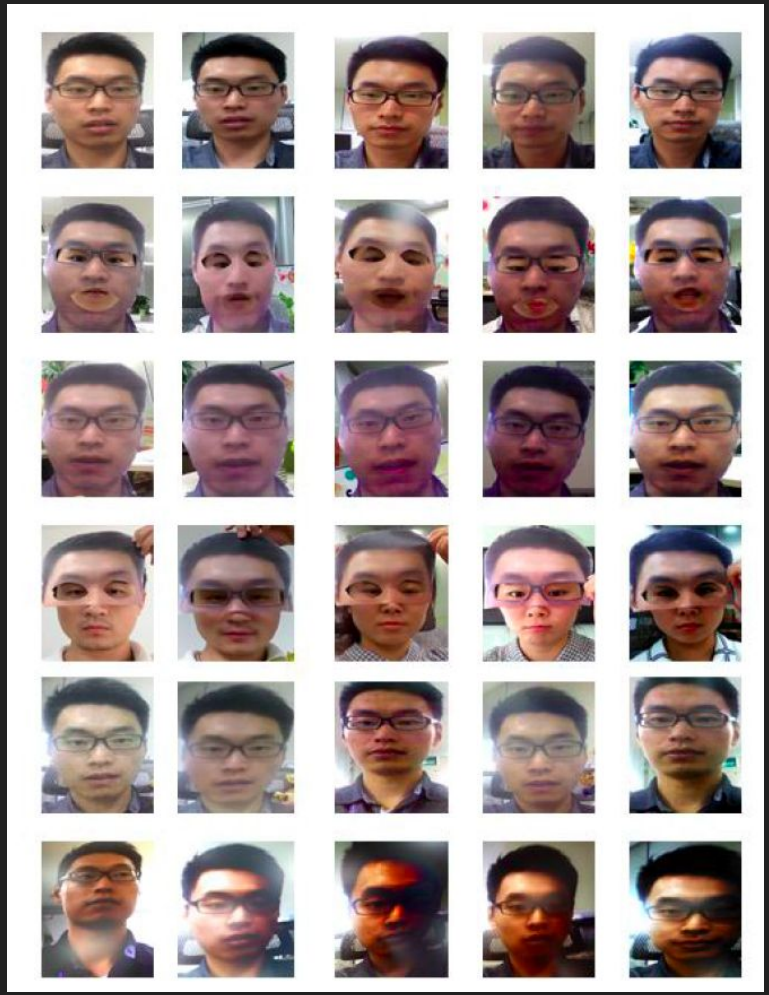
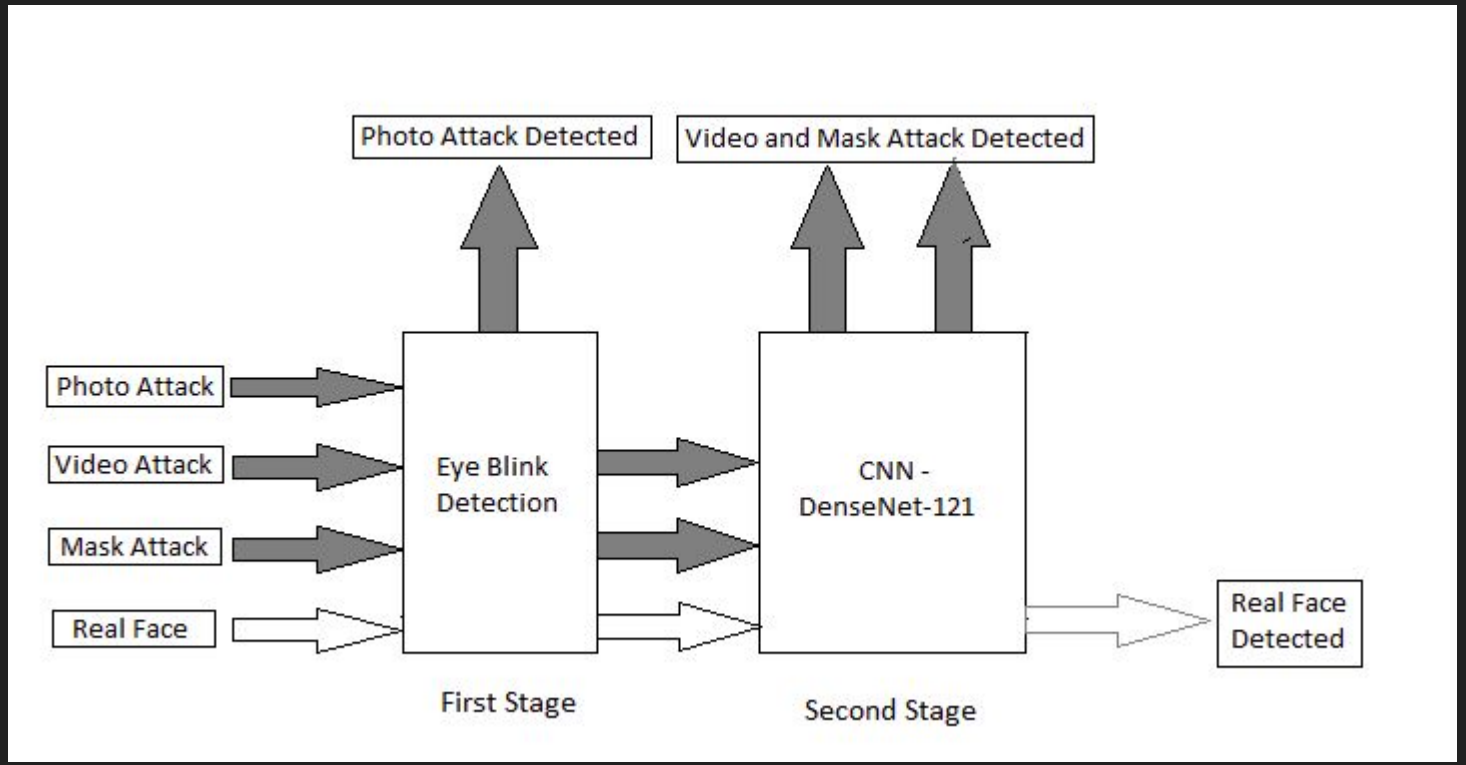
Proof of life detection

Problems

Security systems based on face recognition suffer spoofing attacks, due to the lack of an adequate proof of life detection algorithm. I tried a new method to avoid spoofing attacks with a two-stage approach, one based on movement and the other based on deep learning. The network is based on the ROSE-Youtu Face Liveness Detection Dataset. The entire model is tested in real-time videos on the webcam.

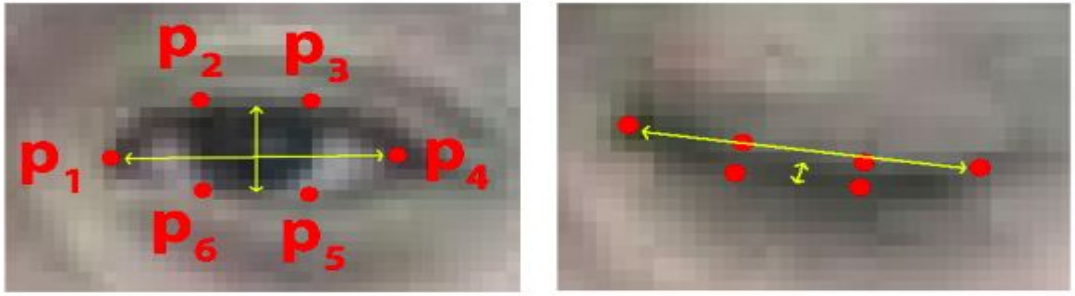


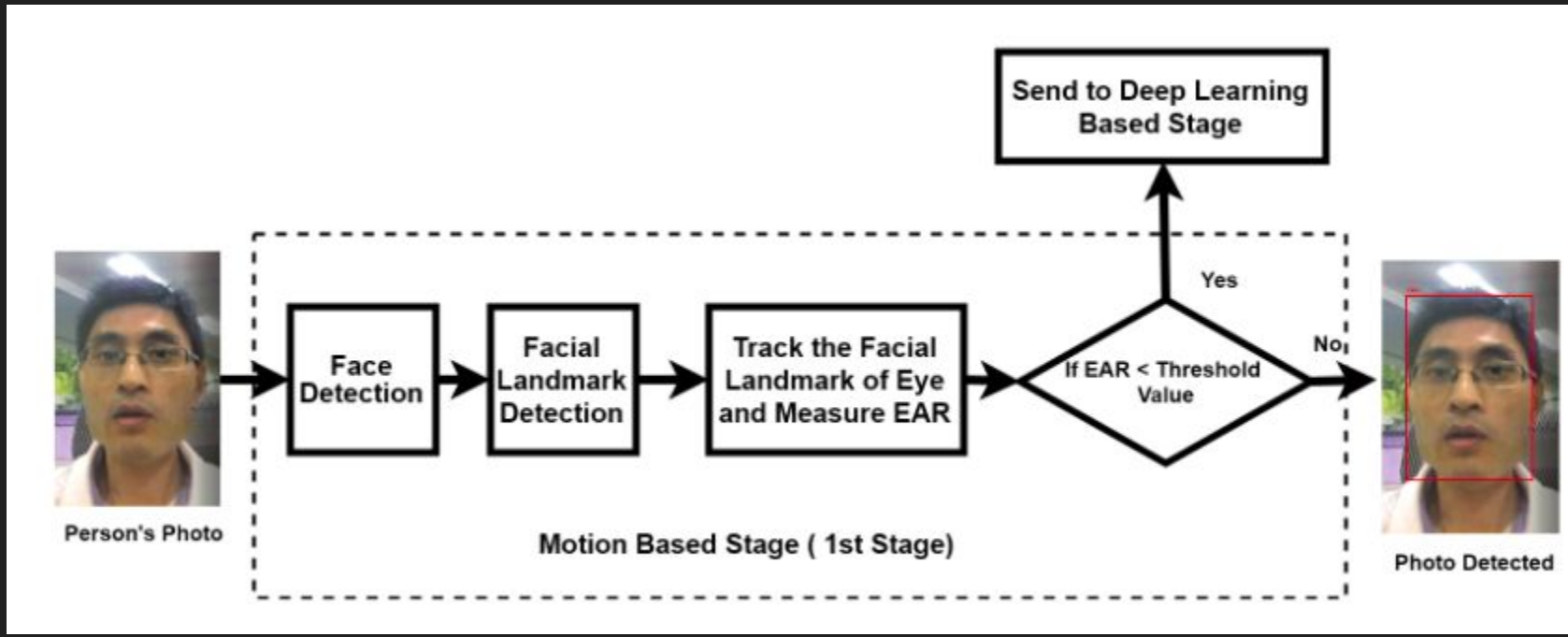
Methodology



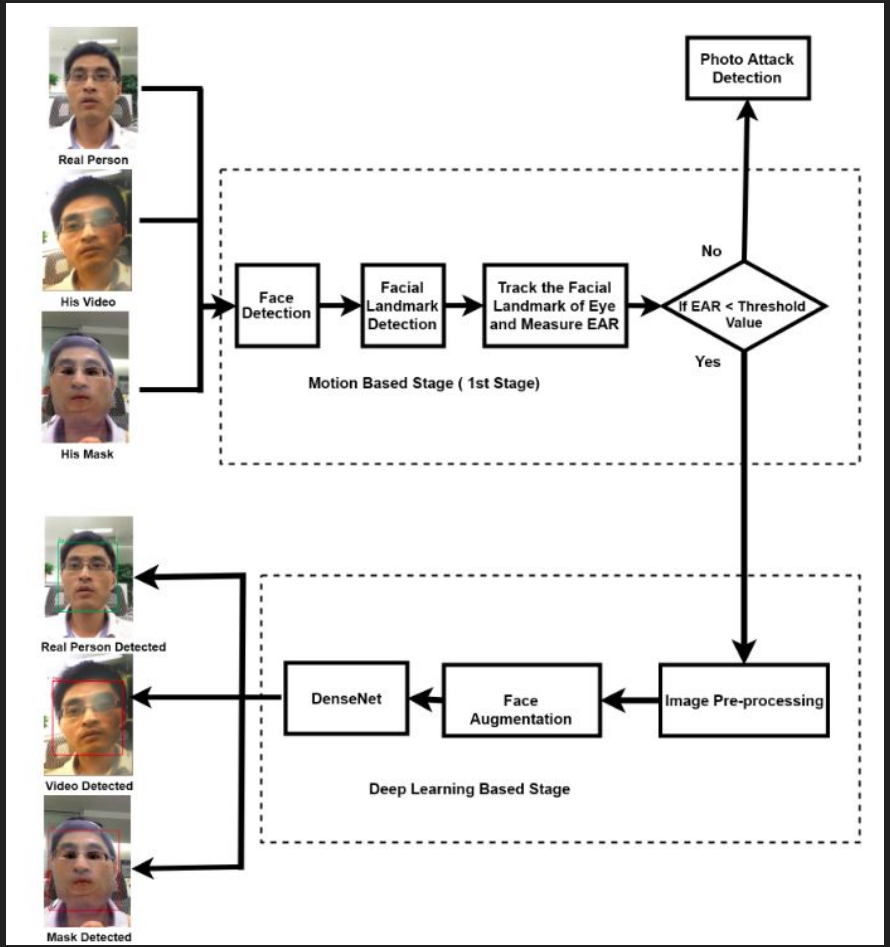
First step

$$EAR = \frac{||P2-P6|| - ||P3-P5||}{2||P1-P4||}$$



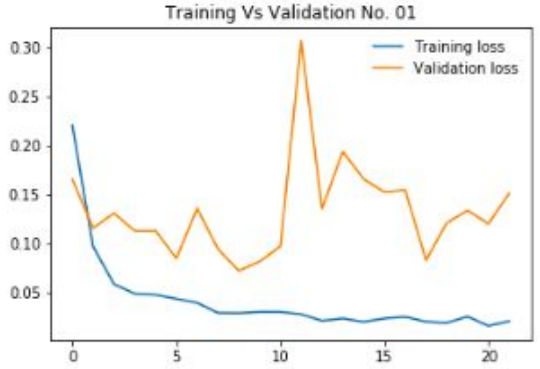

Send to Deep Learning Based Stage
Yes
No
Face Detection
Facial Landmark Detection
Track the Facial Landmark of Eye and Measure EAR
If EAR < Threshold Value
Person's Photo
Motion Based Stage (1st Stage)
Photo Detected

Second step


Real Person
His Video
His Mask
Photo Attack Detection
Face Detection
Facial Landmark Detection
Track the Facial Landmark of Eye and Measure EAR
If EAR < Threshold Value
No
Yes
Motion Based Stage (1st Stage)
Real Person Detected
Video Detected
Mask Detected
DenseNet
Face Augmentation
Image Pre-processing
Deep Learning Based Stage

Results

Firstly, the model is trained for 22 epochs at learning rate 0.001, the lowest validation loss was found 0.072107 and on that loss validation accuracy was 0.974649. This model was saved. After that the saved model was trained again for 20 epochs using learning rate 0.0001 and find the lowest validation loss was 0.059059 and on that loss validation accuracy was 0.978635. So we got 97.86% accuracy in validation dataset.



Train and validation loss at 1st training at learning rate 0.001

Train and validation loss at 2nd training at learning rate 0.0001