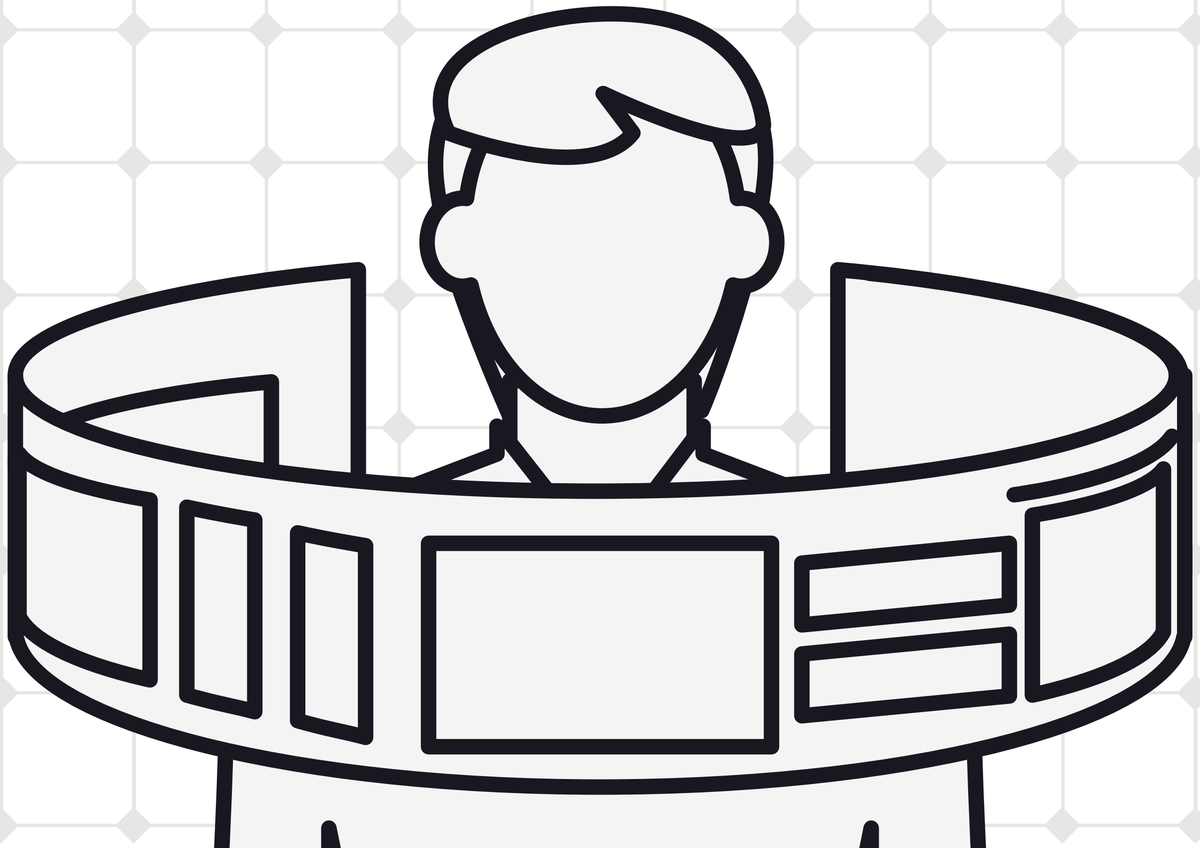
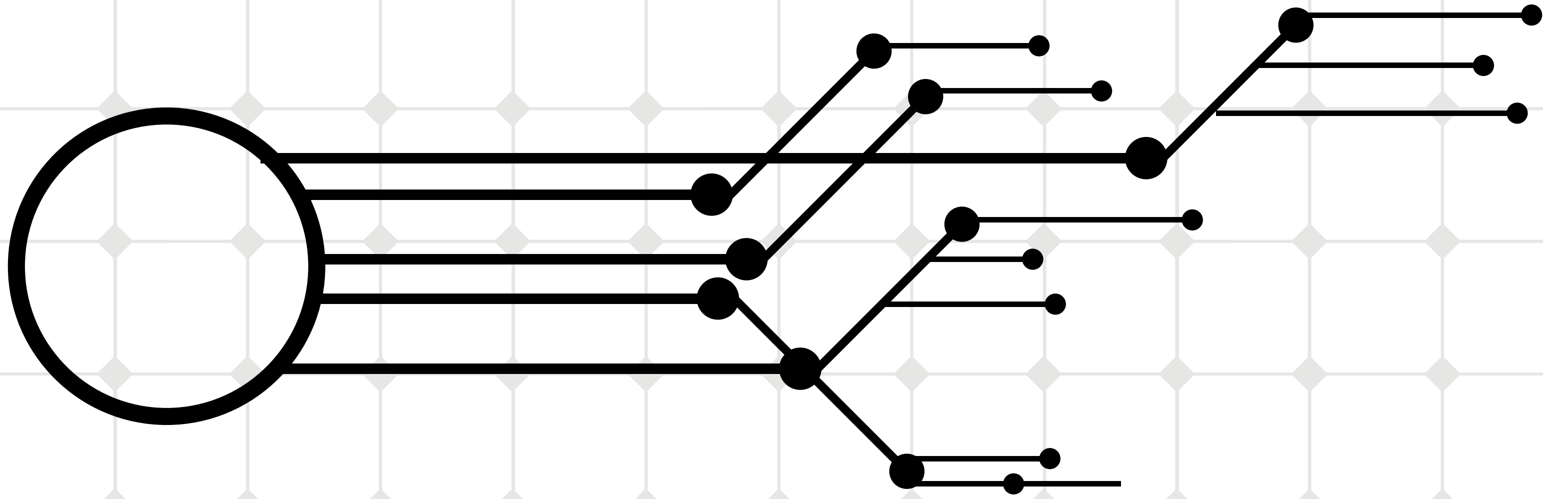
"FACE ANTI-SPOOFING"





OUR TEAM

BHIPANSHU DHUPAR

ASIJA PRAKASH

AYAN SHARMA

AYUSH PANDEY

ARYAK AGRAHARI

INTRODUCTION

- Face recognition is one of the most widely used biometric technologies for identity verification and authentication.
- Face recognition systems provide high accuracy, convenience, and user-friendliness for various applications, such as access control, surveillance, e-commerce, and social media.
- However, face recognition systems are also vulnerable to presentation attacks, which aim to deceive the system by using a fake face artifact, such as a photo, video, mask, or makeup.
- Presentation attacks pose a serious threat to the security and privacy of face recognition systems and their users.

PROBLEM STATEMENT

The problem at hand, therefore, centers on the need to develop and implement robust countermeasures and technologies to mitigate the vulnerabilities of face recognition systems to presentation attacks, thereby ensuring the continued security and privacy of these systems and enhancing their reliability in real-world applications.

PROPOSED METHOD

In our endeavor to conduct a thorough evaluation of face antispoofing models, we have designed a pragmatic solution. Our strategy involves training and assessing models using three well-established architectures: ResNet-121, and DenseNet-121, Densenet201 across a carefully selected set of three diverse datasets (NUAA, SiW, and Replay-Attack). This approach is aimed at providing a realistic and comprehensive understanding of how these models perform in a wide range of real-world scenarios of face
anti spoofing.

We would be evaluating it on the basis on model evaluation accuracy and will be working on it to get the better accuracy from already existing accuracy results on models like VGG16, Inception and Resnet18 .

DATASETS

NUAA DATASET

Comprises real-access and spoofing attack samples captured under different environmental conditions.

SIW (SPOOF IN THE WILD) DATASET

Images are collected from various sources, providing a wide range of potential spoofing methods and backgrounds.

REPLAY-ATTACK DATASET

The Replay-Attack dataset includes high-quality attack samples, such as printed photos and video replays.

MODELS

VGG16

In VGG16 there are 13 convolutional layers, 5 Max Pooling layers, and 3 Dense layers which sum up to 21 layers but it has only 16 weight layers i.e., learnable parameters layer.

RESNET 18

There is a total of eighteen layers in the network (17 convolutional layers, a fully-connected layer and an additional softmax layer to perform classification task)

INCEPTION

It is basically a convolutional neural network (CNN) which is 27 layers deep. When creating a subsequent layer in a deep learning model, one should pay attention to the learnings of the previous layer.

DENSENT201

DenseNet-201 is a deep convolutional neural network (CNN) architecture consisting of 201 convolutional layers, 3 max-pooling layers, normalization layers, fully connected layers, and softmax layer.

DENSENET121

DenseNet-121 is a deep convolutional neural network (CNN) architecture comprising 121 layers with densely connected blocks, transition layers, and a final fully connected layer for classification.

RESNET152

ResNet-121 is a deep convolutional neural network architecture with 121 layers, primarily composed of residual blocks that enable training very deep networks effectively.

RESULT

- Model Comparison:
  - We compared the performance of Densenet-121, Densenet-201 and Resnet-152
  - Each model was put to the test to see how well it detects fake faces.

Network	Accuracy	Flops	Parameters
DenseNet121	99.0212%	2895.99 M	6.96
DenseNet201	99.5106%	4389.4 5M	19.08
ResNet152	99.511%	11601.90 M	58.15

QUESTION

TIME

THANK, YOU