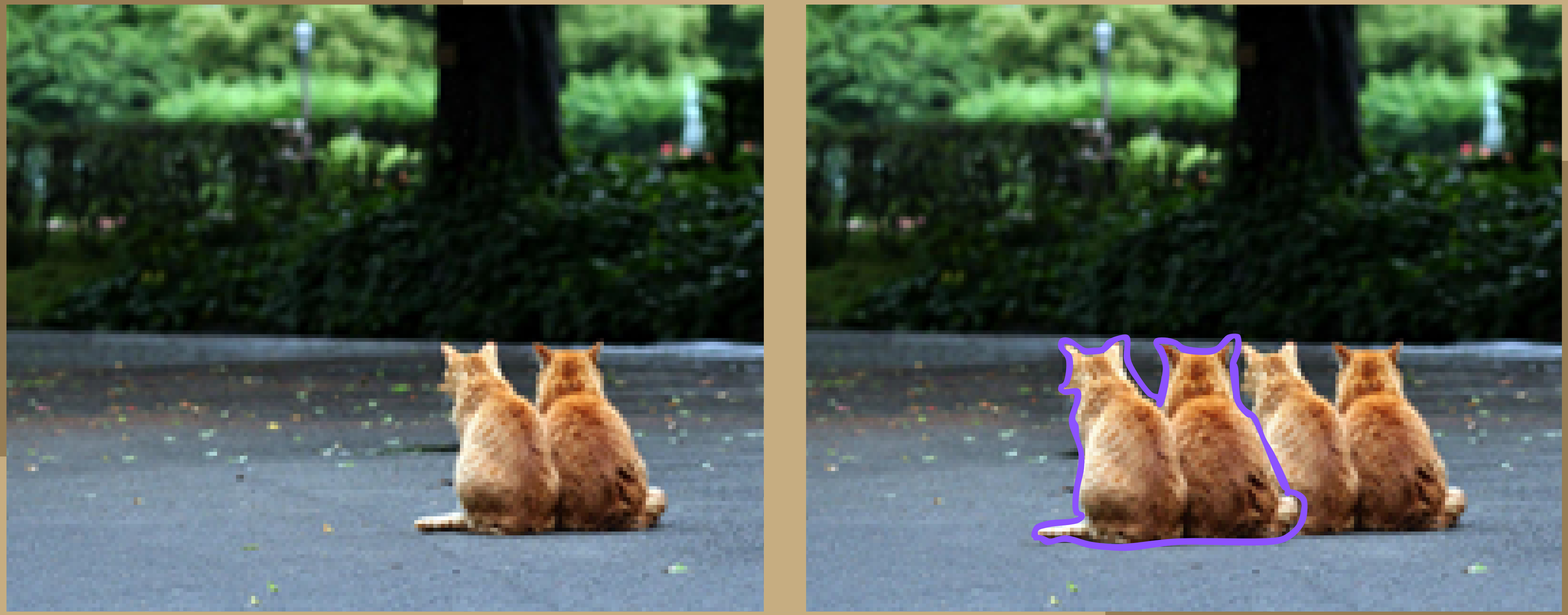
Image FORGERY DETECTION



Gowri Galgali
Lohith R Gowda
Soujanya Manasa
Sudhanva MS

Outline of the presentation

i) Problem Statement

ii) Introduction:
Importance of Image Forgery Detection

iii) Model (Method):
Overview of Deep Learning Architecture
Description of the current Deep Learning model.

iv) Dataset Details:
The Datasets used
Description of Dataset Characteristics

v) Experimental Results:
Comparative Classification report and
AOC curve

vi) Results Analysis:
Interpretation of Findings

vii) Conclusion:
Summary of Key Findings
Discussion of the Limitations

viii) Future Work:
Areas with Potential
Further Development

Problem Statement

Despite the advancements in imaging technology and the widespread use of digital images across various platforms, the increase of fake and altered images poses a significant challenge to the authenticity and reliability of visual content.

Therefore, the problem statement revolves around the need to enhance image forgery detection capabilities, particularly through the utilization of deep learning techniques, to safeguard the integrity and trustworthiness of digital images in the modern era.

Introduction


SPLICING

- *In the recent times, it has become incredibly easy to create fake images with powerful image manipulation software tools that are easily accessible.*
- *Various sophisticated forgery techniques such as Copy-move forgery, Splicing, Inpainting, and DeepFake are difficult to detect using traditional image forensics methods, necessitating the development of more robust and accurate techniques.*

Hence, our main objective of this project is to use deep-learning and classify the images as forged or authentic.

- *We have formed a comparison between two CNN models for the same task: ResNet50 and DenseNet121.*
- *For localizing the forged region in the images, we used a ResNet feature extractor and decoder network for image segmentation and masking the forged region.*

The tampered images that have been used to train our model have used only copy-move and splicing forgery techniques.

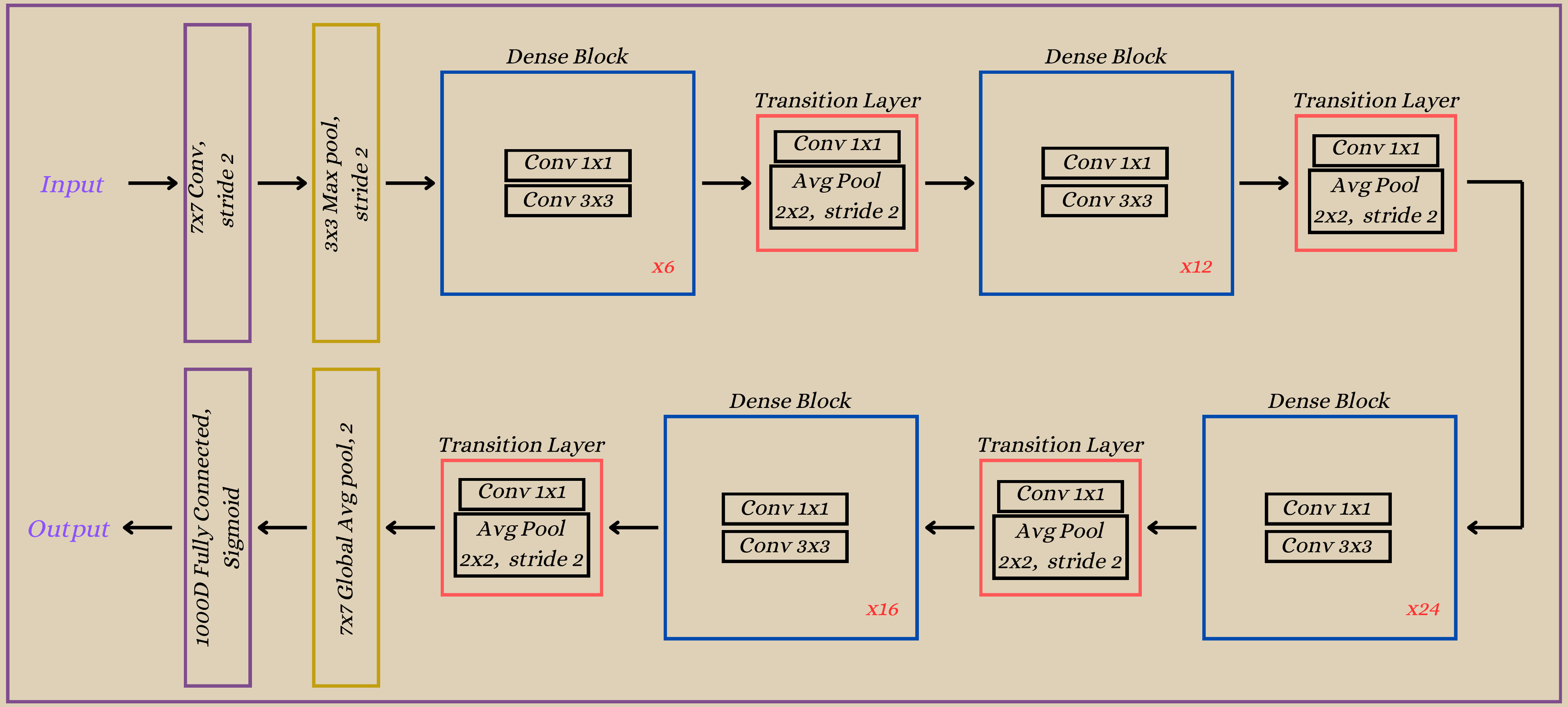

COPY-MOVE FORGERY


INPAINTING

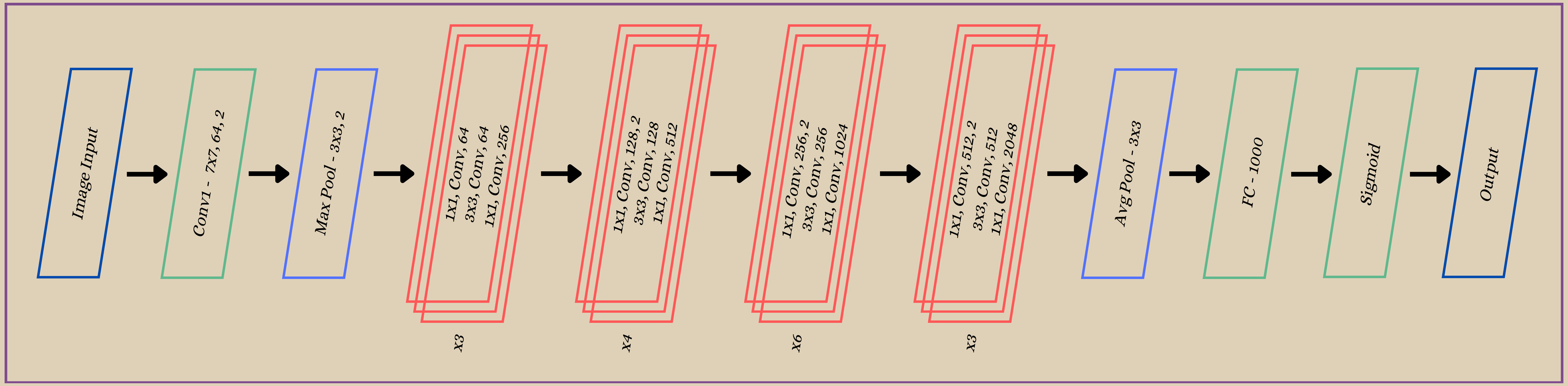

DEEPFAKE

Model

We conducted a comparative study between two pretrained models: ResNet50 and DenseNet121.



DenseNet121 Architecture



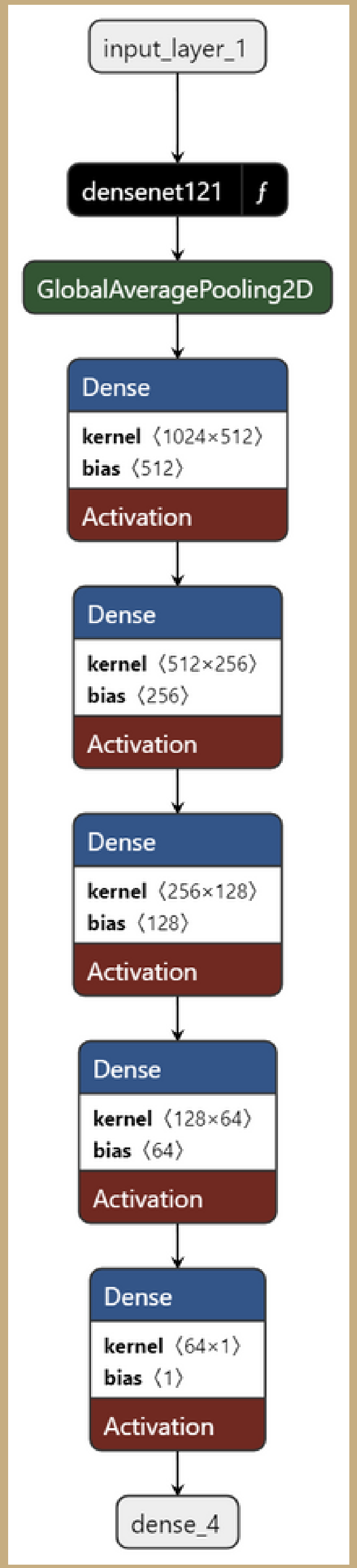
ResNet50 Architecture

Model

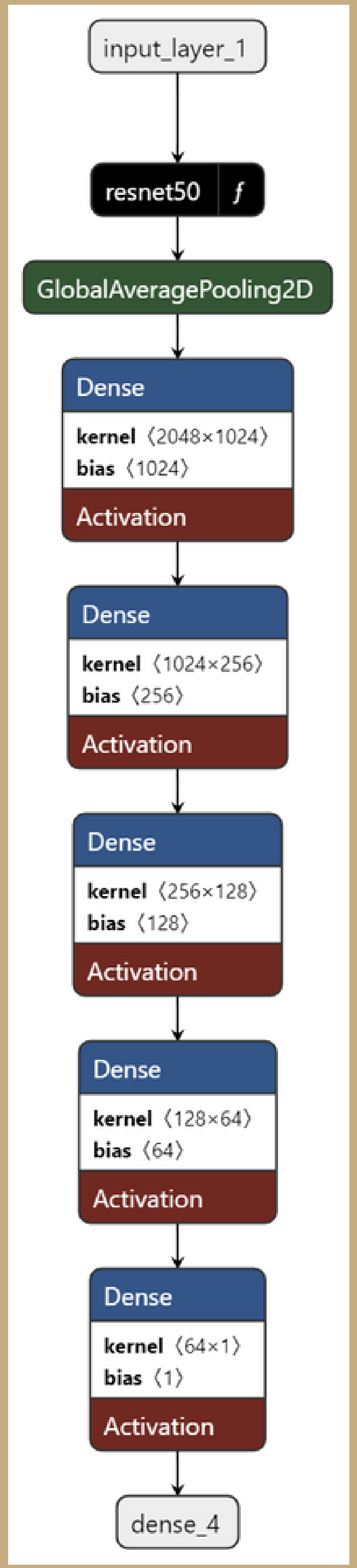
- *Total params: 77,862,277 (297.02 MB)*
- *Trainable params: 25,936,385 (98.94 MB)*
- *Non-trainable params: 53,120 (207.50 KB)*
- *Optimizer params: 51,872,772 (197.88 MB)*

In our ResNet50-based model, the architecture comprises:

- *a sequence of layers, including a ResNet50 base model,*
- *followed by dense layers for further feature extraction and classification.*



Using ResNet50



Using DenseNet121

- *Total params: 23,037,253 (87.88 MB)*
- *Trainable params: 7,651,201 (29.19 MB)*
- *Non-trainable params: 83,648 (326.75 KB)*
- *Optimizer params: 15,302,404 (58.37 MB)*

On the other hand, our DenseNet121-based model comprises:

- *the DenseNet121 architecture for feature extraction,*
- *followed by dense layers for classification, and also the reuse of features.*

*Both models undergo **transfer learning**, wherein pre-trained models (ResNet50 and DenseNet121) are utilized as feature extractors.*

Model

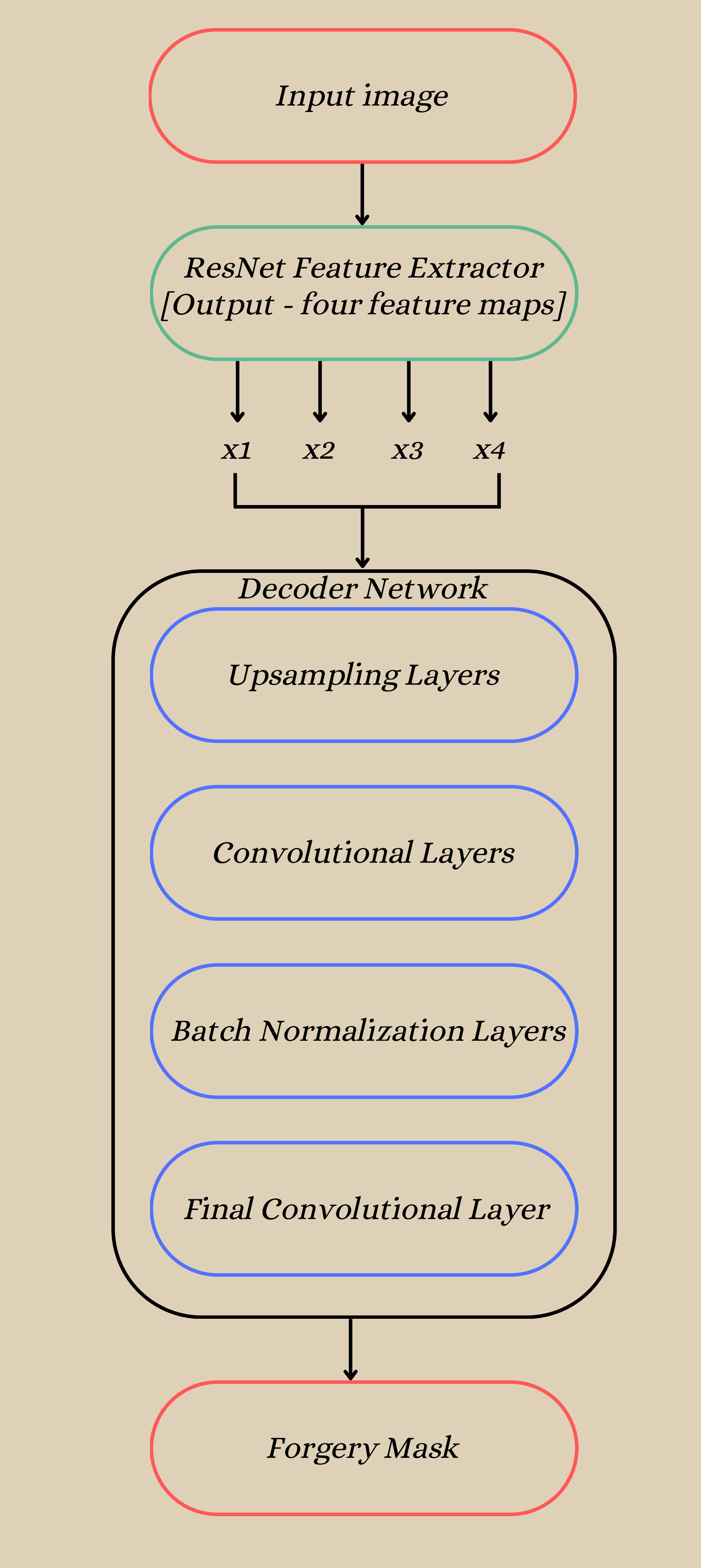
The model for Forgery Localization consists of ResNet Feature Extractor and Decoder Network.

- *ResNet Feature Extractor:*

This class defines a feature extraction network based on the ResNet50 architecture. It extracts features from input images and gives output of four feature maps, corresponding to different scales.

- *Decoder Network:*

This class defines a decoder network that takes the feature maps from the ResNet Feature Extractor. It consists of several upsampling layers followed by convolutional layers, which progressively refines the feature maps to generate the final forgery mask.



Dataset details

We have created a custom dataset from the following pre-existing datasets:

- *CASIA.v2*
- *Columbia uncompressed image splicing detection evaluation (CUISDE) dataset*
- *Image manipulation dataset*
- *COMOFO (**CO**py-**MO**ve **FO**rgery) dataset*

Dataset Characteristics:

- *The dimensions of images: 224 x 224*
- *Number of categories: 2*
  - *Authentic*
  - *Forged*
- *These are split into 70:30 for Train & Validation respectively*

DATASET	NUMBER OF AUTHENTIC IMAGES	NUMBER OF FORGED IMAGES
CASIA.V2	7492	5123
COLUMBIA UNCOMPRESSED IMAGE SPLICING DETECTION	183	180
IMAGE MANIPULATION DATASET	48	48
COMOFO DATASET	5003	5000
TOTAL	12726	10351

Experimental results

ResNet50:

F1 score: 83

Classification Report:

	precision	recall	f1-score	support
0	0.88	0.81	0.84	3809
1	0.79	0.86	0.83	3113
accuracy			0.84	6922
macro avg	0.83	0.84	0.83	6922
weighted avg	0.84	0.84	0.84	6922

Confusion Matrix:

```
[[3091  718]
 [ 422 2691]]
```

DenseNet121:

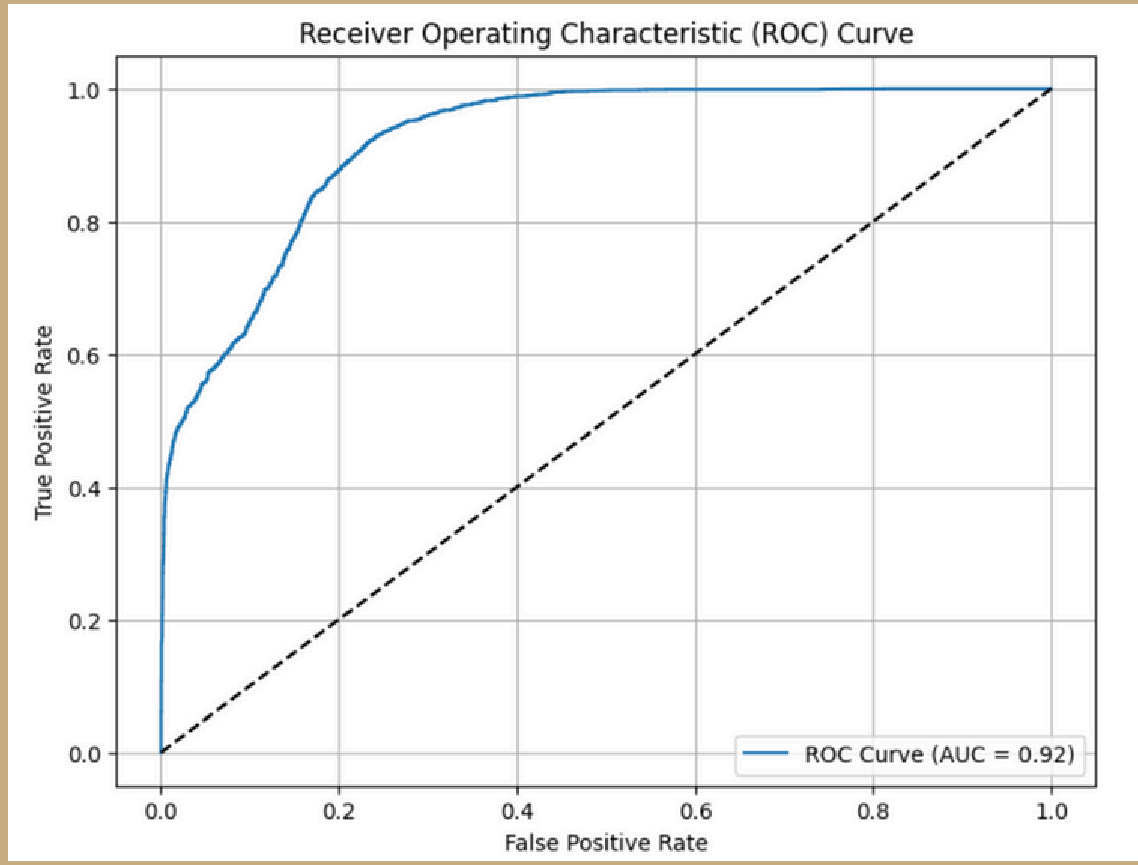
F1 score: 81

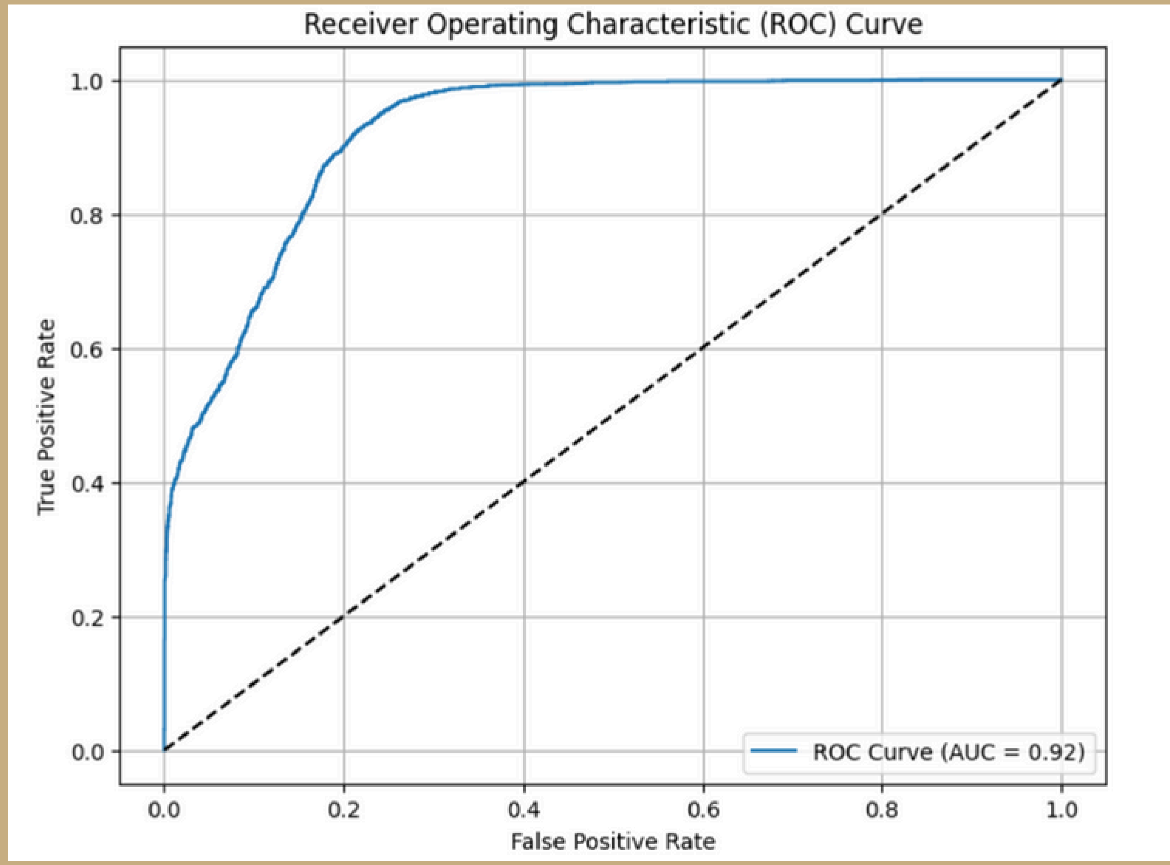
Classification Report:

	precision	recall	f1-score	support
0	0.85	0.84	0.84	3809
1	0.80	0.82	0.81	3113
accuracy			0.83	6922
macro avg	0.83	0.83	0.83	6922
weighted avg	0.83	0.83	0.83	6922

Confusion Matrix:

```
[[3186  623]
 [ 552 2561]]
```





Results Analysis

- As our dataset is slightly imbalanced, we are considering the F1 score as our result metric. Over the validation data, we can see that, ResNet50 has a better F1 score over DenseNet121.

- The ratio of the F1 score and total parameters:
    - For DenseNet-> 81 : 23,037,253
    - For ResNet-> 83 : 77,862,277

As we can see, ResNet has more parameters than DenseNet. Therefore, from the above ratios we can say that DenseNet has a better parameter ratio compared to ResNet.

Conclusion

- *This project shows the potential of convolution neural networks in the field of image forensics, image forgery detection in particular.*
- *Transfer learning and fine-tuning the models ensured that both the models achieved good results with F1 scores of 83% and 81% respectively, on a dataset that comprised images forged using various forgery methods.*
- *Based on our above comparison, we can infer that on valid data ResNet50 has a slight advantage with a better f1 score.*
- *Comparison based on parameters, f1 score ratio, we see that the DenseNet121 model shows a better ratio result.*
- *Localisation model still needs to be trained further to reach our desired goal.*

Conclusion

Limitations:

- *The dataset used for this project includes only splicing and copy move and hence would not give accurate results on other forgeries.*
- *Localization model, which uses RestNet as an extractor and a decoder block, didn't put out the best mask result.*
- *The code could be further enhanced for better performance.*
- *The models have not been tested with real data.*

Future Scope

- *Further fine-tuning of the models can be done, by exploring different loss functions, freezing and unfreezing the layers can give a much better result.*
- *In the case of localization, the extractor and decoder can further be more diligently trained over a larger dataset of ground truths for better results of the masks.*