Indian Institute of Information Technology Kota

Major Project Presentation

Image Forgery Detection

Team Members:

Rikith Devangam	**(2021KUCP1138)**
Mourya Arnepalli	**(2021KUCP1097)**
Sanjay Bhargav Dukka	**(2021KUCP1076)**
Boreddy Muktheswar Reddy	**(2021KUCP1081)**

Project Supervisor:
Dr. Ajay Nehra
Assistant Professor
Department of CSE
IIIT Kota

Overview

- Introduction
- Motivation
- Problem Statement
- Literature Review
- Methodology
- Flow chart
- System Design
- Findings
- Evolution Matrix
- Comparison
- Result
- Flow chart
- Conclusion
- References
- Acknowledgement

Introduction:

- In the digital era, image manipulation has become widespread, raising concerns about the authenticity and credibility of visual content. Detecting forged images manually is challenging and time-consuming, necessitating automated solutions.

- Machine learning offers a promising approach to address this challenge by developing robust forgery detection systems. By leveraging machine learning techniques, researchers and practitioners can automatically identify manipulated regions within digital images and distinguish between authentic and forged content.

- This project aims to contribute to the advancement of digital forensics and integrity verification. By developing and deploying a robust forgery detection system, the goal is to enhance trust in digital media and combat the spread of misinformation.

Motivation

In the digital age, images play a critical role in communication, journalism, social media, and legal evidence. With the advent of powerful image editing software, manipulating images has become relatively easy, which can lead to misinformation, fraud, and other malicious activities. This raises significant concerns about the authenticity of digital images. Therefore, developing robust methods for image forgery detection has become crucial. Our approach leverages Convolutional Neural Networks (CNN) and Error Level Analysis (ELA) to enhance the reliability and accuracy of forgery detection.

- Manual detection is inefficient and impractical for large-scale use. Automated methods, particularly using CNNs, can provide faster and more accurate results.
- Traditional heuristic-based methods may fail against advanced forgeries. CNNs can learn complex patterns and adapt to new forgery techniques.
- By combining CNN and ELA, we aim to create a robust, automated solution to detect image forgeries effectively, addressing the growing challenge of digital image manipulation.

Problem Statement:

- The widespread availability of digital image manipulation tools has led to a surge in image forgeries, undermining the integrity of visual content. Manual detection of these forgeries is impractical given the volume of digital images produced daily. Consequently, there is an urgent need for automated solutions capable of accurately identifying manipulated regions within images and discerning between authentic and forged content. This project addresses this need by leveraging machine learning techniques to develop a robust forgery detection system, thereby preserving the credibility of digital imagery.

Literature Review:

Research Paper	Key Findings
Patekar, Sankalp & Khan, Sumaiya & Bhusare, Diksha & Bhujbal, Manish & Hegde, Gayatri. (2023). IMAGE FORGERY DETECTION. 10.13140/RG.2.2.32571.59680.	ELA implementations in conjunction to Grayscale conversion to reduce data complexity for analysis
Abbas, Muhammad Naveed & Ansari, Samar & Asghar, Mamoona & Kanwal, Nadia & O'Neill, Terry & Lee, Brian. (2021). Lightweight Deep Learning Model for Detection of Copy-Move Image Forgery with Post-Processed Attacks. 000125-000130. 10.1109/SAMI50585.2021.9378690.	VGGNet & MobileNetV2 methods for increasing efficiency of the overall model

Methodology

- **CNN** : Convolutional Neural Networks (CNNs) are a class of deep neural networks primarily used in the field of computer vision for tasks such as image classification, object detection, segmentation, and more.

- **Smaller Visual Geometry Group Net (SVGGNet):** SVGGNet is a custom-built CNN framework inspired by the VGGNet architecture but optimized for efficiency and resource constraints. It features three convolutional layers with 32, 64, and 128 filters respectively.The model is equipped with a SoftMax classifier for two classes (Authentic and Forged).SVGGNet has a disk size of 51 MB with **4,475,458 trainable parameters and 1,856 non-trainable parameters.**

- **MobileNet Version 2 (MobileNetV2):** MobileNetV2 is a lightweight CNN framework originally designed for resource-constrained devices. It utilizes depth-wise separable convolutions for efficiency. The modified model can handle input images of size 224×224×3 and has a disk size of 11 MB with **164,226 trainable parameters and 2,257,984 non-trainable parameters.**

Methodology

The Error Level Analysis (ELA) method is one way to identify the areas of the image that have been modified. It works by creating a difference map of the image by compressing and decompressing it with a low-quality JPEG algorithm. The parts of the image that have been modified will have a different compression rate and will appear as bright spots in the difference map.

Grayscale conversion is often used to simplify the image and reduce its complexity. It involves converting the image into a black-and-white or gray-scale image, where each pixel's value represents its intensity.

Thresholding is a technique used to convert the grayscale image into a binary image, where each pixel is either black or white. This process helps eliminate noise in the image and can improve the accuracy of the detection algorithm.

Methodology

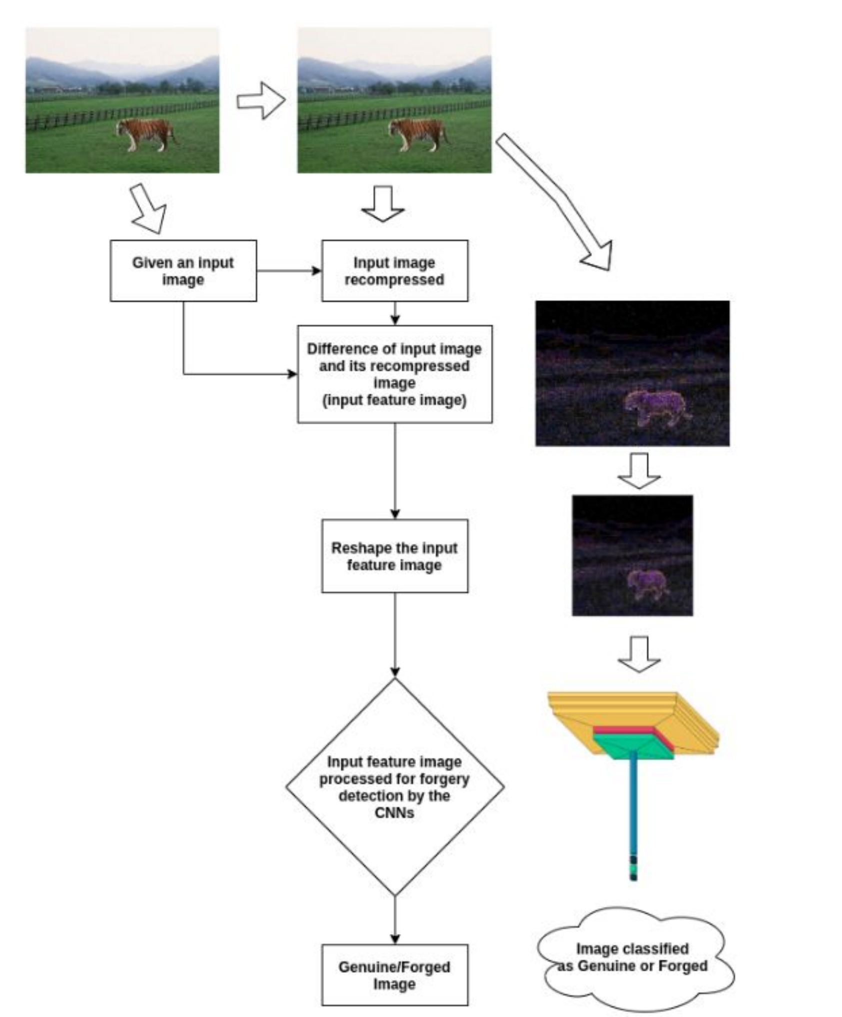
Data Collection: CoMoFoD [16]; a database consisting of copy-move forged images post-processed with visual-appearance related attacks (brightness change, blurring and noise adding), (2) MICC-F2000 [17]; a database consisting of copy-move forged images with attacks related to geometric manipulations including scaling (symmetric/asymmetric), rotation, translation or all combined, and (3) CASIA ITDE 2.0 [18]; a database utilized for original (Authentic class) images only

Preprocessing:Resizing, normalization, reducing noise.

Feature Extraction:Hand contours, key points, motion trajectories.

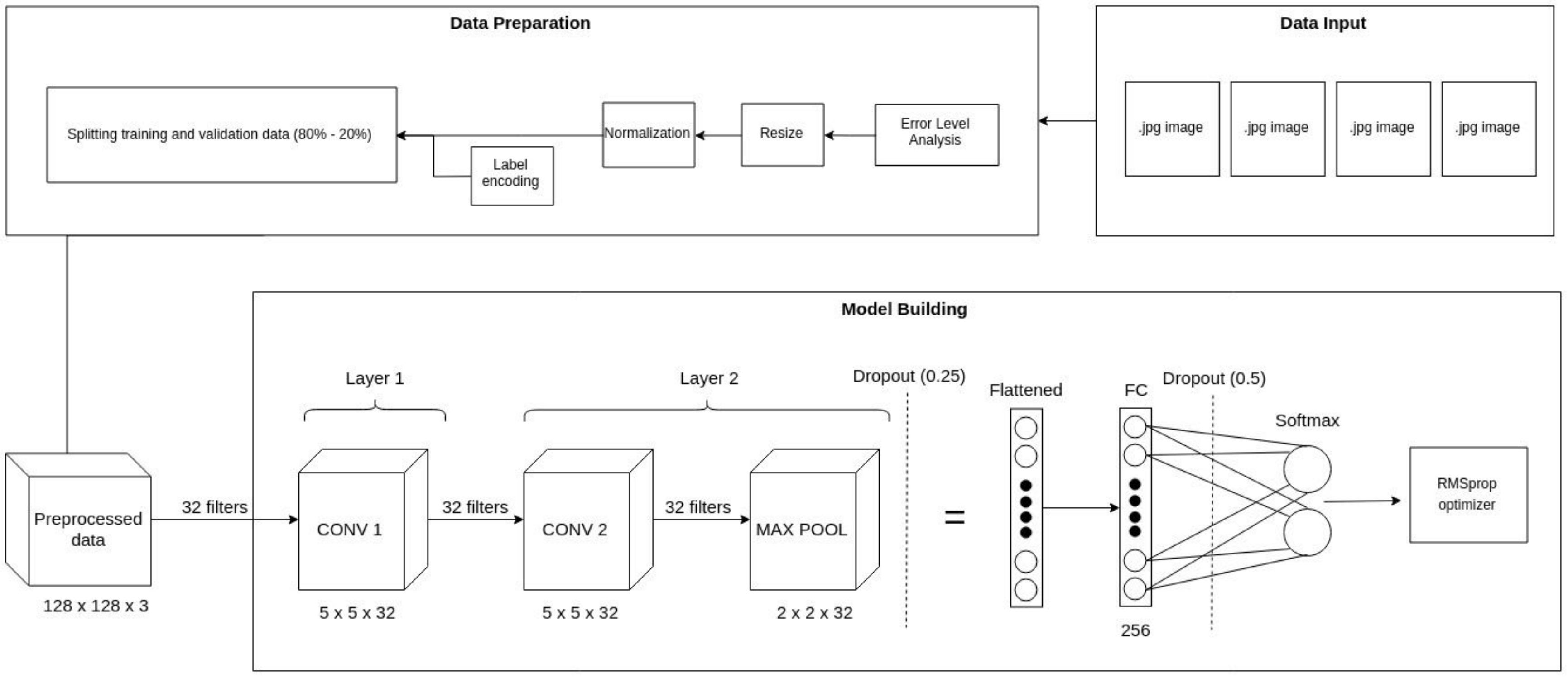
Machine Learning Model: Design, training, CNN , evaluation metrics.

Flow chart



Given an input image
Input image recompressed
Difference of input image and its recompressed image (input feature image)
Reshape the input feature image
Input feature image processed for forgery detection by the CNNs
Genuine/Forged Image
Image classified as Genuine or Forged

System Design



Findings

- **High Accuracy:** Convolutional Neural Networks (CNNs) demonstrated high accuracy in identifying forgeries by learning complex patterns and features that differentiate real images from manipulated ones.

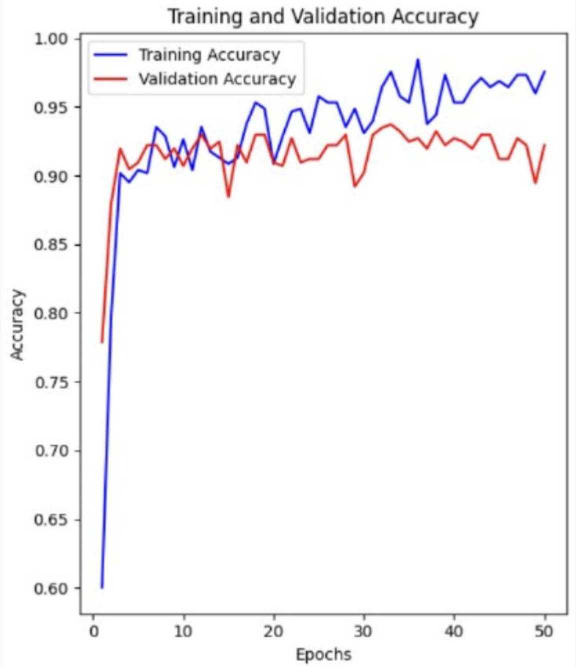
- **Effective Identification:** The combination of CNN and ELA is particularly effective in detecting copy-move forgeries, where parts of the image are copied and pasted within the same image.

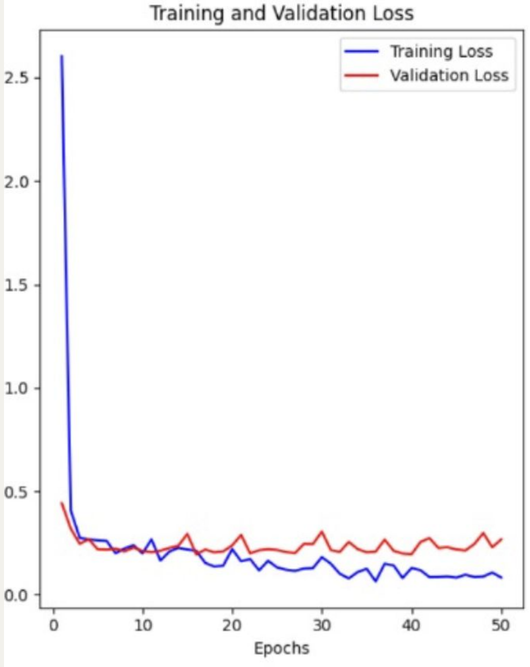
- **Enhanced Detection with ELA:** ELA helps in identifying compression artifacts and inconsistencies that often occur in manipulated images, providing an additional layer of scrutiny.

- **Improved Detection Rates:** Combining ELA with CNNs enhances the detection rates by providing additional features that are indicative of forgery.

Evolution Matrix

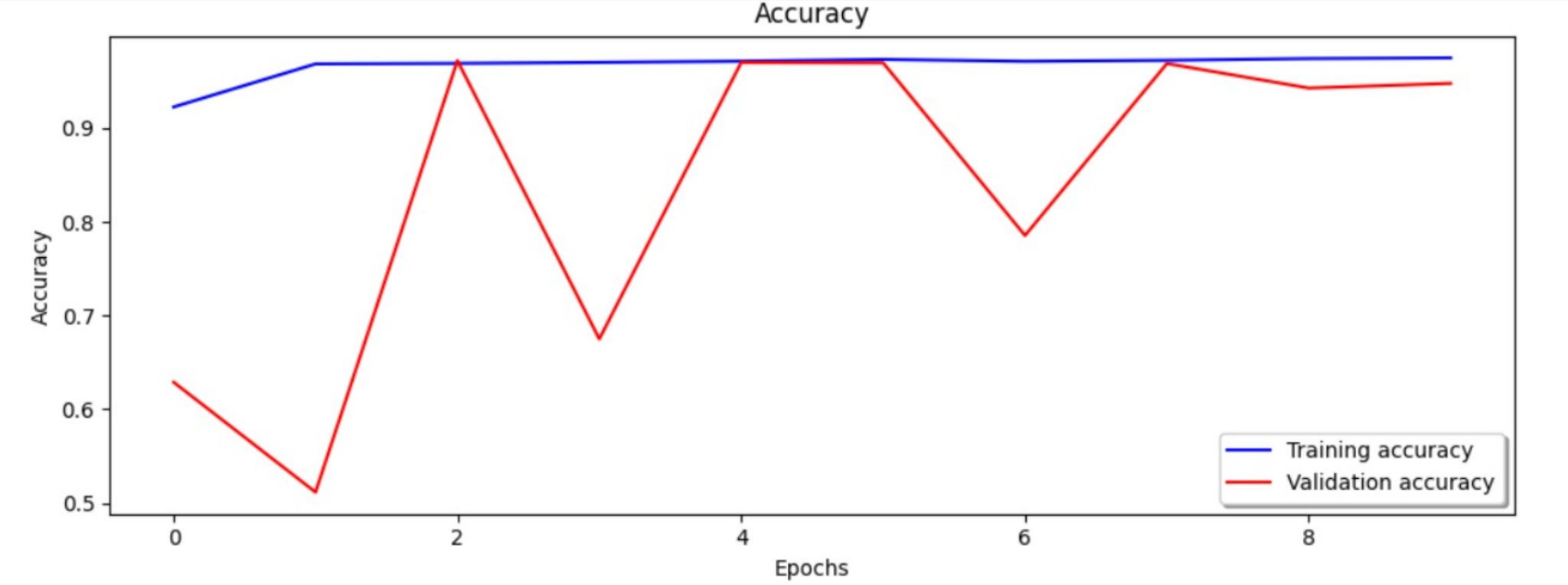
Accuracy and loss of the model one





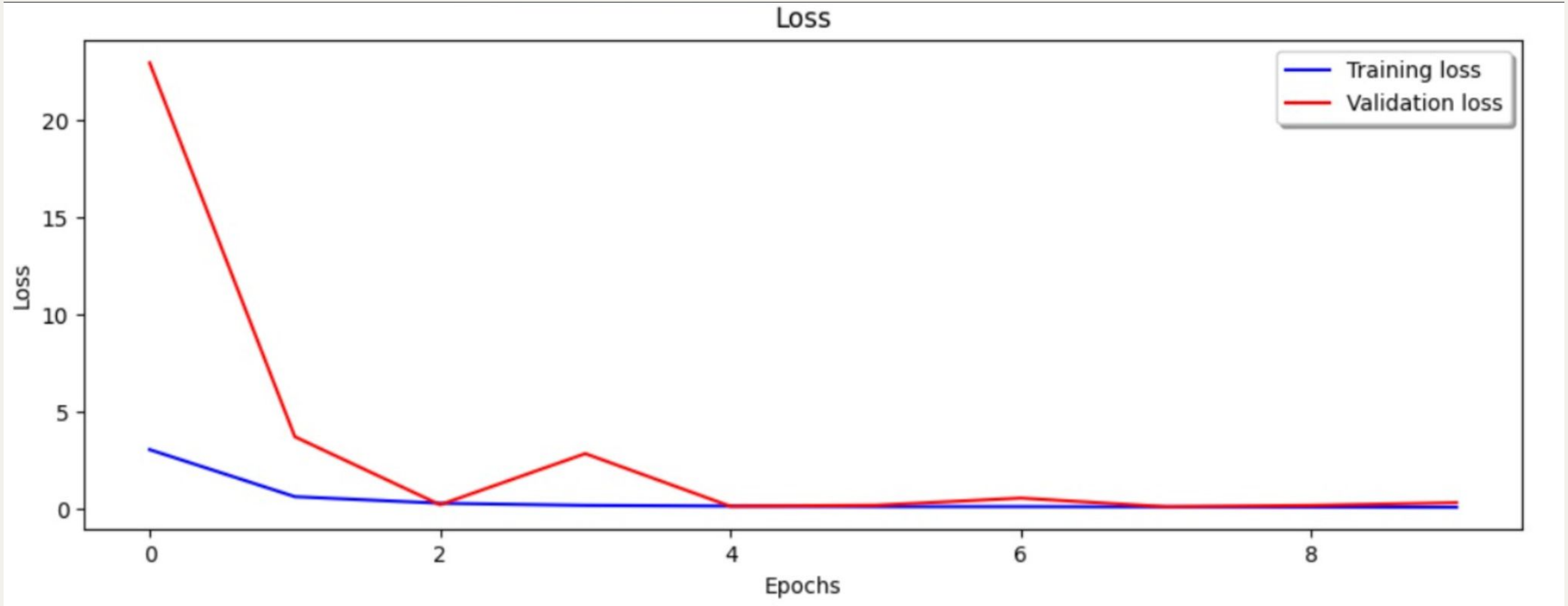
Evolution Matrix

Accuracy of the model two



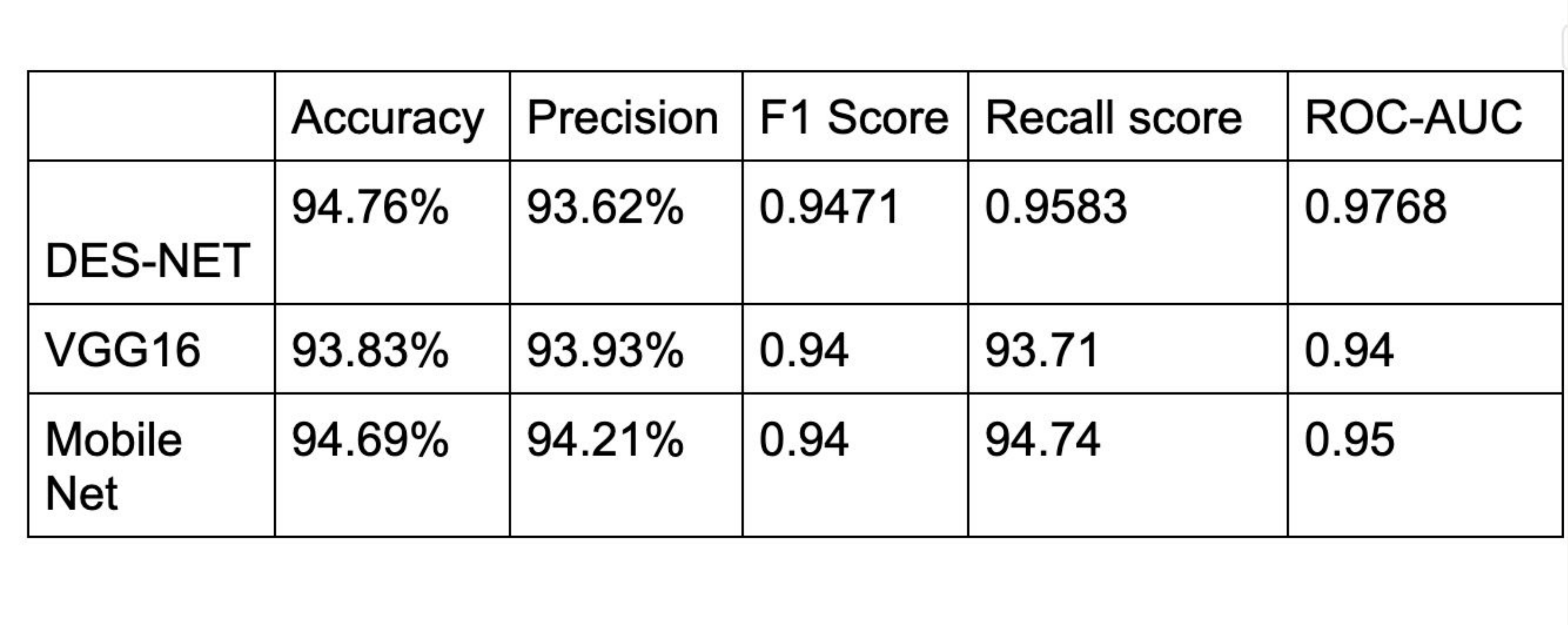
Evolution Matrix

loss of the model two



Comparison

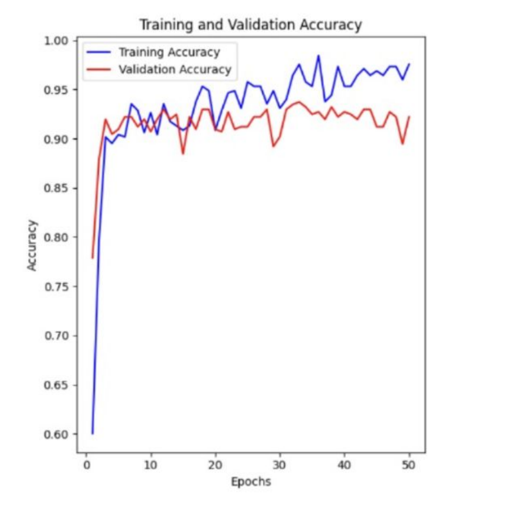
For the comparison of the models here is the proper table explaining all



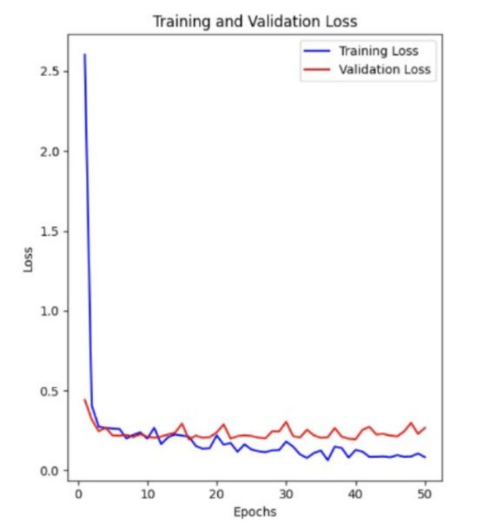
	Accuracy	Precision	F1 Score	Recall score	ROC-AUC
DES-NET	94.76%	93.62%	0.9471	0.9583	0.9768
VGG16	93.83%	93.93%	0.94	93.71	0.94
Mobile Net	94.69%	94.21%	0.94	94.74	0.95

Result

The proposed approach successfully determined the ELA between the original and scaled images. The features retrieved from the ELA were used to train the CNN model, which also produced results with great accuracy. The model's effectiveness is assessed based on its precision, recall, and accuracy.



Graph for training and validation accuracy



Graph for training and validation loss

Conclusion:

- In conclusion, our research highlights the effectiveness of machine learning in detecting image forgeries. Models like SVGGNet and MobileNetV2 show promise in identifying manipulated regions and distinguishing authentic content. Integrating these models into real-world applications can bolster trust in digital media and combat misinformation. Our future focus on detecting deepfake images underscores our commitment to ensuring digital content integrity. Through ongoing research, we aim to strengthen forgery detection systems for a more reliable digital ecosystem.

References:

1. Patekar, Sankalp & Khan, Sumaiya & Bhusare, Diksha & Bhujbal, Manish & Hegde, Gayatri. (2023). IMAGE FORGERY DETECTION. 10.13140/RG.2.2.32571.59680.

2. Abbas, Muhammad Naveed & Ansari, Samar & Asghar, Mamoona & Kanwal, Nadia & O'Neill, Terry & Lee, Brian. (2021). Lightweight Deep Learning Model for Detection of Copy-Move Image Forgery with Post-Processed Attacks. 000125-000130. 10.1109/SAMI50585.2021.9378690.

3. J.Malathi, B.Narasimha Swamy, Ramgopal Musunuri, "Image Forgery Detection by using Machine Learning, International Journal of Innovative Technology and Exploring Engine-ering (IJITEE)ISSN: 2278-3075, Volume-8, Issue- 6S4, April 2019.

Acknowledgement:

We would like to thank Dr. Ajay Nehra for giving us this wonderful opportunity to work on this amazing project. We would also like to thank them for their constant guidance, availability and eagerness to solve any problem that we encountered.We would also like to thank the faculty members present here for taking out time from their schedules to check on the progress of our project and sit through our presentation.

Thank You