VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

CSI3006 - SOFT COMPUTING TECHNIQUES

PROJECT REPORT

TEAM

Praven Kumar C V - 21MIC0070
Rohith V - 21MIC0073
Shanmukha Ganesh – 21MID0063

Image Manipulation Detection

Praveen Kumar C V
Rohith V
Shanmukha Ganesh S

Abstract –

Digital imagery is critical in various fields, but the rise of sophisticated editing software has increased the risk of digital image forgery, which manipulates images to obscure. mislead This practice challenges the integrity of visual data and impacts domains like entertainment, journalism, law enforcement, and scientific research. Manipulated images, often undetectable to the naked eye, contribute to misinformation and raise concerns about the credibility of visual evidence. Common forgery techniques include splicing, cloning, retouching, and morphing. The consequences are far-reaching, affecting news media, social media, legal systems, and national security.

This paper discusses methods to detect forgery, such as error-level analysis, noise inconsistencies, and machine learning. Addressing these challenges requires robust verification tools to ensure visual data's authenticity and protect against the risks of manipulated imagery.

Keywords --

Digital Image Forgery, Image Tampering Detection, Convolutional Neural Networks (CNNs), Error Level Analysis (ELA), Deep Learning, Metadata Analysis, Image Processing, Morphed Image Detection, Image Forensics, Compression Artifacts, Frequency Domain Analysis, Noise Analysis, Geometry-Based Detection, Transfer Learning, Pattern Recognition, Image Manipulation Techniques.

I. INTRODUCTION

A digital image is a visual representation captured and stored in a digital format, typically encoded as binary data that outlines a two-dimensional array of pixels. This representation allows for the manipulation, analysis, and transmission of images through electronic means. The field of image processing encompasses the various techniques used to process, analyze, and transform digital images to achieve specific outcomes, whether it's enhancing visual quality, extracting meaningful information, or compressing data for efficient storage and transmission.

Image processing is central to numerous applications, from medical imaging and remote sensing to facial recognition and video editing. It involves operations like image zooming, segmentation, enhancement, and compression. These processes are crucial for tasks such as feature extraction, pattern recognition, and machine learning applications. By converting traditional images into digital form, image processing enables a vast range of technological innovations and breakthroughs.

II. LITERATURE REVIEW

A. Image forgery detection using Deep Neural Network

Author: Anushka Singh and Jyotsna Singh

Methodology: Employs Error Level Analysis (ELA) to identify image tampering by scrutinizing variations in compression levels. This technique is designed to detect discrepancies in image quality that might indicate forgery.

Deep Learning Techniques: Utilizes Convolutional Neural Networks (CNNs) with standard layers like input, convolution, pooling, and fully connected for feature extraction and classification. The authors explore various pre-processing methods and experiment with transfer learning to enhance forgery detection.

Key Findings: Their approach to forgery detection incorporates deep neural networks, integrating pre-processing, CNN, and transfer learning. They provide insights into these techniques' effectiveness in detecting tampering and outline their experimental setup.

Limitations: The study lacks a detailed analysis of specific transfer learning models and how these models affect forgery detection. Additionally, the research primarily focuses on accuracy, potentially overlooking other crucial evaluation metrics such as precision, recall, and F1-score. This focus on accuracy might limit the overall understanding of the detection system's robustness.

B. Morphed Image Detection Using ELA and CNN Techniques

Authors: Dr. Jayasri Kotti, Dr. E. Gouthami, Dr. K. Swapna, Suneetha Vesalapu

Methodology: This study presents a hybrid approach for detecting morphed images, integrating Error Level Analysis (ELA) with Convolutional Neural Networks (CNN). ELA is employed to identify compression inconsistencies, suggesting tampering, while CNN is used to perform deep learning-based feature extraction and classification. The combination of these techniques aims to improve the accuracy of image authenticity verification.

Key Findings: The proposed method demonstrates robust detection capabilities for morphed and fake images. By leveraging the deep learning capabilities of CNN and the analytical power of ELA, the approach yields accurate results in identifying manipulated images. This methodology's strength lies in its ability to efficiently extract features indicative of forgery and accurately classify images based on these features.

Advantages:

Robust detection of morphed and fake images.

Enhanced accuracy through the combination of ELA and CNN.

Efficient application of deep learning techniques for image forensics.

Limitations:

Requires a large dataset for training the CNN, adding to the time and resource demands.

Implementing ELA and CNN techniques together is complex and may require advanced technical expertise.

Accurate interpretation of results demands a high level of expertise in image forensics.

C. Image Forgery Detection Using Error Level Analysis and Deep Learning

Authors: Ida Bagus Kresna Sudiatmika, Fathur Rahman, Trisno, Suyoto

Methodology: The researchers utilized a Convolutional Neural Network (CNN) based on the VGG16 architecture to detect image forgeries. Given the limited size of available datasets, the VGG16 model, known for its robust pattern recognition capabilities, was selected. The CNN structure comprised convolutional, pooling, and fully connected layers to classify images. Error Level Analysis (ELA) was integrated into the methodology to examine variations in compression artifacts, while metadata analysis was used to identify image authenticity indicators, such as Photoshop tags.

Key Findings: The proposed methodology achieved high accuracy rates—92.2% during training and 88.46% in validation—even with a limited dataset. The combination of ELA and CNN allowed for effective detection of image forgeries, demonstrating the robustness of the VGG16 architecture in recognizing patterns and detecting manipulated images. Metadata analysis provided additional insights into image authenticity, complementing the deep learning approach.

Advantages:

Achieved high accuracy rates with a limited dataset, showcasing the efficiency of the VGG16-based CNN.

Effective integration of Error Level Analysis and metadata analysis with CNN for forgery detection.

The methodology's ability to adapt to smaller datasets demonstrates its potential for broader applications in image forgery detection.

Limitations:

The small dataset size may impact the optimal performance of the Convolutional Neural Network, potentially limiting its generalization capabilities.

Error Level Analysis and metadata analysis are not foolproof methods, as metadata can be easily modified, and ELA has limitations in detecting certain types of manipulations.

Variability in image manipulation techniques could pose challenges in accurately detecting a wide range of image forgeries.

III.EXISTING TECHNIQUES

Several techniques are employed to detect image manipulation, focusing on different aspects of image forensics. Here's an overview of existing methods:

Error Level Analysis (ELA): Identifies areas with different compression levels, indicating possible manipulation. It is particularly useful for detecting inconsistent JPEG compression artifacts.

VGG16: VGG16, a widely used CNN architecture, is adapted for image manipulation detection by repurposing its feature extraction capabilities through transfer learning. With fine-tuning manipulated and authentic image datasets, VGG16 learns to discern between genuine and altered images. Detection methods involve analyzing feature representations and differences between manipulated and unmanipulated images for accurate classification.

Metadata Analysis: Analyzes embedded information, such as EXIF data, to identify signs of editing or inconsistencies in metadata.

Convolutional Neural Networks (CNNs): These deep learning models are trained to recognize patterns indicative of image tampering. Popular architectures like VGG16, ResNet, and EfficientNet are used for image forgery detection.

.

Frequency Domain Analysis: Techniques like Discrete Fourier Transform (DFT) and DiscreteCosineTransform (DCT) are used to detect anomalies in frequency patterns caused by manipulation.

Noise Analysis: Examines noise distribution in images. Inconsistent noise levels or patterns can indicate tampering.

Geometry-Based Methods: Focuses on distortions or changes in perspective, which could indicate manipulation.

IV. COMPARISON OF EXISTING TECHNIQUES

The methodologies across the studies combine Error Level Analysis (ELA), Convolutional Neural Networks (CNNs), and metadata analysis for image forgery detection. These techniques effectively identify inconsistencies in compression levels and extract features using deep learning, achieving high accuracy even with limited datasets.

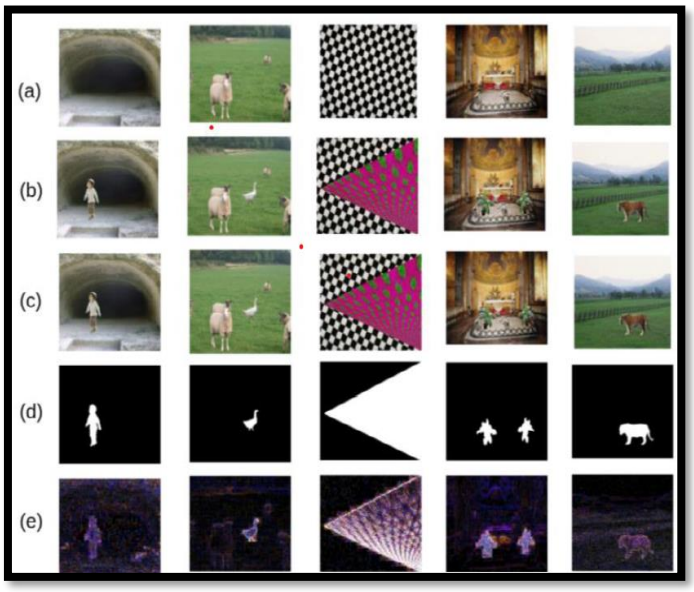
Existing techniques like Frequency Domain Analysis and Noise Analysis focus on detecting anomalies in frequency patterns or noise distribution. Geometry-based methods look for distortions or perspective changes. These approaches complement CNN-based detection, offering additional ways to identify forgery. However, the studies' reliance on ELA and metadata may not be foolproof, as metadata can be altered and ELA has limitations. The versatility of CNNs, especially with architectures like VGG16 and ResNet, provides robustness but requires substantial training data and expertise. The existing techniques can bolster CNN-based approaches, enhancing detection reliability.

V. PROPOSED METHODOLOGY

A. The image is compressed using JPEG compression and the compressed image is subtracted from the original image. Due to the compression difference, the resulting image highlights the forged or sliced part. This CNN-based model detects both copy-move and splicing forgeries.

B. CNN has already proven to have exceptional potential in a number of computer vision applications. Due to the diverse origins of the images, a range of distortions

appear when a piece of an image is transferred from one to another. CNNs can spot these distortions in falsified images even though they may be invisible to the unaided eye .



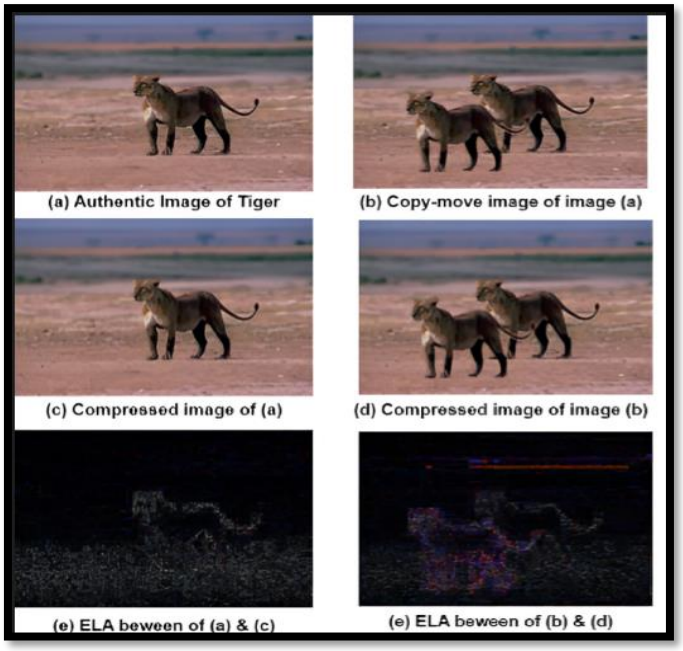
a) Original Image

b) Forged Image

c) Compressed Image

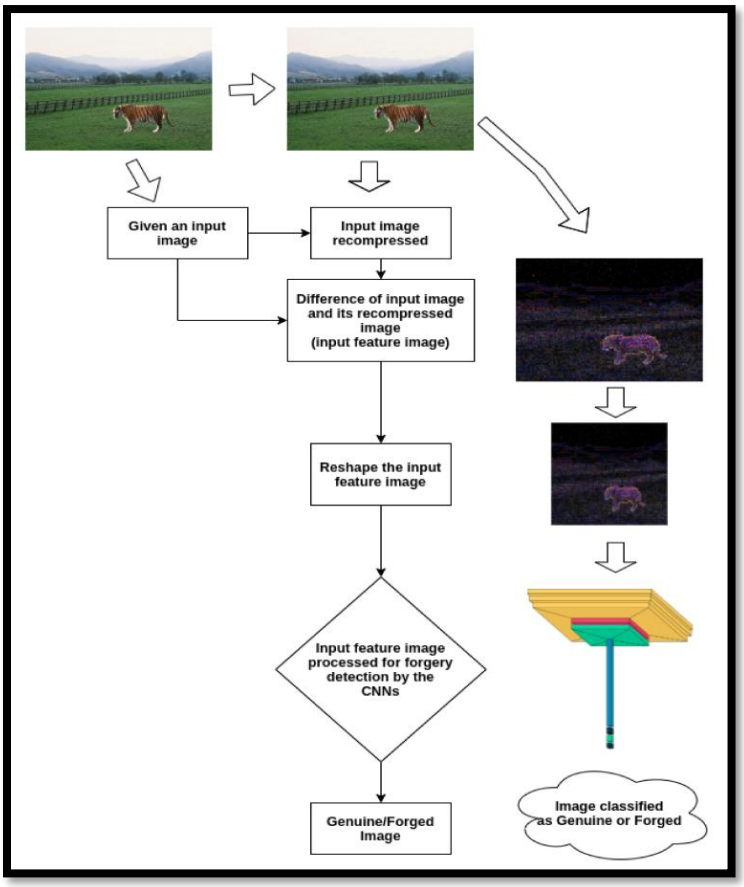
d) Mask of image used to edit original image

e) Subtracted Image



Difference between original image and forged image and their analysis through Compression and ELA methods

Flow Chart (of proposed methodology):

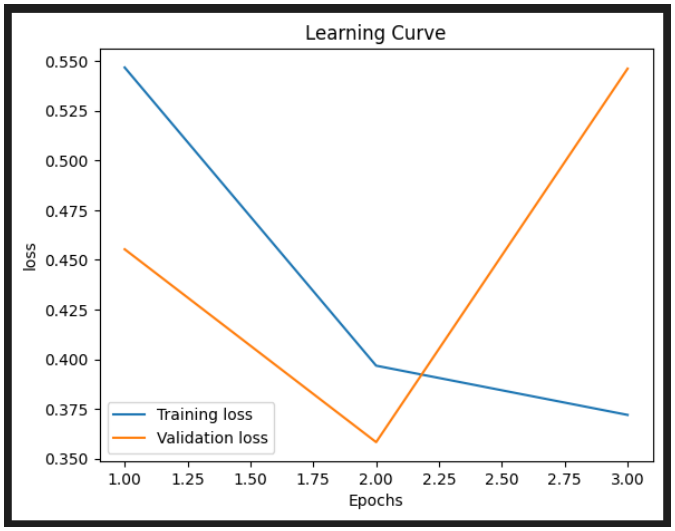


VI. RESULT

Our project integrated a recompression technique for image manipulation detection, yielding an accuracy of 85% on a test dataset containing both manipulated and authentic images. By employing fine-tuning on the pre-trained model and analyzing feature representations, we successfully discern between genuine and altered images.

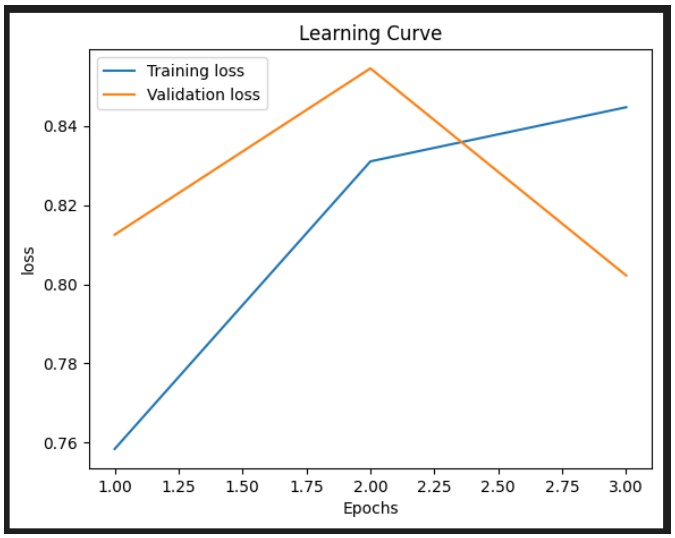
#Loss metrics

```
# Loss metrics
plt.plot(range(1, 4), history['loss'])
plt.plot(range(1, 4), history['val_loss'])
plt.legend(['Training loss', 'Validation loss'])
plt.title('Learning Curve')
plt.xlabel('Epochs')
plt.ylabel('loss')
```



#Accuracy metrics

```
# accuracy metrics
plt.plot(range(1, 4), history['accuracy'])
plt.plot(range(1, 4), history['val_accuracy'])
plt.legend(['Training accuracy', 'Validation accuracy'])
plt.title('Learning Curve')
plt.xlabel('Epochs')
plt.ylabel('loss')
plt.show()
```



#Scores

```
from tensorflow.keras.models import load_model
softmax_rms = load_model('./softmax_rms_new.h5')

y_pred = softmax_rms.predict(X_test)
y_pred = np.argmax(y_pred, axis=1)
y_t=np.argmax(y_test, axis=1)
# print_score()
print_score(recall=recall_score(y_pred=y_pred, y_true=y_t), precision=precision_score(
    y_pred=y_pred, y_true=y_t), acc=accuracy_score(y_pred=y_pred, y_true=y_t))
# confusion_matrix(y_pred=y_pred, y_true=y_t)
```

```
79/79 [==============================] - 38s 469ms/step
Recall score: 0.8282926829268292
Precision score: 0.8163461538461538
Accuracy score: 0.8545382481173206
```

#Outcome

Input (Not forged image):

Output:

```
[10]: from pylab import *
path=input("enter image path: \n")
try:
    img= Image.open(path)
    img=np.array(difference(path).resize((128, 128))).flatten()/255.0
    img=img.reshape(-1, 128, 128, 3)
except:
    print("Image does not Exist.\nWorng path")
```

```
enter image path:
 C:\Users\hp\Downloads\testcases\testlion.jpg
```

```
[11]: pred= model.predict(img)[0]
```

```
1/1 [==============================] - 0s 150ms/step
```

```
[12]: if pred[0]>pred[1]:
    print("Not Forged")
else:
    print('Forged')
```

```
Not Forged
```

Input(Forged Image):

Output:

```
[47]: from pylab import *
      path=input("enter image path: \n")
      try:
          img= Image.open(path)
          img=np.array(difference(path).resize((128, 128))).flatten()/255.0
          img=img.reshape(-1, 128, 128, 3)
      except:
          print("Image does not Exist.\nWorng path")

      enter image path:
       C:\Users\hp\Downloads\testcases\testbug.jpg

[48]: pred= model.predict(img)[0]

      1/1 [==============================] - 0s 235ms/step

[49]: if pred[0]>pred[1]:
          print("Not Forged")
      else:
          print('Forged')

      Forged
```

VII. CONCLUSION

In conclusion, the detection of image forgeries has become increasingly critical due to the rise of sophisticated image manipulation techniques. Various methods, including Error Level Analysis (ELA), Convolutional Neural Networks (CNNs), and metadata analysis, are effective in identifying inconsistencies that suggest tampering. While these approaches offer robust detection capabilities, they have limitations, such as reliance on large datasets and the potential for altered metadata.

A comprehensive approach that combines ELA, CNNs, frequency domain analysis, noise analysis, and geometry-based methods can improve detection accuracy and reliability. This multi-faceted strategy can address a wider range of forgery techniques, contributing to more secure and trustworthy digital imagery.

VIII. REFERENCES

- https://www.doi.org/10.56726/IRJMETS46401
- https://link.springer.com/article/10.1007/s11760-020-01636-0
- https://doi.org/10.22214/ijraset.2023.52367

Dataset Link:

https://www.kaggle.com/datasets/jayaprakashponday/casia2-dataset

Code Link :

https://drive.google.com/drive/folders/1ak6wENlGG50bonds4aeoVETxWM-81C_O?usp=sharing