Digital Image Forgery Detection

Aniket Shinde
Department of Computer Engineering
New Horizon Institute of Technology and Management
Thane, India
e-mail: aniketshindeas20@gmail.com

Kavita Rathod
Department of Computer Engineering
New Horizon Institute of Technology and Management
Thane, India
e-mail: kavitarathod790@gmail.com

Nishchal Tayade
Department of Computer Engineering
New Horizon Institute of Technology and Management
Thane, India
e-mail: nishchaltayade@gmail.com

Dr.S.BrinthaKumari
Department of Computer Engineering
New Horizon Institute of Technology and Management
Thane, India
e-mail: brinthakumaris@nhitm.ac.in

***Abstract*—Image forgery detection is an important field in computer vision and digital forensics that aims to detect any manipulation or alteration in digital images. The proliferation of digital imaging tools and techniques has made it easier to manipulate images for fraudulent purposes, such as spreading fake news, creating fraudulent documents, or defaming individuals.**

We have thus proposed a robust system that will deal with the prediction of an image if it is a fake image or a pristine image with reliable techniques like Convolutional neural network, Error level analysis, and Machine learning techniques.

***Keywords*——Image forgery, Image processing, Classification, binary segmentation, tampering.**

I. INTRODUCTION

Image counterfeit detection refers to the process of identifying whether an image has been altered or tampered with in any way. With the widespread use of digital imaging tools and software, it has become increasingly easy for people to manipulate images for malicious purposes such as: B. to spread fake news, defame someone or create fraudulent documents. Image counterfeit detection is an important area that can help prevent the spread of misinformation and protect individuals from fraud. As the technology for image manipulation evolves, image distortion techniques must evolve as well. The data set we will use is CASIA 2.0 We use ELA (Error Level Analysis) for data pre-processing, which distinguishes between real and fake images. By checking the compression level of the image, it detects if it has been multiply compressed. When you cut a section of an image and paste it into another image, the ALS of the pasted section often sees a larger error, i.e. it is lighter. one ELA level higher than the rest of the image... ELA is applied to the input image.Model construction and model training part is carried out. The first phase is the classification problem that determines whether the image is real or fake. The second phase is the binary image segmentation problem, where we are given an input image and we get the output as a binary image. When the image goes through the CNN layer, we get a 512*512 binary image. Our goal is to classify whether an image is manipulated or not and highlight the manipulated part.The methodology of this project includes data pre-processing, modeling and evaluation.[1] The CNN model is built with the VGG16 architecture and is trained on pre-processed data for 10 epochs with a batch size of 64. Image distortion is detected under the lighting conditions of the objects. A fake is detected based on the difference in the direction of illumination of the fake part and the real part of an image.

The paper introduces a new system based on a combination of error level analysis and convolutional neural networks in machine learning and computer vision to solve the problems. [2] The study split the data set into manipulated images and original images, and then determined the architecture used to train the recognition. They chose to use VGG 16 in this training because VGG is perfect for training with minimal data sets. The result of our experiment is the best training accuracy of 92.2% and 88.46% validation through 100 epochs.

The paper introduces a new system based on a combination of error level analysis [3] They started preprocessing images. Then the segmentation was performed. Finally, CNN was used to classify whether the image is manipulated or not.

Almost all of these techniques exploit the content-based property of the image. For example, visual information is present in the image. CNNs are inspired by the visual cortex. Technically, these networks are designed to extract features from the image to turn them into meaningful ratings. Another example, For which minimizes the function.

Here, the core weights of the network parameters are learned by gradient descent to generate the most discriminatory features of the image fed to the network. These features are all fed into an associated layer that performs the final task of classification.

II. LITERATURE SURVEY OF DIFFERENT DEEP LEARNING APPROACHES.

Syed Sadaf Ali et al., ,2022 [1] used Convolutional Neural Network the error level analysis (ELA) proposed by the authors to detect fakes in an image. A falsification of an image is detected based on the lighting conditions of the objects. It tries to find the fake based on the difference in lighting direction of the fake part and the real part of an image. In US 5,000, several conventional counterfeit detection techniques were evaluated. for detection in image for splicing and copy-move with overall validation accuracy of 92.23%.

Ida Bagus Kresna Sudiatmika Et al., 2019 [2] applied ELA(Error Level Analyzing) and deep learning a new system to combine error level analysis and convolutional neural network in machine learning and computer vision to solve the above problems. First we split the dataset into modified images and original images, then we determine the architecture used to train the recognition. We chose VGG 16 in this training because VGG is perfect for training with minimal data sets.Minimum Storage Regeneration (MSR) codes are an important class of optimal regeneration codes that (initially) minimize the amount of data stored per node and (later) the repair bandwidth that has successfully accuracy of training 92.2% and 88.46% validation.

Diaa Uliyaan et al., 2020 [3] implemented SRM(Spatial Rich Model) and MSR(Minimum Storage Regenerating).The SRM (Spatial Rich Model) is a very effective method of stegoanalysis. It uses sample neighbor noise residual statistics as features to capture dependency changes caused by embedding. Since noise residues are the high frequency components of the image and are closely related to the image content, residues from different types of image regions have different statistical properties and effectiveness for shorthand analysis. with an accuracy of 92.85%.

Junxue Yang et al., 2020 [4] used Stenographic algorithms to determine the forged parts of the image using binary sequence of numbers with a success rate of 98.1% of accuracy.

Castillo Camacho,2021 [5] implemented Comprehensive Review of Deep Learning-Based Methods for Image Forensics J.Imaging with an accuracy of 97.4%.

Meena K.B,2019 [6] applied Detection and Localization of Multiple Image Splicing Using MobileNet V1 has accuracy of 93.5%.

Xiao B,2020 [7] applied Image splicing forgery detection combining coarse to a refined convolutional neural network and adaptive clustering with an accuracy of 98.6%.

Ali,S.S,2020 [8]used a Robust biometric authentication system secure user template with accuracy of 84.2%.

Verdoliva L,2020 [9] studied for Media Forensic and DeepFakes: An Overview.IEEE. Sel.Top. Signal Process with an accuracy of 91.6 %.

Basharat A,2020 [10] implemented for Attentive Generative Adversarial Network for Image Copy-Move Forgery Detection and Localization with accuracy of 98.7%.

III. PROPOSED METHODOLOGY

The proposed method can detect whether the image is manipulated or not, and if so, highlight the area. Tampering detection is effectively implemented using pre-processing, ELA technique and machine learning. ELA is used to detect image tampering by analyzing the compression levels of different parts of the images. The data set is then divided into a training set and a test set.

CASIA record 2.0 is used for the implementation of this project. This problem consists of two phases. In the first phase, real and false image detection is used, which is a classification problem. And in the second phase, the prediction of the manipulated image area (Image2Image) is used, which can be considered as a binary image segmentation problem.

As stated above, when an image is recompressed if it contains a fake, the Fake part of the image is compressed differently than the rest of the image due to the difference between the source of the original image and the source of the counterfeit part. When analyzing the difference between the original image and its recompressed version , this strongly emphasizes the forgery component. As a result, we use it to train ours CNN-based image distortion detection model.

Most likely, a spliced region would have a statistical difference in a different image distribution of DCT coefficients than the original region. The authentic region is compressed. twice: first in the chamber and then again in the forgery, resulting in periodic patterns in the histogram. The spliced section behaves similarly to a single compressed region if the secondary quantization table is used.

The operation of the proposed technique that has been explained here. We took a fake image and then compressed it again. Now we take the difference between the original image and the newly compressed image. Well, due to the difference in the source of forging and the original part of the picture, the corrupted part is highlighted in as we can see We train a CNN-based network to categorize an image as fake or real image as our input function gives the pictorial representation of the general operation of the proposed method.

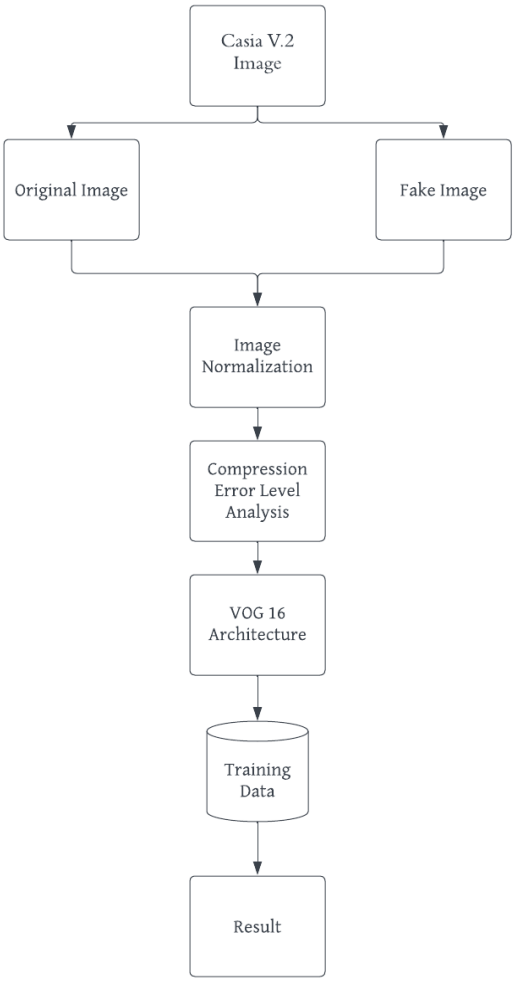


Fig. 1.2 : Proposed Model Architecture

IV. IMPLEMENTATION

Considering all the different methods to implement this given image counterfeit detection problem, we created a workflow that includes all the above works on the related topic.
This section describes the steps we took to complete this project. In our project, we collect enough data to train the model to ensure that the model is not overfitted, and then we implement a model that preprocesses the image, segments the image, and finally manipulates the images using CNN classified as a model of the convolutional neural network architecture.

A. Dataset

The dataset named "CASIA V.2" is taken from the Kaggle website. The folder contains fake and pristine images... In the dataset, there are three folders Tp, CASIA 2 Groundtruth, and Au. Tp contains fake images. Casia 2 Groundtruth contains fake image masks and Au contains real images. The total number of fake images comes out to be 2064. Each fake image has a mask image(stored in CASIA 2 Groundtruth folder) that shows us the region which is tampered with. The number of real images is 7437 which is significantly higher than the number of fake images which can lead to the problem of an imbalanced dataset. Thus we will reduce the number of pristine images. This technique to handle imbalanced datasets is called undersampling.

B. Image processing

The pre-processing phase of our project mainly involves the conversion to grayscale. Grayscale conversion is the simplification of grayscale images using ELA. The pre-processing phase takes an image from the dataset and splits it into patches, and that patch is then sent to the CNN classifier. When you cut and paste part of an image into another image, the ELA for the pasted part often has a larger error, meaning that it is brighter than the rest of the image at a higher ELA level. We use a pre-trained VGG16 model for better accuracy.The input for the first convolution layer is an RGB image of size 224*224. The image then goes through a stack of convolutional layers.

C. Modeling.

We build a simple 2 convolutional layers neural network with a maximum pooling layer and an exclusion layer, followed by two dense layers and an output layer. there are a total of 4,271,841 parameters. We then compile the model using Adam (learning_rate=0.0001) as the optimizer and binary cross entropy as the loss function because there are only two classes. LearningRateScheduler: - Decreases learning rate by 10x every 5 epochs.Early stop: monitors the loss of validation, if it does not decrease after 3 epochs, it stops the training model. will build a dual stream UNET. The first stream takes a normal RGB image as input and the second stream takes a processed image by passing the image through SRM filters. The output of both streams is then concatenated and passed through a CNN layer with a sigmoid activation function. The output is a 512*512 binary image.The loss function I used for this model is the binary cross entropy since the output is a binary image with pixel values of 0 or 1. We have a real mask image and a predicted mask image (threshold = 0.5). We iterate through each pixel (both the actual mask image and the predicted mask image have the same number of pixels) and find how many pixels in both images have the same pixel value (intersect). The union is how many pixel values there are in total (count the number of pixels in each image, both have the same number of pixels).IOU ranges from [0, 1] to 1 when both the predicted mask image and the actual mask image are the same, and 0 when the predicted mask image and the actual mask image are different. You will create a function that takes the input image and passes it. SRM filters and resizes the resulting image. We will then pass both the input image and the resulting image we get by passing the input image through SRM filters to our dual-stream UNET model, which will give us a binary image output, essentially taking an input image and the predict function we created calls
for phase 1, if it predicts the image is wrong, it calls the predict_region function, which gives us a binary image, with the black region showing us what area of the image it is manipulating.

V.RESULTS

In this section, we analyze the performance of the proposed model using various evaluation metrics. All the results we got while working on our model are listed below. original or counterfeit or counterfeit. Pre-processing methods such as gray scaling, dimensionality reduction, feature extraction and segmentation are used to detect tampering. This study presents an approach where we used the convolutional neural network (CNN) as the working model with dual-stream UNET.

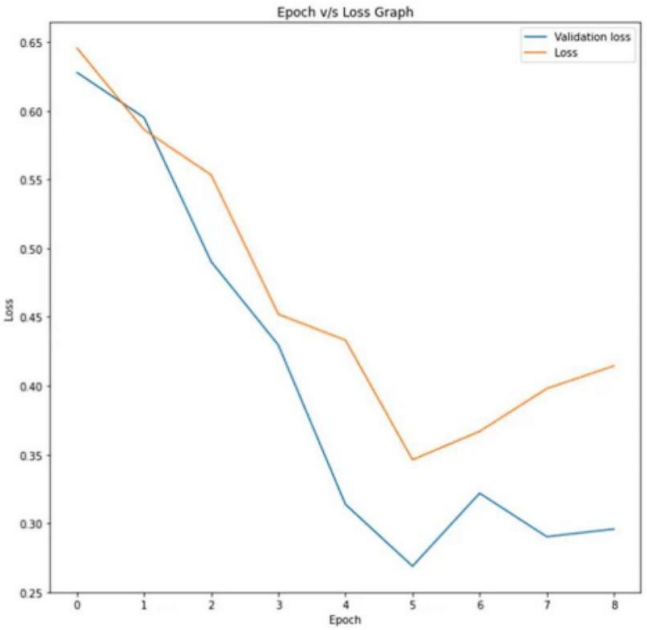


Fig. 4.1 Epoch v/s Loss graph

VI. CONCLUSION

This research article describes the techniques for detecting image tampering and classifying images as real/fake.

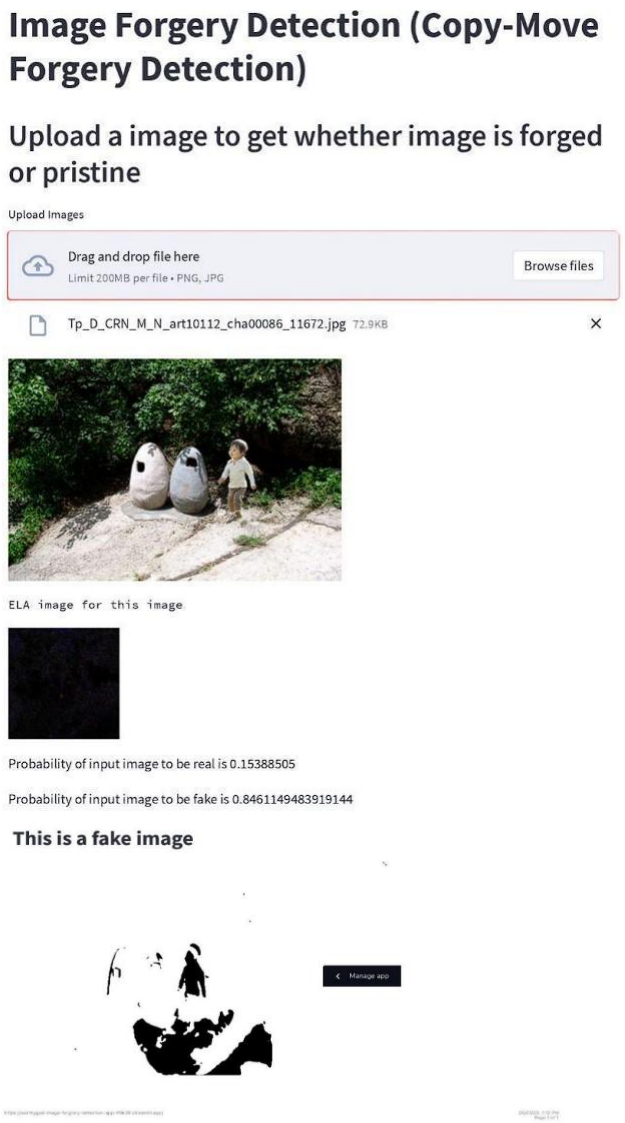
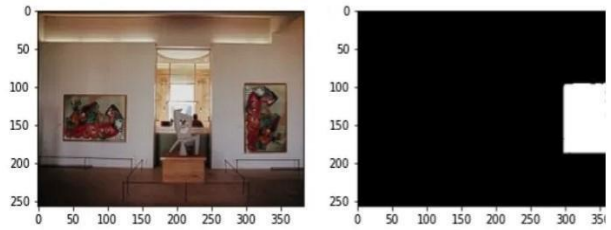


Fig. 4.2: Highlighted Forged Part



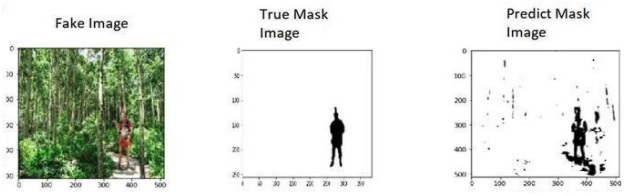


Fig. 4.3 Fake image prediction

VII.REFERENCES

1. Xiao, B.; Wei, Y.; Bi, X.; Li, W.; Ma, J. Image splicing forgery detection combining a coarse to a refined convolutional neural network and adaptive clustering. Inf. Sci. 2020, 511, 172–191
.
2. Ali, S.S.; Baghel, V.S.; Ganapathi, I.I.; Prakash, S. Robust biometric authentication system with a secure user template. Image Vis. Comput. 2020, 104, 104004.

3. Meena, K.B; Tyagi V. Image forgery detection survey and future directions.In data, Engineering and Applications: Volume 2; Shukla, R.K., Agarwal, J.Sharma, S., Singh Tomer, G., Eds.; Springer: Singapore,2019; pp.163-194.
4.Islam,A.;Long,C.;Basharat,A.;Hoogs,A.DOA-GAN: Dual-Order Attentive Generative Adversarial Network for Image Copy-Move Forgery Detection and Localization.In Processing of the 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR), Seattle, WA, USA,13-19 June 2020; pp. 4675-4684.

5.Kadam,K;Ahirrao,D.S.;Kotecha,D.K,;Sahu,S.Detection and Localization of Multiple Image Splicing Using MobileNet V1,2021.arXiv:2108.09674.

6.Ali,S.S.;Iyappan,G.I.;Prakash,S.Fingerprint Shell construction with impregnable features. J. Intell.Fuzzy Syst.2019,36,4091-4104.

7. Bi, X.; Liu, Y; Xiao, B.; LI, W.; Pun, C.M.; Wang, G.; Gao, X.D-Unet for Image Splicing Forgery Detection and Localization.arXiv 2020,arXiv:2012.01821.

8.Abdalla,Y.;Iqbal,MT.;Shehata,M.Convolutional Neural Network for Copy-Move Forgery Detection.Symmetry 2019,11,1280.

9. Verdoliva, L.Media Forensic, and DeepFakes: An Overview.IEEE.Sel.Top. Signal Process.2020,14,910=932.

10. Castillo Camacho, I; Wang, K.a Comprehensive Review of Deep Learning-Based Methods for Image Forensics J.Imaging 2021,7,69.