Image Forgery Detection Using Deep Learning Model

Rekapalli Praveen Kumar, Maradani Roopasri, Thumu Brahma Reddy,
Talari Manoj Dora
Department of Computer Science Engineering, Raghu Institute of technology
Visakhapatnam, Andhra Pradesh, India
Corresponding Author: Dr. M A Srinuvasu (Asst. professor)

Abstract:
This report examines the results of Two image forgery detection algorithms.The two Image Forgery Detection algorithms are Error Level Analysis and Convolutional neural network. Each algorithm was implemented with Python and trained on a sample of dataset of forged and unforged images, including a selection of images from an image manipulation dataset. Each method has its own set of advantages and limitations, however with all two methods combined then the overall detection rate was an impressive 92%. Error Level Analysis and Convolutional neural network provided the decent results.The metadata tag detection was also run on each image, however it was found to be too introductory to be considered a method in it's own right, as tags within files can be cleared or removed without much effort. This project therefore provides an perfect base for a user to determine the most applicable image forgery detection method for their use, depending on the different types of images that they commonly deal with.

Date of Submission: 12-08-2021 Date of acceptance: 27-08-2021

I. Introduction:

Since the invention of photography, individuals and different organisations have often looking for ways to manipulate and modify images in order to mislead the viewer.In the same time fairly it is a difficult task and many hours of work required to a professional technician, with the arrival of digital photography it is now possible and fairly simple for anyone to easily modify images, and even easier to achieve the professional looking results. This has result of social issues.There contains the number of methods available in which to manipulate an image, image forgery detection has become a growing area of research in both academic and the professional world.Many methods available in order to detect forgery within digital images, however it is difficult to find which are most efficient and practical to implement and run.

The aim of this project is to research and investigate in to the various methods surrounding image forgery detection. so as to cut back the complexity of this task, as commenced within the initial report, algorithms are grouped in to 5 distinct algorithm types. These are JPEG Compression Quantization, Edge Detection, Clone Detection, Resampling Detection and light-weight & Colour Anomaly Detection. More specific research will then be concluded on these different groups, determining the efficiency of the described algorithm type normally. If the method is found to be reliable, then an algorithm from this group is implemented. These groups are chosen as their detection methods are entirely different from one another, and so should achieve very different results reckoning on the image forgery type.

The results of this research are of great use so as to boost the credibility of images used within the media. Image forgery is an ever increasing issue in modern society, and there are instances where forged images have been employed by mistake, or when images have specifically doctored so as to be misleading. Despite the importance of the problem, there's still no widely recognised method so as to detect image forgeries, and definitely no industry standard. This represents a chance to produce an insight that may benefit one of the biggest industries within the world, and potentially improve the reliability and credibility of the pictures presented by the media. This also allows individuals the opportunity to see the credibility of the pictures provided to them, either through official, credible sources or elsewhere, like on an online message board or shared by a disciple on social media.

II. Literature Review:

Now a days marphing an image is very easy.There consists number of photo editing tools like adobe photoshop,picsart etc.on multiple platforms windows,android,mac etc.So we have to use the some fabricated image detection tools to know the photo edited or not.Some of the researchers are published the some of the articles,and their methods.

As machine learning and also the computer vision are a trending topics since last two years. There has already been an enormous amount of research and existing projects on this particular domain. More over Deep learning concepts made complex tasks feasible that might only be handled by human brains by means of Neural Networks.

There are various techniques performed by researchers during this case. Meera Mary Isaac et al. doing image forgery detection using Gabor Wavelets dan Local Phase Quantization. By using CASIA TIDE v.1 Dataset . Birajfar et al. Employing a passive technique method in analyzing false images. In his research summarizes some research that does image forgery .Youseph et al. using the illuminant color Estimation method, by combining the canny detection and HOG edge descriptor to induce the sting border of the image. afterward training using SVM with 74% accuracy value . Mohhamad F.H using an efficient and robust method combining un-decimated wavelet transform and scale invariant feature transform and judging from precision, recall, false positive rate . Jie Zhao et al. analyze image forgery using DCT and SVD algorithm analyze supported DAR and FPR . A. Dixit et al. reviewing a number of the studies discussing image forgery . In his research, he stated some methods of image forgery and its application. Wu-Chih Hu analyze image forgery supported image watermarking and alpha mattes analysis . Ghulam Muhammad et al. in his research to research image forgery using dyadic wavelet transform . Ashwini V Malviya et al. using Auto Color Correlogram on analyzing image forgery. Rani Susan Oommen used Fractal Dimension and singular values in analyzing original image and pretend image .

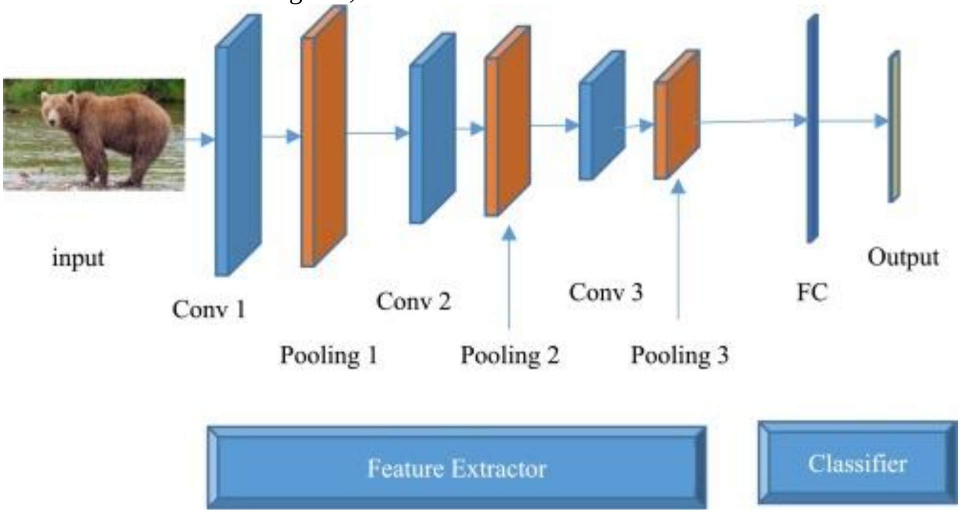
III. Research methodology:

Here we used the Convolutional neural network and Error level analysis and VGG-19.

Convolutional Neural Network:

Convolutional neural network has mainly been used for classifing the processing of images. CNN network has an input and an output layer,and multiple hidden layers. The hidden layers of a CNN[1] normally consist of a series of convolutional layers. ReLU is the activation function, which is typically followed by additional operations such as pooling layers, fully connected layers and normalization layers. Backpropagation used for the error distribution and weight adjustment.This work makes learning completely automatic and performance is better than the manual coefficient adjustment. It is useful for variety of image recognition problems and image types. This approach became a foundation of modern computer vision.The efficient use of convolutional neural networks depends on more layers and larger networks. Therefore, this technique is limited by computing power and availability of a big data.

Fig. 8.1, Illustrate the structure of CNN.



Error level analysis:

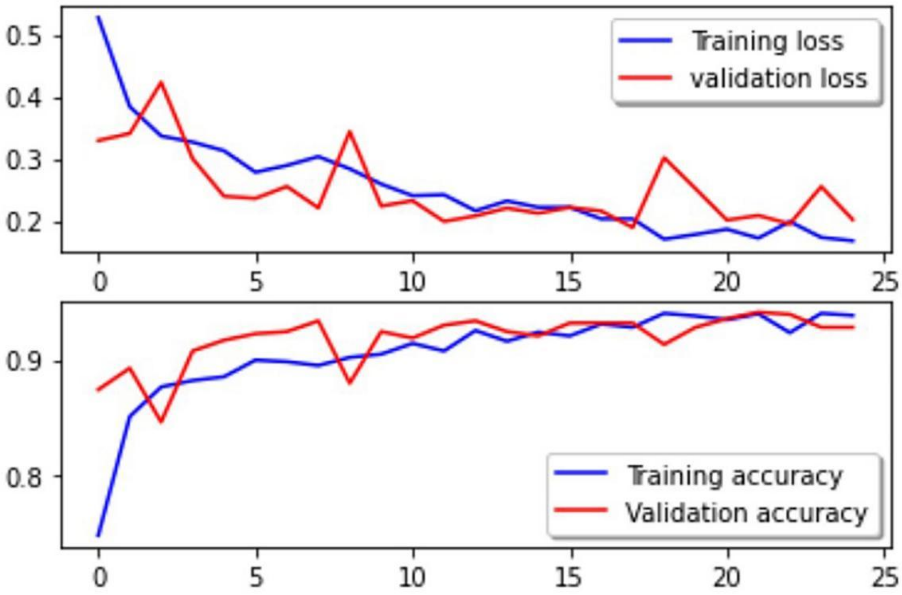
Error Level Analysis or ELA has become the foremost common method for image modification detection. This method relies on the actual fact that JPEG compression removes overmuch information about original's brightness and color. the quantity of knowledge being removed depends on compression rate and, of course, signal quantization matrix. If original image compressed just the once is quantizated by the identical matrix because the original, modified image won't differ from the initial. But if the initial image is saved in JPEG variety of times, there'll be significant differences between the first and modified image. The results of ELA is error pattern, which shows differences between the initial and modified image. The aim of forensic examiner is to interpret error pattern right.

VGG-19:

VGG-19 is convolutional neural network that's 19 layers deep. you'll load a pretrained version of the network trained on over 1,000,000 images from the ImageNet database. The pretrained network can classify images into the 1000 object categories, like keyboard, mouse, pencil, and plenty of animals. As a result, the network has learned the rich feature representations for a large range of images. The network has a picture input size 224-by-224.

IV. Results:

In this section, we are going to discuss about the results we achieved despite of smaller dataset compared to datasets in existing systems. We obtained training accuracy of 93.80% and validation accuracy of 92.78%.



V. Conclusion:

This project has successfully illustrated the strengths and weaknesses of the two distinct image forgery detection algorithms, and the ability to perform on an oversized sample set of both unique sample sets and dataset image libraries.

It was clear that from the beginning of the project that no algorithm would work flawlessly in every situation, however the variability of images used has allowed the user to work out the algorithm best suited to their needs.

First of all the success rate of the chosen algorithms were very promising,we’ve also learnt that new methods are constantly being developed so as to provide better results and improved performance. it's therefore appreciated that further work are going to be required so as to completely investigate a wider range of forgery detection methods. Research in to the present new and exciting field is becoming very important, as determining the trustworthiness of images becomes a wider issue in modern society. This project provides sound framework for additional tests to be come out on a good wider range of algorithms within the future.

References:

[1]. Simonyan K, Zisserman A 2014 Very deep convolutional networks for large-scale image recognition arXiv preprint arXiv:1409.1556

[2]. Error Level Analysis (https://fotoforensics.com/tutorial-ela.php)

[3]. IEEE research paper (https://ieeexplore.ieee.org/document/8203904)

[4]. Amerini I, Uricchio T, Ballan L, Caldelli R 2017 Localization of JPEG double compression through multi-domain convolutional neural networks IEEE Conference on Computer Vision and Pattern Recognition Workshops 1865-1871.