International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 12 | December - 2022 Impact Factor: 7.185 ISSN: 2582-3930

Tampering Detection System (A Machine Learning Approach)

Tarun

Enrollment No. - 13614803119

(Information Technology scholar at Maharaja Agrasen Institute of Technology, Delhi-India)

Under supervision of:-

1. Dr. ML Sharma (H.O.D)

(Department of IT , Maharaja Agrasen Institute of Technology, Delhi-India)

2. Dr. KC Tripathi

(Department of IT , Maharaja Agrasen Institute of Technology, Delhi-India)

ABSTRACT

With a big section of the population having access to the internet and a camera, the quantity of photographs shared online is growing exponentially. Using cutting-edge software like Adobe Photoshop, where we can copy and paste one image over an original one, it is simple to create fake images. Social media businesses' top issue is doctored photographs. These altered photographs are the main source of false information and are frequently used to incite mobs. Since it is getting harder for the average person to tell the difference between a true image and one that has been altered thanks to the development of photo and video editing tools, forensic experts are needed. Social media is a virtual environment where many photographs are shared. There is no doubt that there are a lot of fake photographs with the numerous altering programmes available. By employing Error Level Analysis to forensically examine the image, it is possible to compare the actual and false photos'

DOI: 10.55041/IJSREM17333

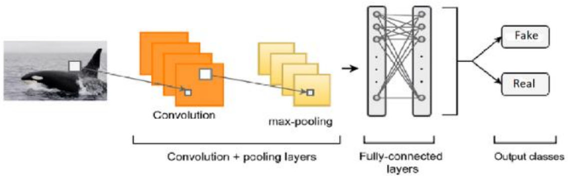
levels of compression because they differ. While it is possible to edit the metadata, it is also possible to analyse the image's metadata in order to determine whether it is real or phoney. It can be done by using a simple neural network with two convolutional layers, a max pooling layer, a dropout layer, two dense layers, and one output layer to apply deep learning to recognise images of manipulations using a dataset of a fake image and original images.

INTRODUCTION

The quick development of technology has made it simpler for people to transmit false information and photos. With so many pieces of software available for image manipulation, the public can easily edit images. Due to the proliferation of fraudulent photographs on social media that can cause controversy, the image's forensic validity must be established. Image forensics, in general, is the study of tracing an image's lineage and establishing its veracity. There is a need for a tool to assist individuals in determining whether the photographs being shared on social media and the Internet are authentic or phoney because there are so many misleading images that do so. one of the many approaches used to assess the level of authenticity of the image. The nearest neighbour field approach is the method utilised in this study to gauge the degree of compression. This method is used to identify photographs that have been digitally altered. Scientific research on picture tampering has produced a number of methods for determining whether an image has been altered. Resampling is a crucial 2 characteristic of modified photos, according to Bunk et al discussion's. They suggested employing resampling detectors and deep learning classifiers to identify and pinpoint the area of alteration on a picture. Abdalla et al. provided a method for determining whether an image is faked that involved transfer learning. To identify and pinpoint the area of alteration, Bappy et al. used a long-short term memory network with encoder decoder architecture.

RESEARCH METHOD

. The dataset for this experiment is split into two parts: the training set, and the test, each of which contains two categories: the category of false images, and the category of the original image. The dataset from Casia V2 was split into two categories When viewed with the naked eye, the image appears identical, but when utilising this technique, it is possible to tell the difference between a fake and the real thing Calculation of the luminance and Chrominance. The image is not optimised by the digital camera for a particular camera quality level. High ELA values should be present in the original digital camera photos. The possible error rate will drop with each additional saving. High values can be seen through the white of original photographic photographs.



The most crucial layers of CNN are the pooling and convolutional layers. By merging the image region

first: real photographs and fraudulent images. For the study on the level of compression error in the image, we utilise CNN to distinguish between real and fraudulent photos in accordance with the ELA.

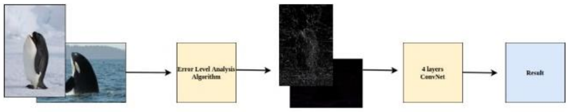
with numerous filters, convolutional layer is utilised to extract feature. The convolution layer's output map is made smaller by the pooling layer, which also inhibits overfitting. There are far fewer neurons, parameters, and connections in these two layers than in a CNN model.

The layer, which is typically applied in MLP applications, tries to modify the dimensions of data such that they may be categorised linearly . Before each neuron in the convolution layer can be incorporated into a fully linked layer, it must first be converted into one dimensional data. In this architecture, the convolutional layer employs a filter, the pooling layer, and the remaining three layers are completely connected. Send the activation function in each convolutional layer. As an activation function, the Recified Linear Unit (ReLU) is used to eliminate non-linear values from process data.

METHODOLOGY

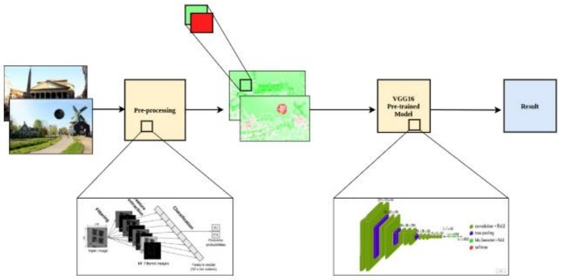
In this research we propose a machine learning model with boosted accuracy to predict whether the image is real or have been tampered by different tempering methods. Data collection means pooling data by scraping, capturing, and loading it from multiple sources, including offline and online sources. The total number of fake images collected comes out to be 2064. 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 imbalance dataset. Thus we will reduce the number of pristine images this technique to handle imbalances datasets is called undersampling.

So the idea is to do error level analysis on the input image and pass the ELA of the input image to a simple convolutional neural network which is trained to differentiate between a fake image or a pristine image.



In this case , we are building a simple neural network with 2 convolution layers with a max pooling layer and a dropout layer followed by two dense layers and one output layer. Then we compile the model with Adam (learning_rate=0.0001) as optimizer and binary cross entropy as loss function because there are only two classes.

Then we put the model to train for 30 epochs but it stopped after 9 epochs because of our early stopping callback as our validation loss didn’t decrease for 3 epochs.



we are using streamlit to locally host the model in our pc which have a dropbox to select images and then predicts whether the image is most probably pristine or not.

CONCLUSION

In this research we build a application for determining that whether the given image is fake or pristined . Image tampering is the malicious manipulation of photos, sometimes including images of persons. This entails altering an actual image that was published on a public website or digital communication platform into a completely different one.

The new image is probably going to be immoral or intended to generate bad press. When the quality of the input photos is similar to the quality utilised in the algorithm, the ELA method can detect whether an image has been altered. The outcome will always be inaccurate if there is a significant gap between the quality of the algorithm and the quality of the image. The program also hides the precise area of manipulation. A model that has already been trained on a certain task using the ImageNet dataset is referred to as pre-trained. It is a model that has been taught to address problems that might be comparable to the one at hand.

REFERENCES

[1]. Y. Wu, W. Abd-Almageed, and P. Natarajan. Image copymove forgery detection via an end-to-end deep neural network. In WACV, pages 1907–1915. IEEE, 2018.

[2]. Wu, Yue, Wael Abd-Almageed and Premkumar Natarajan. "BusterNet: Detecting Copy-Move Image Forgery with Source/Target Localization." ECCV (2018).

[3]. Capsule-Forensics: Using Capsule Networks to Detect Forged Images and Videos. Huy H. Nguyen, Junichi Yamagishi, Isao Echizen.

[4]. J. Chen, X. Kang, Y. Liu and Z. J. Wang, "Median Filtering Forensics Based on Convolutional Neural Networks," in IEEE Signal Processing Letters, vol. 22, no. 11, pp. 1849-1853, Nov. 2015. doi: 10.1109/LSP.2015.2438008

[5]. K. Uchida, M. Tanaka, and M. Okutomi, "Coupled convolution layer for convolutional neural network," in 2016 23rd International Conference on Pattern Recognition (ICPR), 2016, pp. 3548–3553.

[6]. Rao, Yuan and Jiangqun Ni. "A deep learning approach to detection of splicing and copy-move forgeries in images." 2016 IEEE International Workshop on Information Forensics and Security (WIFS) (2016): 1-6.