INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 7, Issue 4 - V7I4-1510)
Available online at: https://www.ijariit.com

Tamper Detection of Social Media Images using CNN

Gaurav Shetty
gauravbvr@gmail.com
Sahyadri College of Engineering and Management, Mangalore, Karnataka

G. S. Shrijitha
shrijitha99@gmail.com
Sahyadri College of Engineering and Management, Mangalore, Karnataka

Shravika Nempe
shravikanempe2@gmail.com
Sahyadri College of Engineering and Management, Mangalore, Karnataka

Nandan N. K.
gowdanandan20@gmail.com
Sahyadri College of Engineering and Management, Mangalore, Karnataka

Shwetha S. Shetty
shwethas.is@sahyadri.edu.in
Sahyadri College of Engineering and Management, Mangalore, Karnataka

Abstract*—Images are often manipulated with the intent and purpose of benefiting one party. images are often seen as evidenceof a fact or reality, therefore, fake news or any form of publication that uses images that have been manipulated in such a way has the greater capability and potential to mislead. The web permits clients to process any type of digital media within seconds all over the globe. With expanding utilization of digital multimedia contents like pictures and video, the techniques for detecting the digital image forgery have also increased parallelly. people tamper with images to make the image look more pleasant for appearance but it is suspectable if one changed someone's face within the image and misuse it. Hence this demands automatic tools for identifying the differencebetween authentic and tampered images. To detect such image falsification, a large amount of image data is required, and a model that can process each pixel in the image. In addition, efficiency and flexibility in data training are also needed to support its use in everyday life. The concept of big data and deep learning is the perfect solution to this problem. Therefore, with an Error Level Analysis (ELA), Convolutional Neural Network (CNN).

***Keywords*—** *Digital Image Forgery, Photo Editing Software Tools, Image Tampering Detection, Convolutional Neural Network*

1. INTRODUCTION

An image is a visual representation of something. It is also defined as a picture that is created or copied and stored in electronic form. Images can be described in terms of vector graphics as well as raster graphics. An image stored in raster form is also called a bitmap. An image map is a file containing information associated with different locations on a specified image with hypertext links.

nowadays digital multimedia contents are effortlessly accessible and available to the general public. Portable cameras and other handy gadgets permit anybody to capture images. Image Forgery is not a new concept. History has recorded its first image forgery in the 1840s. Hippolyta Bayard is the first person who created a fake image which is the pictureof him committing suicide. He has done that because he lost the chance of becoming the inventor of photography to Louis Daguerre since Daguerre patented a photography process earlier than him. Digital Image Tampering does not differ verymuch in nature compared to conventional Image Tampering. Instead of using a photograph, the digital image Tampering deals with the digital image. The process of creating a fake image has become simple with the introduction of computer graphics editing software like GIMP, Adobe Photoshop, and Corel Paint Shop, some of the editing software's are easily available for free. There are many types of digital image tampering. These cases can be categorized into three major types, based on the process involved in creating the tampered image. The types are Image Retouching, Image Splicing as well as Copy-Move Attack.

One can easily edit images with the help of computer software or mobile applications easily before sharing the doctored images on social media sites. Due to the increase in technology many advanced image manipulation software has been launched in the market which grants the forgers to manipulate the image in any desirable way that is visually not perceivable. Although most people do it for fun, it is susceptible if objects are concealed or changed someone'sface within the image. Before finding intentions behind the Tampering, we need to first identify how and which part of the image has been tampered with. It, therefore, demands automatic tools for identifying differences between authentic images and tampered images.

2. PROBLEM STATEMENT

In this day and age, tampering with images can be done easily with widely available image editing software. Most people tamper with images to make them look more pleasant for appearance but it is suspectable if an object concealedor

changed someone's face within the image and misuses it. Hence this demands automatic tools for identifying tampered images.

3. METHODOLOGY

There are two main methods in this project, namely Error Level Analysis (ELA) and machine learning with deep learning techniques in the form of Convolutional Neural Network (CNN).

3.1 Error Level Analysis

ELA is one technique used to detect image manipulation by restoring the image at a certain quality level andcalculating the ratio between compression levels. In general, this technique is performed on images that have a lossy format (Lossy compression).Image type JPEG is used in mining this data. In JPEG images, compression is performed independently for each 8x8 pixel in the image. If an image is not manipulated, every 8x8 pixels in the image must have an error rate .

Fig. 1. Real Image

Fig. 2. ELA converted Image

3.2 Convolutional Neural Network (CNN)

CNN is the type of Feedforward based network, t hat is the flow of information is only one direction, namely from input to output. While there are several types of CNN architectures, in general, CNN has some convolutional layer and pooling layer followed by one or more fully connected layers. In image classification, the input on CNN is in the form of an image, so every pixel can be processed. In short, a convolutional layer is used as a feature extractor that studies the representation of these features from images that are input on CNN. Meanwhile, the pooling layer is responsiblefor reducing the spatial resolution of the feature maps. Generally, before fully connected layer, there are piles of several convolutional and Pooling layer that serves for extract representation for more abstract features. After that, the fully connected layer will interpret its features and performs functions that require high-level reasoning. Classification at the end CNN will use the function SoftMax.

In general, architectural design is divided into two major parts, namely Data preparation and model building. In theInitial stage, input data consisting of images with the format ".jpg", Tampered and Non-tempered images with real labels, put into stage data preparation. Data stage preparation is the stage where each image is input data converted first intoa result image Error Level Analysis . Then, the ELA image will be Resize into an image with a specific size.

The conversion of raw data to the ELA result image isa method used to increase the training efficiency of the CNN model. This efficiency can be achieved because the results of the ELA image contain information that is not as excessive as the original image. The features produced by the ELA image are focused on the part of the image that has a level error above the limit. Other than that, the pixels of an ELA image tend to have colors that are similar to or in sharp contrast tothe pixels nearby, so training the CNN model is becoming more efficient.

After that, the image size changes. In the next step,each RGB value is divided by the number 255.0 to normalize so that CNN converges faster (reaching the global minimumof loss values belonging to validation data) because the value of each RGB value only ranges between 0 and 1. The nextstep is by changing the label of the data, where 1 represents tampered and 0 represents real in to a categorical value. After it was done by dividing training data and validation data using the division of 80% for training data and 20% for validation data. The next step is to use training data and validation.

The following is deep model training learning using CNN. Optimization is applied during training is Adams optimizer, Which is one method adaptive learning rate. Onthe model, Deep learning used the first layer CNN consists of a convolutional layer with the kernel size 5x5 and the number of filters is 32. The second layer of CNN consists of a convolutional layer with the size of the kernel of 5x5and the number of filters as many as 32 and a MaxPooling layer with a size of 2x2. The second Convolutional layer is used using kernel initializer and the ReLU activation function to make neurons that are convolutional the layer makes a selection so that it can receive useful signals from input data. After that, the MaxPooling layer added a dropout of 0.25 to prevent overfitting. The next layer is a Fully connected layer with the number of neurons as many as 256 and the ReLU activation function. After a fully connected layer, a dropoutof 0.5 is added to prevent overfitting.

The output layer to use has a softmax activation function. In the architecture used, only two convolutional layers are needed, because the results are generated from the conversion process to an ELA image can highlight the important features of knowing whether an image is original or has been properly modified.

4. CONCLUSION AND FUTURE WORK

We proposed CNN and Error Level Analysis (ELA) astwo main methods that are used in this project to detect tampered images. This project mainly focuses on identifying tampered images on social media sites. In our proposed method, the accuracy of tampered image detection is improvedsignificantly. We will further aim to improve the tampering- detection accuracy. In the future, we plan to add new methods which we believe will result in much higher accuracy in detecting tamperedimages.

5. REFERENCES

[1] Kunihiko Taya, Nobutaka Kuroki, Naoto Takeda "Detecting tempered images in jpeg images via CNN" 2020 18th IEEE International New Circuits and Systems conference.

[2] Prasenjit Maji, MoumitaPal, Riya Shil "Image Tampering Issues in Social Media with Proper Detection" 2020 8th International Conference on Reliability.

[3] Jitendra Ravan, Dr. Thanuja "Image Forgery Detection against Forensic Image Digital Tampering", 2018 International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)".

[4] Kejun Zhang, Yu Liang, Jianyi Zhang, Zhiqiang wang "No One Can Escape: A General Approach to Detect Tampered and Generated Image"2019 IEEE conference.

[5] Chaitra. B, P.V Bhaskar Reddy "A Study on Digital Image Forgery Techniques and its Detection" 2019 International Conference on Con- temporary Computing and Informatics(IC3I).

[6] Sandeep Kaur, Prof. Alka Jindal "Singular Value Decomposition (SVD) based Image Tamper Detection Scheme" International Conference on Inventive Computation Technologies (ICICT-2020).

[7] Amrutha S, Dr. Manju Manuel "Blur Type Inconsistency Based Image Tampering Detection" International Conference on Trends in Electronics and Informatics ICEI 2017.

[8] Ankita Meenpal, Dr. S. Majumder, Shubhangi Pandey "Digital Image Watermarking technique for tamper detection and restoration" 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T).

[9] S. S. Chaughule, D. B. Megherbi "A Robust, Non-blind High Capacity & Secure Digital Watermarking Scheme for Image Secret Information, Authentication and Tampering Localization and Recovery via the Dis- crete Wavelet Transform" 2019 IEEE.

[10] Quentin Bammey, Jean-Michel Morel "Automatic Detection of Demo- saicing Image Artifacts and its Use in Tampering Detection" 2018 IEEE Conference on Multimedia Information Processing and Retrieval.

