

Digital Image Sham Detection Using Deep Learning

Mr. Hemanth C¹, Ms. Divya A Srivathsa², Ms. Gouthami M³, Ms. Monica S⁴, Ms. Sarika B V⁵

¹ Assistant Professor, Dept. of Computer Science and Engineering, Maharaja Institute of Technology, Thandavapura

^{2,3,4,5} Students, Dept. of Computer Science and Engineering, Maharaja Institute of Technology, Thandavapura

Abstract - "Digital Image Sham Detection Using Deep Learning", Capturing images day by day as been increasing since there are availability of variety of cameras. Images as become a part in our daily lives because they contain an lot of information and sometimes it is also required to capture extra images to find additional information. This increases the grievousness and recurrence of fake image, which is now a major source of concern. A lot of customary techniques have been come into being over time to detect image falsification. In recent years, convolutional neural networks (CNNs) have come across much intentness, and CNN has also supremacy the field of image forgery detection. Even so, most image falsification techniques based on CNN that survive in the literature are limited to detecting a distinct type of sham . As a result, a technique capable of logically and well aimed detecting the presence of out of sight forgeries in an image is required.

Key Words: Image, Detection, CNN

1. INTRODUCTION

Now-a-days a handful of software are accessible that are used to exploit image so that the image is a look alike of the unedited. Images are cast-off as substantiate galley for any offence and if these image does not remain veritable then it will cause an issue. In this scientific era a large number of people have become casualty of image falsification.

A large number of people operate technology to modify images and use it as verification to mislead the court. Image manipulation is any type of operation that is accomplished on digital images by utilizing any software, it is also mentioned as image polish. So, to end to this, all the images that are allocated through social media should be designated as original or fraud errorless.

Social media is a huge party line to mingle, split and widen knowledge but if heedfulness is not employed, it can misguide people and even cause devastation due to unwitting false advocacy. Image tampering is a type of image falsification which return some content of an image with up to date content. If the up to date content is emulated from the same image itself then it is called copy-move tampering and if the up to date content is emulated

from non-identical image then it is known as image splicing.

1.1 Overview

Numerous methods have been uplifted in the literature to compact with image falsification. The large number of conventional methodology are based on specific artefact left by image falsification, whereas fresh techniques based on CNNs and deep learning were established, which are brought up below. First, we will mention the various orthodox techniques and then progress on to deep learning based techniques. It provides two level inspection for the image. At first level, it examine the image metadata. Image metadata is not that much authentic since it can be changed using effortless programs. But most of the images we come across will have nonchanged metadata which helps to figure out the changes.

1.2 Problem Statement

Since the innovation of photography, individuals and company have often look for paths to modify and manipulate images in order to defraud the viewer. Existing systems have worked on the contrast of image falsification identification methods, these are frequently narrowed in span and only weigh up alternate of the identical algorithm on images that are expressly fabricate for that type of routine. There are also shamed images which cannot be identified by the existing applications.

2. EXISTING SYSTEM

In existing forgery image detection system, it can be use to detect only limited type of image forgery like splicing and copy-move and not able to detect all types of forgery images.

Using new technologies any images can be forged with help of variety of tools available in the internet which makes impossible for humans to differentiate whether an image is forged or not.

Even with the help of complex neural network it is nearly impossible to determine forged or not.

3. PROPOSED SYSTEM

In this proposed system the application is able to detect whether an image is forged or not for all types of forged images like copy-move, splicing, tampering, morphing etc., here the application uses VGG16 and VGG19 algorithm and with the help of learning rate 0.0001 the VGG16 and VGG 19 algorithm gives 100% accuracy and for comparison purpose this system also uses error detection analyses also. The process how application works are

-First it will train the model using the provided datasets.

-Then in testing the user can choose one analyses type out of three and as to put an image for the test then the result is published in the form of Pie Chart.

The main advantage of this system is the user can clearly compare with each algorithm to check the image originality and then decide what to do with that image.

4. SYSTEM ARCHITECTURE

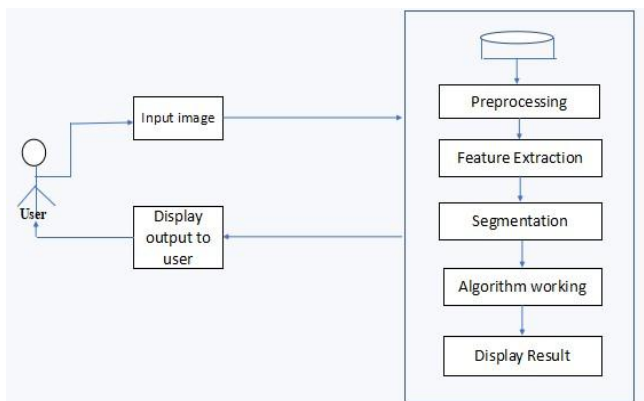


Fig-1 Architecture of Image Forgery

The system architecture defines the way how the system is designed. It also defines the relationship with other components and other aspects of software and reflects how it interacts with other systems and outside world. The architecture above describes the proposed system. It describes the way this system is developed and how it is connected to other components and the working flow of it.

5. Need of Digital Image Forgery Detection

The image forgery detection is very important nowadays because of rapid growth in the technology field there are many tools using which any one can tamper the original image and it will be very harmful if they use it in a bad way. So, it is very important to distinguish between authenticate image and the fake image which human cannot do it with their eyes. Image forgery detection is important in many aspects such as,

Maintaining Authenticity: Most of the images are often used as evidence in legal and investigative contexts as well as in journalistic and documentary contexts.

Preventing misinformation: In today's generation any image can be forged according to the needs and can spread false information for the society which is very dangerous. With the help of detection system this can be prevented.

Protecting Intellectual Property: Image forgery can also be used to steal intellectual property of an artist. Detecting image forgery can help protect the rights of the creator.

Overall, image forgery detection is essential for maintain the integrity of images and ensuring that they are used appropriately and accurately in a variety of contexts.

6. IMAGE FORGERY TYPES

The image may be forged either by adding, removing or replacing some regions in the original image with only one thing in mind that it leaves no visually detectable trace. The image can be forged by using several methods, these methods are commonly categorized

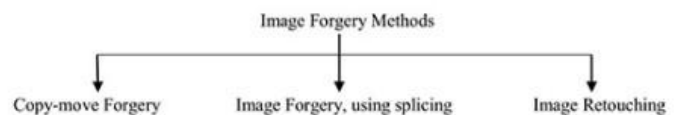


Fig-2 Types of Image Forgery

6.1 Copy Mover Forgery

Copy-Move Forgery means duplicating some part of the image and replacing in other part of the same image as shown in below figure. The intention of this is to conceal some part of the image information. It is the most usually utilized methods to forge an image. As the forged part of the image remains in the same image itself. Therefore, its detection is usually tough.



Fig-3 Effect of Copy Move Forgery and Image Retouching



(a) First Image (b) Second Image (c) Forged Image

6.2 Image Forgery, using retouching

It is the process of combining more than one image. The images are combined to make an altered image. It uses cut/copy paste operations. A bit of one image is taken and pasted onto some other image. In order to completely connect the cut/copied part of an image into another image as shown in the above figure, it need some additional postprocessing operations. The pasted portion alters the pattern of the image. Thus, analysis of image pattern helps in detection of image forgery.

7. ALGORITHM

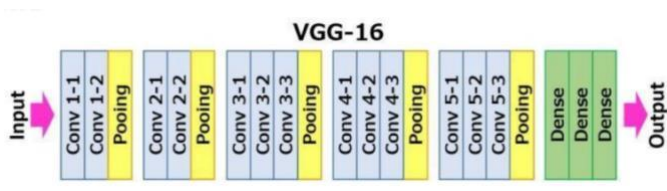


Fig-4 Convolution layers of VGG-16 Algorithm

Step 1:

Input Image: An image from the training datasets is taken.

Step 2:

Image Processing: Scale down the image pixel and convert them into numpy.

1. Filtering: Suppress the high frequency and smoothen the image.
2. Padding: To have zero padding so that the output does not differ from the input image.

Step 3:

Data preprocessed: Flipping the images vertically and horizontally.

1. 2D/3D convolution: To perform element wise multiplication.
2. Pooling: $(I_h - f + 1) / S * I_c$ (I_h - Image height, I_w - Image width, I_c - Number of channels in feature, f -filter, s Stride length)

Step 4:

Activation function: Based on the test cases it activates the model along with background verification.

Step 5:

Output: Predicts the image score whether the image is original image or forged.

Step 6:

End

8. MODULE DESCRIPTION

i. Tensor Flow

A free and comprehensive open-source software library for artificial intelligence and machine learning is called TensorFlow. The creation and training of machine learning models use it.

ii. Keras

The Keras high-level Python library runs on top of the TensorFlow framework and is small, simple to learn and effective. It is made with an emphasis on comprehending deep learning methodologies.

iii. PyQt

It is a python binding for Qt, a collection of libraries and development tools that offer abstractions for graphical user interfaces regardless of platform.

iv. Pillow [Pi]

All the fundamental image processing capabilities are available in the pillow library. It supports a wide range of picture file types for opening, editing and saving.

v. Epoch

The entire number of interactions of all the training data in one cycle for training the machine learning model is referred to as all the training data and is utilized all at once.

9. FLOWCHART

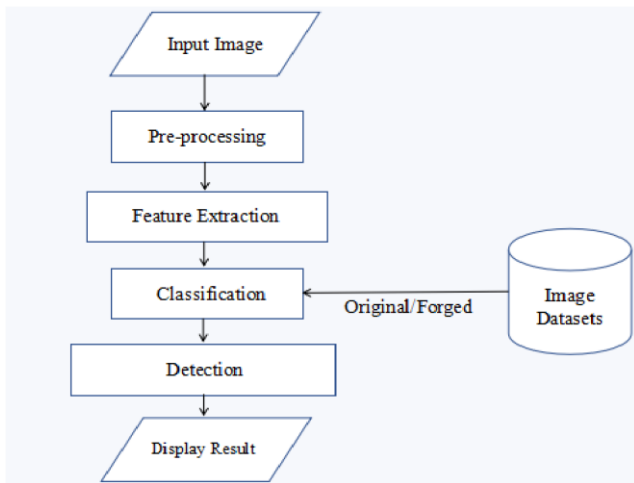


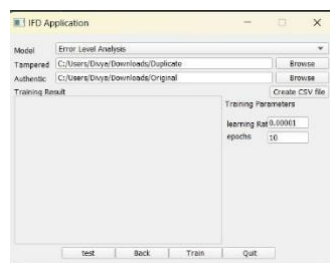
Fig-5 Flowchart of Image Forgery Detection

10. EXPERIMENTAL RESULTS

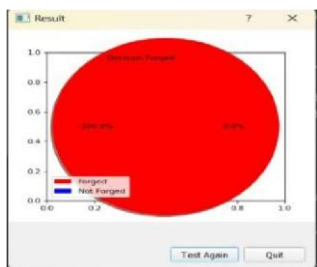
In this project we are majorly using VGG-16 and VGG-19 algorithm. The reason behind using these algorithms is that the accuracy of these two algorithms is too high in comparison to others. Also, this project delivers 98.8% accuracy to all the datasets provided. The results are shown as below.



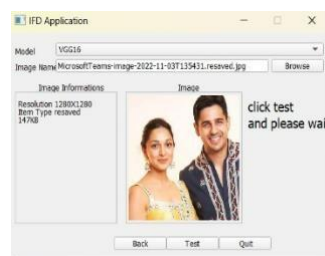
(a)



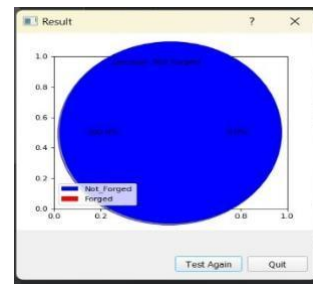
(b)



(c)



(d)



(e)

Fig-6 Snapshot Results of the Experiment

- (a) Window of Image Forgery detection.
- (b) Epoch for training datasets.
- (c) Result of training data.
- (d) Epoch for testing datasets.
- (e) Result of testing datasets.

11. CONCLUSIONS

In this study, multiple passive picture forgery detection methods were sketched out. A thorough examination of several forgery detection methods is also provided. In addition, this publication offers a variety of data sets that may be used with various forgery detection strategies. The primary shortcoming of currently available forgery detection methods is that they require human intervention in order to be detected. The failure of the procedures up to this point to distinguish between malicious and lawful tampering is another significant flaw in their design. Additionally, the discussed methods are only designed to detect the forgery type for which they were developed. Therefore, a comprehensive, reliable method to spot any kind of image forgery is required. A potential solution for digital picture forensics is proposed with the development of powerful artificial intelligence algorithms. Although deep-learning-based methods show promise, they lack the power to perform well in a number of digital image forensics applications. All of these parameters still require a lot of work to be done.

ACKNOWLEDGEMENT

We would like to give Prof. Hemanth.C, our project leader, our heartfelt appreciation for leading us through this project, for sharing his invaluable insights and recommendations with us, thus helping us better it beyond our wildest expectations. Secondly, we would like to express our gratitude to our project coordinators, Dr. Ranjit K. N. and Dr. HK Chethan, who continuously encouraged us and assisted us in completing this project within the allotted time frame. We also want to extend our sincere gratitude to our department's head, Dr. Ranjit KN, for giving us a venue to work on

