Image Forgery

Pratik Ramesh Hinge, Sneha Ambhore, Yogesh Ratnaparkhe, Kshitij Wadekar
Guide: Prof Sneha Ambhore
ADYPU
Charoli Bk.via Lohegaon,
Maharashtra , India

Abstract- In today's digital world there are many things which are being done online, as compared to the past. In this digital world, also the manipulation of images is getting increased which is called as Image Forgery. Image forgery has two types of techniques which is active protection and the other is passive protection. To understand between the fake and real image we need to invent various tools for it.

I. INTRODUCTION

Image is one of the most powerful tool in the way of communication. Many of the people around the world are editing there images using various free software available. As every coin has its two side one is head and other one is tail in the same way usage off image has its two sides. For processing images and photographs many different types of tools are being introduced. The use of Photoshop is mainly done in good or bad image direction. From the past images are one of the most main evidences and were also being used in the court but nowadays as the image forgery has increased, it is not a sufficient evidence. Tinkering the image is often believed as bad direction. Edited images are very difficult to be identified by the naked eye. I have prepared various techniques through which we can identify the image forgery. It has also removed our trust in the digital technology, it have made us think to trust in today's digital knowledge.

II. TYPES OF ATTACKS

a. Image Modification

This Image Modification is not considered as one of the most dangerous attacks as the reason is, it does not completely changes the image the only thing done it does is, they modify the image and add some grace to it. This type of image forgery is mostly applied by magazines and newspaper editors. The fact is this type of editing is ethically wrong.

b. Image Splicing or Photomontage

This technique is more different than image modification, in image modification the only thing you can do is modify the image but in image splicing/photomontage you have to cut the specific part of the image and and then you can add that part to another image as the part of its original one. When you look at the image it looks a bit original and it is hard to figure out the mistakes from it.

Fig . 1

As shown the e.g. 1 is the example of Image Splicing/photomontage. The image is of the war done in Hiroshima Nagasaki and the editor has replaced the people in the place of bombs. The editor has cropped the image from the other photo and then placed them in the place of bombs.

c. Copy Move attack

The copy move attack is one of the most commonly used attack and also one of the most difficult attack, like other attack this attack does not require any second image. This attack is done on the single image, the object/person is copied and pasted to the same image itself. The main intention of that image is to hide the original portion with some kind of the same image.

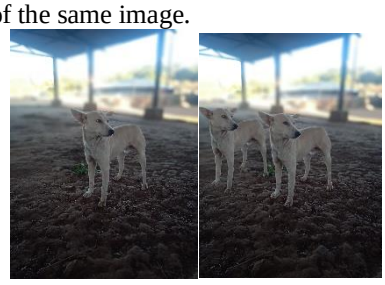

Fig.2:

In fig.2 the original picture is of the single dog, but in the given second box they have copied the same dog and have shown them, dogs this type of image editing is called as Copy Move attack.

III. IMAGE FORGERY DETECTION AND PREVENTION TECHNIQUES

a. SVM classifier

SVM classifier is mainly created for detecting the forged images. The detection of images is done on the regular basis by SVM classifier, this consists of two phases one is training phase and the other is testing phase. In training phase a database is being created and then it is tested with many number of images. The use of RSA key is made to check whether the user is authorized person or not. Many of the values are extracted and Pre-processing is done such as this is converted into gray scale from rgb. The SVM handles many sequence analysis such as handwriting, image classification and text.

The main functioning of the SVM classifier can be known when it is in the training step and these methods can be used in many main actions. Binary and multiclass targets are both designated with SVM. When there is suitable type of kernel function then only this type of mapping could be done.

b. Copy move forgery Detection Using pixel based approach

This is a type of algorithm which is based on the Pixel. Its functioning is done as dyadic wavelet image this form is applied to the input image. This form reduces the pixel form and the dimensions in it and then it divides them into sub images, with the help of pixel matching the copy move regions can be easily detected and later it calculates the difference between the the shifted image and the original image. In the end to improve the location Mathematical morphological operation are used.

1. The partition based copy move forgery detection approaches

In this copy move forgery detection there are block based approach which is defined below.

2. Block-based approach

Firstly on the provided images some pre-processing is done. Detection method uses merger which is of red, blue and green colors which operates on gray scale. To find out the forgery in the photo first we have to understand that the source and the target are both located in the same photo, at least two images must be exhibited from the forged image. It reduces the cost of the search by dividing it, the comparison of it is done on the block level.

IV. CONCLUSION

In this paper we have learnt that how the technology has made the editing of the photo easy. As with the help of technology many high resolution capturing devices are created. In them they can be categorized into two main groups' active and passive approaches which is based on the image faking. We have also discussed about three types of attacks which are image splicing, photomontage and copy move attack. In now days it is the need to trust in all images for the kind of image forgery.

V. REFERENCES

[1]. Mankar, S.K. and Gurjar, A.A., 2015. Image forgery types and their detection: A review. International Journal of Advanced Research in Computer Science and Software Engineering., 5(4).

[2]. Garg, T. and Saini, H., 2017. A Review on Various Techniques of Image Forgery Detection. vol, 4, pp.490-493.

[3]. Farid, H., 2009. Image forgery detection. IEEE Signal processing magazine, 26(2), pp.16-25.