ISSN 2348 – 9928
IJAICT Volume 5, Issue 5, May 2018 Doi:01.0401/ijaict.2015.11.11 Published on 05 (05) 2018

FORGERY IMAGE DETECTION

Saurabh Shinde *Neeraj Bansod* *Akshay Pawar* *Abhijeet Waghmare*

Computer Science and Engineering,
Marathwada Mitra Mandal's College of Engineering,
Pune, India.

Abstract*— The digital images play important role in the field of information forensics and security, also there uses are increased. So it was needed to create forensic techniques capable of detecting image frame alteration operations and forgery image. A number of image processing operations including Contrast Enhancement, histogram equalization are equivalent to pixel value mappings. In this paper, results show that pixel value mappings leave behind statistical traces, which we will refer to as a mapping's intrinsic fingerprint, in an image's pixel value mapping histogram. We also represent the forensics methods for detecting applied contrast enhancement and method for detecting histogram equivalence in image by identifying the features of each operations intrinsic fingerprint. In the end, by performing a number of simulations, so we get the efficiency of each proposed forensic technique.

Keywords*— Histogram Equalization, Contrast Enhancement, Image, Processing, Additive Noise, Digital Forensics, Intrinsic Fingerprints.

I. INTRODUCTION

Now a day there is lot of work takes place on digital image processing in society. Many governmental, legal, scientific, and news media organizations are depend on digital images to make critical decisions or to use as photographic evidence of specific events. At present, an image forger can easily change adigital image in a visually realistic way. To avoid both embarrassment and legal aspects, many of these organizations now require some means of identifying image alterations and verifying the image authenticity.

Fig 1 : Tthe original image from which an object is cut

On the basic of results come out, the field of digital image forensics has been discover. The primary goals of image forensics are the identification of images and image regions which comes under some form of manipulation or alteration. Because of the poor posed nature of this problem. There is no universal method of detecting image forgeries exists. Instead of that, there are number of techniques have been used to identify image alterations under a variety of scenarios. While each of these methods have their own limitations, it has been posited that if a large scales of forensic techniques are developed, it will be difficult for a forger to create an image capable of fooling all image authentication techniques.

II. RELATED WORK

Absence of Color Filter Array (CFA) detection of lighting angle inconsistencies [2]-[3], interpolation-induced correlations [4] has dealt with the previous image forensic work. These methods can be used in detecting the image forgery. Previous work which has been dealt with the identification of image modification by detecting operation specific fingerprint include the detection of re-sampling, double JPEG compression [3]-[4]. There will be limitations in each of these methods. Detection of inconsistencies in chromatic aberration also the absence of CFA interpolation induced correlations. Though these methods detect forgery images but they are unable to detect the image regions. Through this method, we can analyze the region in which the forgery has been done.

III. MOTIVATION

Due to enhancement in image processing software, it has now become very easy to forge the digital images. Many times we need to check the authenticity of digital images (For Example: IT Companies need scanned copies of documents).People is not aware how to detect the forged images and the part of image on which the forgery is performed. So the basic aim of this paper is

to illustrate techniques which will help to classify between real and forged images. The scope of paper not only limits up to detecting forged images but also helps to determine the part of image which has been forged.

IV. PROPOSED WORK

4.1 Detecting global contrast enhancement

Contrast enhancement techniques can be viewed as non linear pixel mapping introducing artifacts into histogram of the image. Almost the entire contrast enhancement techniques can be viewed as a nonlinear pixel value, followed by quantization. A non linear pixel value mapping can be separated into various regions where the pixel value mapping is locally contractive.

The contract pixel value mappings can map multiple different input pixel values to the same output pixel value, result is the addition of the sudden peak to an image histogram. Also, contractive pixel value mappings can cause mapped output pixel values to skip over, so results in gaps in contrast enhancement which is used to perform detection.

Now we have to calculate a modified histogram g(l) by computing the multiplication between h(l) and a pinch off function p(l). So we get,

$$g(l)=p(l)h(l)$$

Where p(l) is the pinch off function, h(l) is the high frequency component. G(k) is discrete Fourier transform of g(l).

Now we have to calculate E, a ―normalized measure of the energy in the high frequency components of the pixel value histogram from g(l) according to the formula

$$\text{Energy}=\begin{cases}\frac{1}{N}\sum_{k} |a(k)G(k)|, & c \le k \le 128 \\ 0, & else\end{cases}$$

Where c varies from 32 to 112. After calculation of E, we use the decision rule δ_c to classify an image as contrast enhanced by using μ_c threshold value like following:

Fig 2 : The original image onto which the cut object is pasted

4.2 Detecting locally contrast enhancement

The forensic technique can be extended into a method of the forgery image detection that can be used to locate regions in image that can be performed by selecting a set of pixels comprising a region of interest and then apply the test. To make this possible, the image can be divided into some fixed size blocks, where each of them constitutes a separate region of interest. Detection can be performed on each block individually and the results can be aggregated to identify image, image regions which show the evidence of locally applied contrast enhancement.

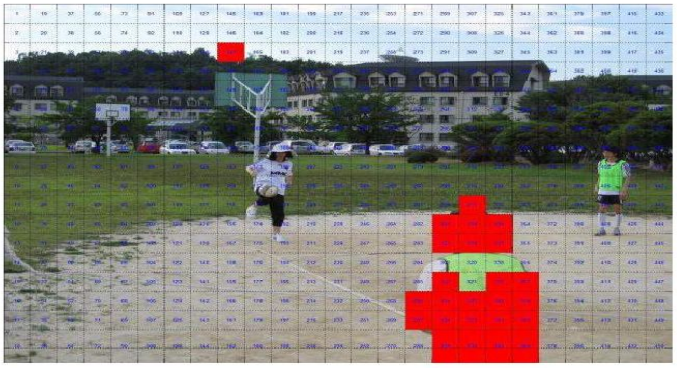

Fig 3 : The composite image

4.3 Detecting Histogram Equalization

To enhance contrast, Histogram equalization is used. It is not compulsory that contrast will always be enlarge in this. In some cases were histogram equalization cannot be good. In that case the contrast is reduced.

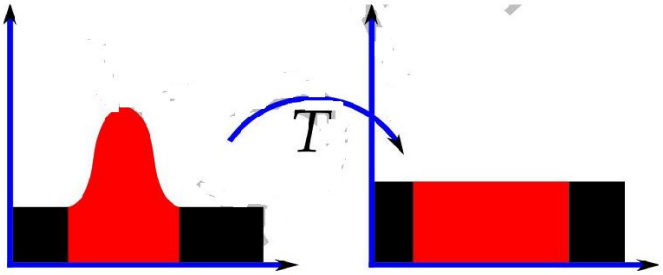

Fig 4 : Result- Forged Part This method is similar to Global Contrast Enhancement detection but here we consider only some part of image.

Contrast enhancement operation, Histogram equalization introduces sudden peaks and sudden gaps into histogram of an image. A particular set of traceable outputs are left behind in addition to those performed previously, If contrast enhancement is implemented using histogram equalization. To know what these outputs are, we first briefly explain how Histogram equalization is implemented. Histogram equalization highly expands the dynamic range of an image's Pixel values that is approximately uniform. First, we have to calculate the frequency domain measure of the distance (D), it is the distance of image normalized histogram and the uniform distribution, after this calculation, using this distance (D), we conclude whether the image has undergone histogram equalization or not.

V. CONCLUSION

In this paper, we are introducing the local and global contrast enhancement technique. Identification of such type of enhancement is take place by using histogram equalization and globally added noise to a previously in image. In each of these techniques, detection takes place on the basic of the presence or absence of an intrinsic fingerprint introduced into a histogram by a pixel value mapping We are defining the intrinsic fingerprint which a mapping leaves in the histogram of an image's pixel values. We propose a technique which detects the globally added of noise to a previously JPEG-compressed image by searching for the intrinsic fingerprint of a specific pixel value mapping applied to the image in question. Through such simulations, we tested the effectiveness and workability of each of the proposed forensic techniques. Our simulation results give that aside from exceptional cases. These all of the introduced forensic techniques are very useful tools for identifying image manipulations and forgeries.

References

[1] Matthew C. Stamm, Student Member, IEEE, and K. J. Ray Liu, Fellow, IEEE, Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints, IEEE transactions on information forensics and security, vol. 5, no. 3, september 2010

[2] M.K.Johnson and H.Farid, Exposing digital forgeries by detecting inconsistence in lighting, in proc. ACM Multimedia and security workshop, New York, NY, 2005,pp. 1-10.

[3] J.Lukas,J.Fridrich, and M.Goljan, ―Nonintrusive component forensics of visual sensors using output image, IEEE Trans. Inf . Forensics Security, vol. 2, no, 1,pp.91-106,Mar,2007.

[4] M.K. Johnson and H.Farid, ― Exposing digital forgeries through chromatic aberration, in Proc. ACM Multimedia and Security Workshop, Geneva, Switzerland, 2006, pp. 48-55.