ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Image Forgery Detection Based on Illumination Inconsistencies

Shraddha Asati, Rajesh Nasare, Hemant Turkar,

M. Tech Student, Dept. of CSE, Rajiv Gandhi College of Engineering and Research, Nagpur, India

Assistant Professor, Dept. of CSE, Rajiv Gandhi College of Engineering and Research, Nagpur, India

Assistant Professor, Dept. of CSE, Rajiv Gandhi College of Engineering and Research, Nagpur, India

ABSTRACT: Photographs are used to represent real-world events. Today many powerful image editing software's like Gimp, Photoshop etc. are available. Any kind of images can be manipulated by using these software's. Image composition or splicing is one of the important image manipulation technique. Sometimes these manipulated images are provided as evidence in court and this may cause serious problems. So it is important to check whether the images available are forged or not. So based on the challenges of forgery detection here a new method is proposed which incorporates the illumination inconsistencies for detecting forged images. Illumination inconsistency is due to the fact that while creating a forged image it is difficult to achieve proper illuminant condition for the entire image.

KEYWORDS: Illuminant color, wavelet packet decomposition, grey world algorithm, illuminant map, splicing.

I. INTRODUCTION

Every day, millions of digital images are produced by different devices and distributed through newspapers, televisions and websites. In all these information channels, images are a powerful tool for communication. But, it is not difficult to use computer graphics and image processing techniques to create forged images, it is important to check whether these images available in information channels are forged or not. Image Forgery deals with creating fake images or manipulating images. The process of creating forged images is becoming simple with the introduction of powerful image editing software's such as Adobe Photoshop, GIMP, Corel Paint Shop etc, some of which are available for free [1]. These software's help to create forged images without leaving any visual clues. Such forged images are sometimes provided as evidence in court also. This may create many serious problems. So it is important to have an accurate detection techniques for identifying these forged images.

Figure 1: Example of a Forged image

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Image composition or splicing is one of the important manipulation techniques [2]. This technique involves a composite of two or more images which are combined to create a composite forged image [2]. Figure 1 shows an example of a forged image. In this picture 'the shark' image is copied to base image 'helicopter rescue'. Before pasting 'the shark' image, the base image is flipped horizontally, to make the image more convincing. While assessing the authenticity of an image, forensic investigators use all available sources of evidences such as color filter array artifacts [4],inconsistencies in chromatic aberrations [5], inconsistencies in sensor noise, inconsistencies in camera response function[, inconsistencies in statistical features , jpeg inconsistencies , inconsistencies in illuminant color etc.

Among other evidences, illumination inconsistencies are potentially effective for splicing detection. Illumination inconsistencies occur in a forged image because, for a manipulator proper adjustment of the illumination conditions is difficult to achieve while performing forgery The previous methods based on illumination inconsistencies concentrates on region based approach i.e. their method can be applied to image with faces only. Also they use a single algorithm for illuminant color estimation. So their accuracy is low. So in this work in order to improve accuracy, illumination inconsistencies are combined to produce a new technique for image forgery detection.

II. RELATED WORK

Different methods have been developed for forgery detection based on different evidences of tampering. But these available methods in digital image forensics does not provide complete forgery detection. Each method has certain drawbacks. Some of the methods are discussed below. Lukas *et.al.* used sensor pattern noise to detect digital image forgeries. This method was based on detecting the presence of the camera pattern noise in individual regions in the image. Sensor pattern noise is a unique stochastic characteristic of imaging sensors. The tampered region is the one that lacks the pattern noise. The disadvantage of this method is that the method is only applicable when the camera used is known or other images taken by the camera is known. T.Bianchi and A.Piva proposed another method to discriminate original and forged regions in JPEG images. He believed that the forged region of jpeg image undergoes double jpeg compression. So the DCT coefficients of modified areas will contain double quantization artifacts.

These double quantization artifacts can be used for identifying forged regions. This method is applicable only when both the original and tampered images are stored in jpeg format. Mahdian and Saic used periodic properties of interpolation caused by resampling for tampering detection [3]. To create a composite image it is often necessary to resize, or stretch certain portions of image. This requires resampling the image into a new sampling lattice. This introduces specific correlations between the neighbouring pixels. These correlations are used to detect image manipulation. The detection performance decreased as the order of interpolation polynomial increased. Riess.C.Angelopoulou proposed a method based on illumination inconsistency. This method is based on the fact that the illuminant color of images taken under different lighting conditions will be different. They first estimate then illuminant color locally per segment. Then each region is colored according to its local illuminant estimate to obtain illuminant map. Then an expert is left with the difficult task of visually examining an illuminant map for evidence of tampering. Xuemin Wu and Zhen Fang proposed another method based on illumination inconsistency to identify forged images. In this method, first the image is divided into various blocks and illuminant color is estimated for each image block. Then the difference between estimated and reference illuminant color is compared against a threshold to identify whether the image is tampered or not. The drawback of this method is that accuracy is low for this method. This paper is organized as follows. Section II contains the detailed block diagram of the developed forgery detection system and its explanation. Section III is completely devoted to presenting and analyzing the simulation results. Finally, conclusion is stated in Section IV.

III. PROPOSED ALGORITHM

The proposed image forgery detection method is based on illumination inconsistencies. This is based on the fact that the illuminant color of images taken under different lighting conditions will be different. So while creating a spliced image it is hard to achieve proper adjustment of illumination conditions. So inconsistency in illuminant color can be

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

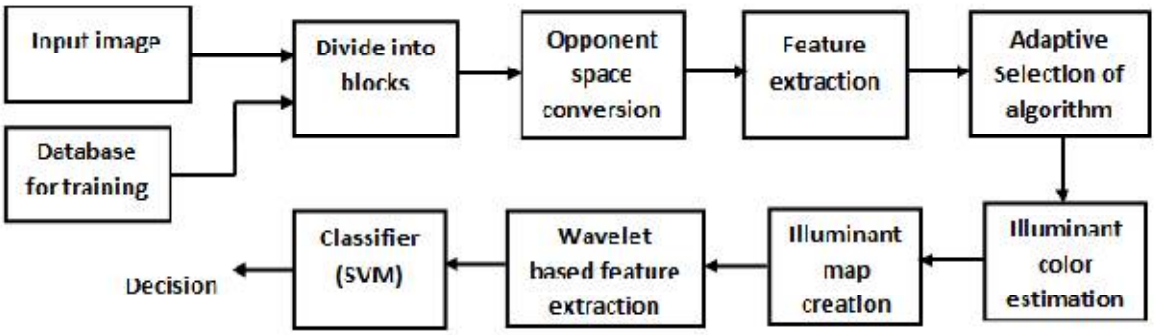
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

used as an evidence of image forgery. This produces specific correlations into the image. These correlations can be used as an evidence of image forgery.
The block diagram for proposed image forgery detection system is shown in figure 2.In the image forgery detection is done based on illumination inconsistencies. The output of the detection method is combined to obtain the final decision i.e whether the image is forged or not.



The block diagram for proposed image forgery detection system is shown in figure 2.

Here a color image is first divided into many non overlapping sub blocks. The block size is taken as 32 * 32. This is because when block size increases the location accuracy decrease and when block size increases the angular error increases. Angular error is the error between true and estimated illuminant color. Since for a color image, the R, G, and B channels are highly correlated each block is transformed into an opponent color space called HSV color space before feature extraction. Then from the opponent color space block features are extracted. The extracted features include contrast and mean values. Contrast is the difference in luminance or color that makes an object distinguishable. The contrast value for each block can be calculated by finding the standard deviation of pixel values of corresponding block. The mean value for each block can be calculated by finding the average grey level of pixel values of corresponding block. Based on the values of extracted features, proper illuminant color estimation algorithm is selected for each block.

The illuminant color estimation algorithms include grey world algorithm, first order grey edge algorithm and second order grey edge algorithm. For blocks having low value of contrast and texture first order Grey Edge algorithm is used for illuminant color estimation. For blocks having high value of contrast and texture second order Grey Edge algorithm is used for illuminant color estimation. And for all other blocks i.e. having high value of contrast and low value of texture or having high value of contrast and low value of texture, Grey World algorithm is used for illuminant color estimation. The three algorithms are incorporated into a single framework as shown below.

$$e(n, p, \sigma) = (1/k) \left(\int\int \left| n f_{\sigma}(x, y) \right|^{p} dx\, dy \right)^{p} \quad (1) \qquad (1)$$

where *n* is the order of the derivative and *p* is the minkowski norm. The derivative is defined as convolution of the image with the derivative of a Gaussian filter with scale parameter s. The Grey-World algorithm, first-order Grey-Edge and second order Grey Edge is equivalent to e (0, p, 0), e (1, p, s) and e (2, p, s) respectively. After estimating the illuminant color for each block the next stage is to create an illuminant map for the image. This is done by recoloring each block of the image with its estimated illuminant color. This produces an intermediate representation called illuminant map.

Then texture features are extracted from the illuminant map using wavelet based texture descriptor. Tree structured wavelet or wavelet packet decomposition provides a rich range of possibilities for texture analysis. In wavelet packet decomposition both low pass sub images and high pass sub images are further decomposed into low pass and high pass

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

sub images. This is based on the fact that dominant frequencies of textured images do not only lie in the lower resolution band, but also in the middle band as well. Figure 3 shows two level wavelet packet decomposition. Textural information can be extracted from the transformed coefficients. Extracted information includes mean and standard deviation.

The mean and standard deviation for each block provide feature vector for that block. Then feature vector for each block is then fed to the classifier. The classifier has two stages a training stage and a testing stage. In the training stage, the classifier is trained for different real and forged images in the data base. In the testing stage the classifier select appropriate class for each test image based on the training data.

IV. SIMULATION RESULTS

Results for Illumination based forgery detection . The simulation results are given below. Figure 3 shows the input image. The image is a jpeg image having size450*356*3.

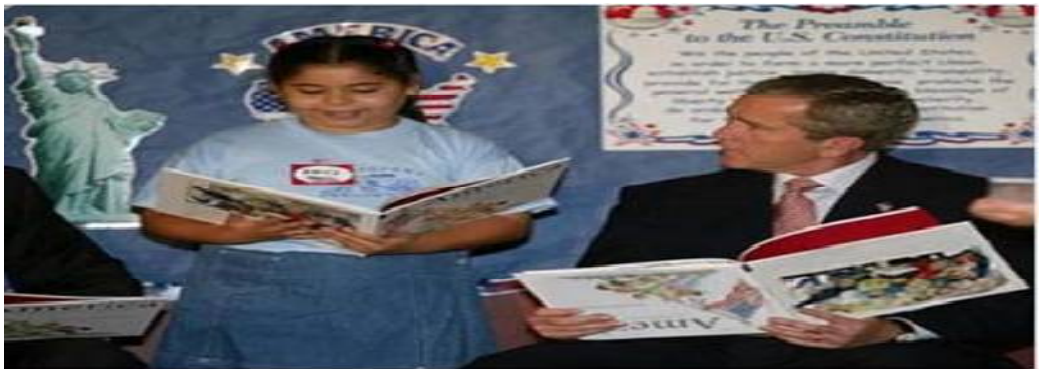


Figure 3 : Input image

The input image is first divided into non overlapping sublocks of size 30×30. Then image blocks are converted into an opponent color space called HSV as shown in figure 4.

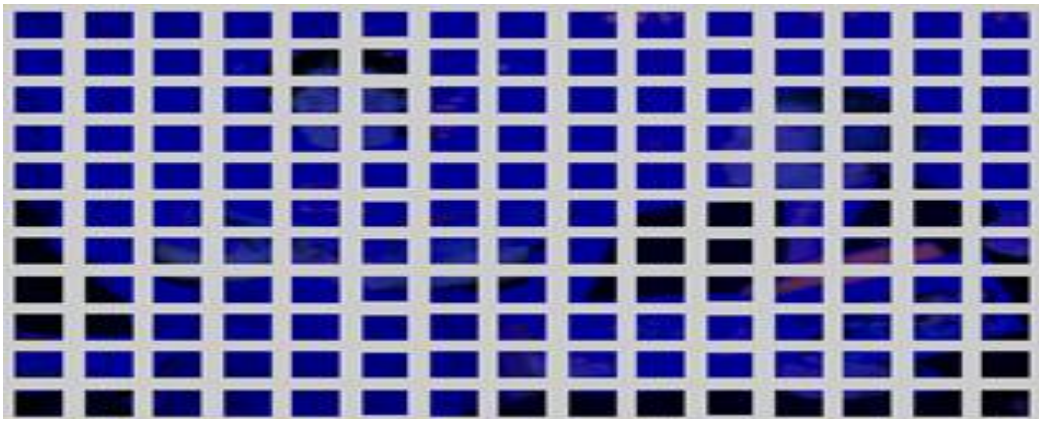


Figure 4: Input image blocks in HSV color space

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Statistical texture features such as contrast and average grey level are on the calculated for each sub block. Based extracted texture features, illuminant color for each block is estimated using appropriate algorithm. Then each block is recolored with the estimated illuminant color for that block. The illuminant map thus obtained is shown in figure 4.

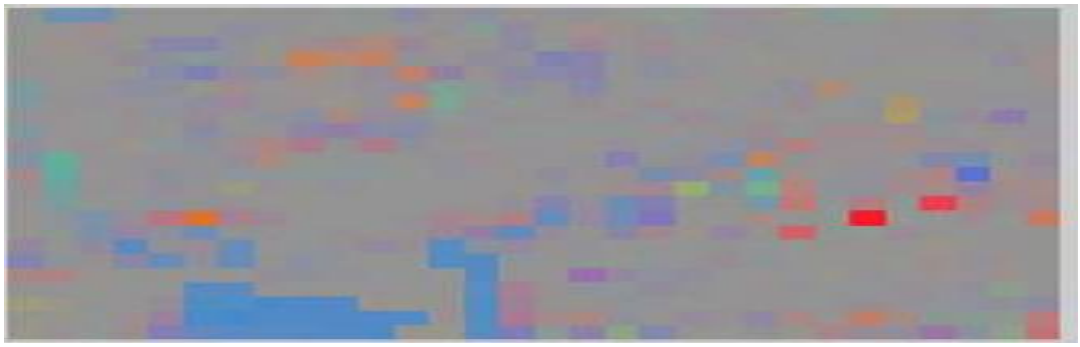


Figure 5: Illuminant map for the input image

Wavelet based features are extracted from the illuminant map and the feature vector obtained is fed to the SVM classifier. The output of classifier is either 1 or -1. Output=1denotes image is real and output =-1 denotes image is forged.

V. CONCLUSION AND FUTURE WORK

Image forgery deals with creating fake images or manipulating images. Due to the advanced technologies in image editing software image forgery is becoming more difficult to identify. This is because with the help of these software image forgery can be created without leaving any visual clues. So based on the challenges of forgery detection here a new method is proposed which uses illumination inconsistencies and for detecting forged images. This method overcomes drawbacks of previous methods and provides accurate results. This method can be used in forensic and medical applications to check genuinity of images.

REFERENCES

[1] Carvalho, C. Riess, E. Angelopoulou, H. Pedrini and A. R. Rocha, "Exposing Digital Image Forgeries by Illumination Color Classification," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 7, pp. 1182–1194, Jul. 2013.

[2] A. Rocha, W. Scheirer, T. E. Boult, and S. Goldenstein, "Vision of the unseen: current trends and challenges in digital image and video forensics,"*ACM Comput. Surveys*, vol. 43, pp. 1–42, 2011

[3] A.Popescu, H.Farid, "Exposing digital forgeries in color filter array interpolated images," *IEEE Transactions on Signal Processing*, vol.53, no.10, pp.3948–3959, 2005

[4] M.Johnson, H.Farid, "Exposing digital forgeries through chromatic aberration," in *Proc. of the 8th workshop on Multimedia and security*, pp. 48–55, 2006

[5] J.Lukas, J.Fridrich, J.M.Goljan, "Detecting digital image forgeries using sensor pattern noise,"*Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, vol. 6072, pp. 362–372, 2006

BIOGRAPHY

Shraddha Asati is a Student of Mtech in the Dept. of CSE, Rajiv Gandhi College of Engineering and Research, Nagpur, India. Her research interests are Image Processing for forgery detection etc.