IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 4, April 2015
ISSN: 2394 - 6598
www.ijetie.org

DEPICT FORGED IMAGE USING COLOR CLASSIFICATION TECHNIQUE

Nilima J. Khatale
Sir Visvesvaraya
Institute of technology,
Nashik
nilimakhatale.nk@gmail.com

Monali B. Ghumare
Sir Visvesvaraya
Institute of technology,
Nashik
monaghumare18@gmail.com

Dipali V. Jachak
Sir Visvesvaraya
Institute of technology,
Nashik
jachak.deepali@yahoo.com

Bhagyashri S. Padhyar
Sir Visvesvaraya
Institute of technology,
Nashik
bhagyashri2513@gmail.com

ABSTRACT

In the day to day life the techniques are increasing with related to photographics. This paper performs exposing digital forgeries images and extracting same pair of feature of face framework using the color classification approach. The framework aims to exposing forgery image or object from the given input image of willing without any user interaction or the use of any training data automatically. To expose forged part from the any modified or either any image, the preffered method for that dence local illuminationfrom the image. Our Proposed work does not require any prior knowledge on the object of interest or any interaction from the user. As another technology that we are used i.e face exractioncor to detect same pair of face features from the input image. This can realize the based on the information of color consistency of each object or the main attribute from the image object. Experiments reveal the advantages of using the face recognization using color classification.

General Terms

Illumination Map Estimation(IE)-

In the dence local estimation the color extracted from the image and each region from the iamge is colored with the extracted illuminant color. Before that the regions are segmented into homogenious regions. And new iamge is created as per above applying above method. After that the final resulting images calles illumiant map(IM). Also called dence local illumination of image.

Features extracting from face-

Process that require human interaction to set the boundry box out of human face present in tha input iamage.(simply clicking on two corners of the bounding box). After boundry setting crop every bounding box out of each illuminant map. So resulting image is only face regions are remains.

Same Feature of face -

Detecting same feature of face from the image. We use SASI and HOGedge descritors capture different properties of the face region.

Classification-

Classifying features vector we use the machine learning approach.

Keywords-

Forgerd image detection, Dence local illumination, color consistency, based on color classification, face extraction, pair face feature, classification

1. INTRODUCTION

This paper describes the strategy followed by various techniques to tackle with Image Forensics Challenge on image forgery detection. Several authors have been working in recent years on the forgery detection problem, focusing on techniques based on camera sensor noise, and on techniques based on dense local descriptors and machine learning. Therefore, For detection we decided to follow both these approaches, on two separate lines of development, with the aim of combining decisions at some later time of the process. Indeed, it is well known that, given the different types of forgery encountered in practice, and the wide availability of powerful photo-editing tools, several detection approaches should be used at the same time and judiciously merged in order to obtain the best possible performance. Based on this consideration, we also followed a third line of development working on a technique for copy move forgery detection which, although applicable only to a fraction of the image set, provides very reliable results. Unfortunately it was very soon clear that the PRNU-based approach[1] was bound to be of little use. Lacking any information on the cameras used to take the photos, we had to cluster the images based on their noise residuals and estimate each camera's PRNU based on the clustered images. However, more than 20% of the test images could not be clustered at all and in some cases the number of images collected in a cluster was too small to obtain a reliable estimate of the PRNU. On the contrary, techniques based on dense local descriptors appeared from the beginning very promising, and we pursued actively this line of development, drawing also from the relevant literature in the stegano-analysis field.

Images and videos have become the main information carriers in the digital era and used to store real world events. The significant possible of visual media and no trouble in their storage, division and acquisition is such that they are more and more exploited to pass on information. But digital images are easy to influence because of the availability of the sophisticated digital cameras and powerful editing software.[2] Without leaving any evidence, Image processing experts can access and modify image content. Moreover, with the spread of low-cost user friendly editing tools the art of tampering and counterfeiting visual content is no more restricted to experts. As a result, the modification (manipulation) of images for malicious purposes is now more common than ever. At the beginning, the manipulation is simply improve the image's performance, then again many of us began to amendment the image's content, even to achieve their ends by these illegal and immorality strategies.

Supported on top of reasons, it's necessary to develop a reputable technique to discover whether or not a digital image is forge. During the process of digital image authenticity all the existing sources are used by forensic investigators of tampering evidence. The most effective sign for the detection of tampering is illumination inconsistencies as compared to other signs available. From the viewpoint of a manipulator, proper adjustment of the illumination circumstances is hard to achieve when creating a composite image [3].

In this paper we are taking the review of digital image forgeries detection and their different techniques .In section I, we are talk about illuminant inconsistencies.

I. Illumination Inconsistencies

In blind image forgeries exposure, investigation of image automatically is by its assessment of illuminant color consistency. Methods for illumination color estimation are machine-learning based. C. Riess and E. Angelopoulos in [4] presented a different approach by employing a physics-based color constancy algorithm that operates on partly reflective pixels. during this approach, the automated detection of extremely reflective half is unnoticed. The author implies to segment the image to estimate the illuminant color per segment. Recoloring every image region in step with its native illuminant estimate yields a suspected illuminant map. Unlikely illuminant color estimates point towards a influenced region. Unfortunately, the authors do not provide a statistical decision criterion for forgery detection. Thus, an expert is left with the difficult task of visually examining an illuminant map for evidence of tampering. Inconsistencies in illumination distribution can be used to identify original and doctored image.[5]

2. EXISTING SYSTEM

For the exposing forged image from the given input image we use color classification method in that dence local estimation, face extraction features are used. But befor that the some methods are introduced by,

Johnson and Farid proposed spliced image detection by exploiting specular highlights in the eyes.[6] In a subsequent extension, Saboia *et al.* automatically classified these images by extracting additional features, such as the viewer position. The applicability of both approaches, however, is somewhat limited by the fact that people's eyes must be visible and available in high resolution.

Gholap and Bora, introduced physics-based illumination cues to image forensics. This physics based illumination based on dichromatic reflectance model which authors examined inconsistencies in specularities. But specularity is very challenging approach on real-world images is challenging. Therefore, the authors require manual annotation of specular highlights.[7] Additionally, specularities have to be present on all regions of interest, which limits the method's applicability in real-world scenarios.

3. RELATED WORK

Formally there are two methods used to figure out the problem of detecting forged iamge i.e. geometry based and color based. Geometry based detecting inconsistancies in light source postions between object. And color based method work on inconsistancies in the object color and light color. As per Kobus Barnard proposed a context for testing calculating color constancy, he specify his approach to the implementation of a number of the leading algorithms, The algorithms chosen for close study include two gray world techniques, a limiting case of a edition of the Retinex process, several alternatives of Forsyth's gamut-mapping technique, Cardei *et al.*'s neural web technique, and Finlayson *et al.*'s Color by Correlation schemes. Author scrutinizes the ability of these algorithms to make estimates of three different color constancy quantities: the chromaticity of the picture illuminant, the overall corrected illumination invariant, and degree of that illuminant, and image. Author consider algorithm performance as a function of the number of surfaces in scenes generated from reflectance spectra, the relative consequences on the algorithms of added secularities, and the effect of subsequent clipping of the data.

Arjan Gijsenij proposed a technique for multiple light source Color constancy algorithms are commonly based on the simplifying hypothesis that the spectral distribution of a light source is uniform across picture. But, in reality, this hypothesis is often violated due to the presence of multiple light sources. In this paper, he were address more realistic scenarios where the uniform light-source assumption is too restrictive[8]. First, a technique is implement to broaden existing algorithms by applying color constancy regionally to image scraps, rather than globally to the complete image. After native (patch-based) illuminant estimation, these estimates area unit combined into additional strong estimations, and a native correction is applied supported a changed diagonal model. Quantitative and qualitative experiments on spectral and real pictures show that the given methodology reduces the influence of two light sources at the same time present in one picture. If the chromatic diversity between these two illuminants is more than 1 , the given framework outperforms algorithms based on the uniform light-source assumption (with error-reduction up to approximately 30%)[9]. Otherwise, when the chromatic difference is less than 1 and the scene can be considered to contain one (approximately) uniform light source.

4. PROPOSED SYSTEM

In the proposed work the aim is to automatically extract the forged object from input image which are taken by the freely working cameras. Along with that to extract face features and to show the result of pair face feature,whether it is same or not in the input image. In blind image forgeries exposure, investigation of image automatically is by its assessment of illuminant color consistency.[4][5] Methods for illumination color estimation are machine-learning based. Color is generally used in computer vision, but in a very fundamental, primitive way. One reason for utilizing very basic color primitives is that the color information of a pixel is always a mixture of illumination, geometry and object material. Consider, for example, changes in illumination, which are likely the spectrum of sunlight varies over the daytime, shadows can fall on the object, or fake light is switched on. Fig. 1 shows two examples for different color appearances. The pictures are element of the dataset. The picture is once exposed to comparatively neutral (white) light, and once to illuminants that approximate the surroundings light at night. Thus, for robustness, methodologies that make use of color be supposed to openly address such emergence variations. Two separate static methods to obtain a color illuminant: the statistical generalized gray world estimates and the physics-based inverse-intensity chromaticity space are as given below. Both schemes do not require training data and are applied to any image.

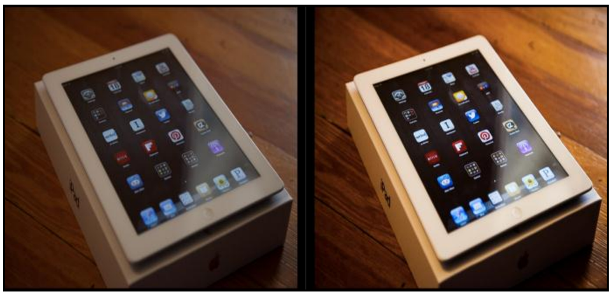


Fig. 1: Color Illumination.

Consider, above figure shows the result of illuminate color of image i.e. difference of illuminat color in the image. For the reading or scanning of input image we need image decode into binary values in the black and white color combination. The resulting image of black and white also know as gray scaled image as below[10].

Fig. 2: Gray scale input image.

For the gray world image generally we preffer difference between color consistency in the color model i.e. Red(R), Green(G), Blue(B)[11]. In this proposed system for calculating the gray scale value we require value of RGB model. The basically RGB color model values range is from 0 to 255 and if the clor pixel is near to 0 then whole part of same color set as black i.e. set binary '0' and if color pixel value is near to 255 then this particular part set as white i.e. binary '1'.

Using this gray scale, we can show the actual forged part by using filtering the original color from the image. And the forged part remains as it is in the output window. So we get propor forged part from the image.

For the actual forged calculation we need some algorithem as well as some attribute calculations. This calculation shows the absolute result.

5. MODULE DESCRIPTION

5.1 Illumination Map Estimation-

To calculate values for dence local illumination estimation we have to segmented image into homogeneous part called region. This regrions colord with the illuminant extracted color and formd map as a resultant image. This resulting image called illuminant map(IM)[12]. Using the algorithem the superpixel color of illuminant is estimated. We use separate illuminant color estimator (a) Gray scale estimates.

5.1.1 Compute Bilevel Images-

In photography, when we are computing bilevel image values basically we are consider RGB color model. A Bilevel digital image is an image in which value of each pixel is single sample that carries the intensity information of image[13].

Bilevel image is also known as binary world image or grayscale image. Bilevel image are reprent in black and white combination. For computing original image value we consider the length and width of the image and image is scanned or read with the pixel by pixel.

For e.g., Consider image as I,
Scannd I(image) upto its length and width.
Height =X
Width =Y
Getpixel(X,Y)

Using get pixel method get each pixel from I.
Conver into bilevel image,
New pixel= RGB/3

Using above technique we can easily compute the value of bilevel image.

5.1.2 High Pass Filter-

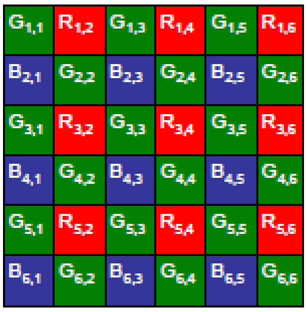
In the filtering techniques two types of filtering techniques are consider (A) high pass filter (B) low pass filter.

We use high pass filter technique in this proposed method. Both the filtering methods are same but only the difference is that the high pass consider the high illuminated color object and low pass filter is exactly oppite to high pass filter.

High pass filter mainly used to make image appear sharper. Such file emphasize fine details in the image[14].

To ensure image we apply this filtering method using following matrix.

Consider,



$G_{1,1}$	$R_{1,2}$	$G_{1,3}$	$R_{1,4}$	$G_{1,5}$	$R_{1,6}$
$B_{2,1}$	$G_{2,2}$	$B_{2,3}$	$G_{2,4}$	$B_{2,5}$	$G_{2,6}$
$G_{3,1}$	$R_{3,2}$	$G_{3,3}$	$R_{3,4}$	$G_{3,5}$	$R_{3,6}$
$B_{4,1}$	$G_{4,2}$	$B_{4,3}$	$G_{4,4}$	$B_{4,5}$	$G_{4,6}$
$G_{5,1}$	$R_{5,2}$	$G_{5,3}$	$R_{5,4}$	$G_{5,5}$	$R_{5,6}$
$B_{6,1}$	$G_{6,2}$	$B_{6,3}$	$G_{6,4}$	$B_{6,5}$	$G_{6,6}$

Fig. 3 pixel representation

The above matrix shows the representation of image pixel bye pixel. Using such representation we compute the high pass filter range.

$$\hat{g}(x,y) = \frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}\begin{bmatrix} g(x-1,y) \\ g(x,y-1) \\ g(x+1,y) \\ g(x,y+1) \end{bmatrix}$$

Using above calculation we find out the high intensity value of pixel. i.e. those pixel who have range greater than its decided range then it will consider as high point of that image. And after that this computed matrix multiply with another matrix as follow. Like this way we calculate the high pass filter value[15].

new matrix[]= { { -1, -2, -1,},
{ -2, 4, -2,},
{ -1, -2, -1,} }

The above matrix consider at the time of multiplication.

5.2 Face Extraction:

In this step we have to just set boundary box out of each face from image. Those face are selected by human interaction those face features are compiared with each other[16]. When the boundary box select out of face region the extra part or out of boundary box region area get cleard or only face reagion or selected object remains as it is. The following are the steps to perform in the face extraction module.

1) Select image I as a input image :
In that the input image is given by user those who are access this system. And this image consider as I. and then pass for further process.

2) Apply preprocessing algorithm :
At the time of scanning of image, each image having different size. At that time system require to resize that images those images are not in proper size as system required. That time system get resize image i.e. preprocessing of image.

3) Create box around human face :
It generate boundary box around face.

4) Crop the bounding box :
Remains only selected part within the boundary box.

5) Get the illumination of face :
After that finally user get output whether the face features are same or not.

5.2.1 Computation of Illuminant Features:

For all face regions, texture-based and gradient-based features are computed on the IM values. Each one of them encodes complementary information for classification.[4][5]

5.3 Paired Face Features:

Our goal is to assess whether a pair of faces in an image is consistently illuminated. For an image with faces, we construct joint feature vectors, consisting of all possible pairs of faces.[16]

5.4 Classification*:*

We use a machine learning approach to automatically classify the feature vectors. We consider an image as a forgery if at least one pair of faces in the image is classified as inconsistently illuminated.

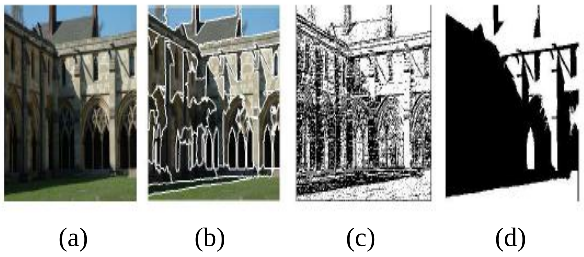


Fig. 4: Example of forged image detection. (a) Original image. (b) illuminant map (c)high pass filter (c) bilevel image.

6. ACKNOWLEDGMENTS

We extend our thanks to Prof.G.J.GAGARE, Our guide, for providing us the opportunities & facilities and inspiration, gather professional knowledge and material to complete this project, without which it would have been impossible to complete this hard task.

7. REFERENCES

[1] 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.

[2]C.Riess and E. Angelopoulou,“Scene illumination as an indicator of image manipulation,” Inf. Hiding, vol. 6387, pp. 66–80, 2010.

[3] H. Farid and M. J. Bravo, “Image forensic analyses that elude the human visual system,” in Proc. Symp. Electron. Imaging (SPIE), 2010, pp. 1–10.

[4] Y. Ostrovsky, P. Cavanagh, and P.Sinha, “Perceiving illumination inconsistencies in scenes,” Perception, vol. 34, no. 11, pp. 1301–1314, 2005.

[5] H. Farid, A 3-D lighting and shadow analysis of the JFK Zapruder film (Frame 317), Dartmouth College, Tech. Rep. TR2010–677, 2010.

[6] M. Johnson and H. Farid, “Exposing digital forgeries by detecting inconsistencies in lighting,” in Proc. ACM Workshop on Multimedia and Security, New York, NY, USA, 2005, pp.1–10.

[7] M. Johnson and H. Farid, “Exposing digital forgeries in complex lighting environments,” IEEE Trans. Inf.Forensics Security, vol. 3, no. 2, pp. 450–461, Jun. 2007.

[8] M. Johnson and H. Farid, “Exposing digital forgeries through specular highlights on the eye,” in Proc. Int.Workshop on Inform. Hiding, 2007,pp. 311–325.

[9] E. Kee and H. Farid, “Exposing digital forgeries from 3-D lighting environments,”in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Dec. 2010, pp. 1–6.

[10] W. Fan, K. Wang, F. Cayre, and Z. Xiong, “3D lighting-based image forgery detection using shape-

from-shading," in Proc. Eur. Signal Processing Conf. (EUSIPCO), Aug. 2012, pp. 1777–1781.

[11] J. F. O'Brien and H. Farid, "Exposing photo manipulation with inconsistent reflections," ACM Trans. Graphics, vol. 31, no. 1, pp. 1–11, Jan. 2012.

[12] S. Gholap and P. K. Bora, "Illuminant colour based image forensics," in Proc. IEEE Region 10 Conf., 2008, pp. 1–5.

[13] X.Wu and Z. Fang, "Image splicing detection using illuminant color inconsistency," in Proc. IEEE Int. Conf. Multimedia Inform. Networking and Security, Nov. 2011, pp. 600–603.

[14] P. Saboia, T. Carvalho, and A. Rocha,"Eye specular highlights telltales for digital forensics: A machine learning approach," in Proc. IEEE Int.Conf. Image Processing (ICIP), 2011, pp. 1937–1940.

[15] C. Riess and E. Angelopoulou,"Physics-based illuminant color Estimation as an image semantics clue," in Proc. IEEE Int. Conf. Image Processing, Nov. 2009, pp. 689–692.
.

[16] Tiago José de Carvalho,Christian Riess, Elli Angelopoulou, Hélio Pedrini, and Anderson de Rezende Rocha, Exposing Digital Image Forgeries by Illumination Color Classification",IEEE Transactions on Information Forensics and Security,Vol. 8, No. 7, July 2013

[17] K. Barnard, V. Cardei, and B. Funt, "A comparison of computational color constancy algorithms–Part I: Methodology and Experiments With Synthesized Data," IEEE Trans. Image Process., vol. 11, no. 9, pp. 972–983, Sep. 2002.

[18] A. Gijsenij, R. Lu, and T. Gevers,"Color constancy for multiple light sources," IEEE Trans. Image Process., vol. 21, no. 2, pp. 697–707, Feb. 2012.

[19] Andrew C. Gallagher, Tsuhan Chen "Image Authentication by Detecting Traces of Demosaicing"

[20] Giovanni Chierchia, Giovanni Poggi,Carlo Sansone, and Luisa Verdoliva, "A Bayesian-MRF Approach for PRNU-Based Image Forgery Detection" IEEE Transactions on Information Forensics and Security,Vol. 9, No. 4, April 2014

[21] Jiayuan Fan, Hong Cao, and Alex C. Kot, "Estimating EXIF Parameters Based on Noise Features for Image Manipulation Detection " IEEE Transactions on Information Forensics and Security,Vol. 8, No. 4, April 2013