International Journal on Emerging Technologies (Special Issue on *RTIESTM-2016*) **7**(1): 175-178(2016)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Digital Image Tampering Detection Based on Illumination Inconsistency: A Review

Gurleen Kaur*, Rupinder Kaur** and Kanwaljeet Kaur***
**Department of CSE & IT , B.BSCET, Fatehgarh Sahib, (Punjab), INDIA*
***Assistant Professor, Department of EE, Engg. , A.I.E.T, Faridkot, (Punjab), INDIA*
****Assistant Professor, Department of ECE, Engg., A.I.E.T, Faridkot, (Punjab), INDIA*

(Corresponding author: Gurleen Kaur*)*
(Received 24 November, 2015 Accepted 29 December, 2015)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: In today's digital age, powerful and low cost digital technology has made it possible to create effective photographic forgeries. Therefore it becomes very challenging for end users to distinguish whether the image is novel or tempered. In the fields such as forensics, medical imaging, e-commerce, authenticity and integrity of digital images is crucial. The usage of digital images in such fields generates the need for detection tools that can reveal whether the image is real or fake. Whenever tampering is done, it affects or changes the basic characteristics of images such as blurriness,sharpness,noise, luminance intensity etc.There are various methods which detects divergence in different characteristics.Now days, there exist different techniques that detect tampering in digital images based on illuminant color inconsistencies. The goal of this paper is to provide a review of the existing literature available on illumination based digital image tampering detection techniques.
Keywords: Digital images, Illuminant color, Tampering detection.

I. INTRODUCTION

Forgery is an illegal modification or reproduction of an image, document signature, legal tender or any other means of recording information. Generally, people believe in whatever they see rather than what they hear or read.But now-a-days digital technology has begun to erode this trust. Thus, forgery detection becomes very important for real world events. Every day, millions of digital documents are produced by a variety of devices and distributed by newspapers, magazines, websites and television. In all these information channels, images are a powerful tool for communication. Unfortunately, it is not difficult to use computer graphics and image processing techniques to manipulate images. When we are using such images for an important purpose like evidence in court, it becomes an important issue to prove the authenticity of image.

A. Image Forgery Classification

Digital image forgery detection techniques can be divided into two major groups: intrusive and non-intrusive. In intrusive (active) techniques, some sort of signature (watermark, extrinsic fingerprint) is embedded into a digital image, and further authenticated by verifying if the original signature matches the retrieved signature from the test image.The main limitation of this method is that watermark (or signature) must be inserted at the time of recording, which requires specially equipped digital camera. Unlike active approaches, there is no need of any prior information regarding image in case of passive detection. This is the main advantage of these passive forgery detection methods over the active techniques.

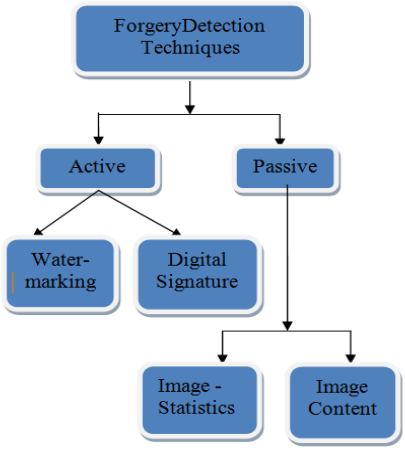

Fig. 1. Classification of forgery detection techniques.

Image composition(or splicing) is one of most common form of passive image manipulation. This technique involves composites of two or more images which are combined to create a fake image. The steps of image splicing are shown below:

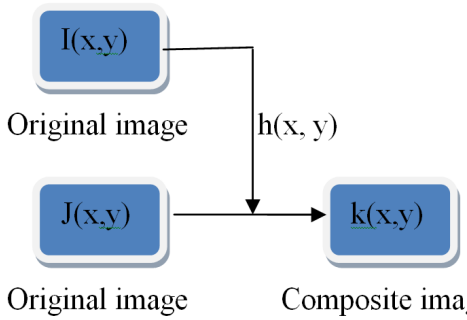

Fig. 2. The process of image composition (or splicing).

I(x,y) and J(x,y) are original images. Where k(x,y) is a part of I(x,y) which is embed into J(x,y) in order to create a image composite k(x,y).An example of such type of forgery is shown in the Fig. 3.

Fig. 3. Example of composite image.

Digital image forensics is an emerging field where forensic investigators use all available sources of tampering evidence for assessing the authenticity of an image. While creating a composite image, various mismatches are introduced in the image e.g. brightness, lighting and color mismatches. It will become extremely hard to match the color of one object with reference to other. Therefore, one can easily detect the forgeries by exploiting color mismatches among the objects in the image. This is done by detecting changes in illuminant color.Illumination based forgery detection method can be classified into two categories:

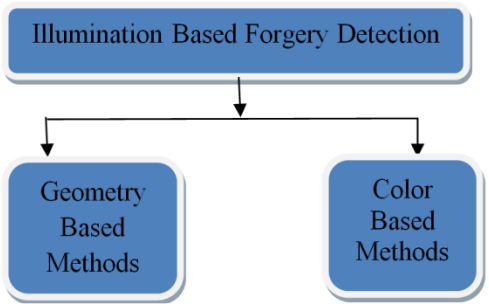

Fig. 4. Illuminant color based forgery detection.

B. Illumination Based Digital Image Forgery Detection

Illumination-based techniques for forgery detection are either geometry-based or color-based. The detection of inconsistencies in light source positions between specific objects in the scene is done by geometry-based methods. In contrast, color-based methods search for inconsistencies in the interactions between object color and light color.

While creating a composite image, it is difficult to match the lighting conditions of two images. These lighting inconsistencies are used to detect the forgeries. M. Johnson and H. Farid [3] proposed a technique which computes a low-dimensional descriptor of lighting environment in the image plane (i.e., in 2-D).It estimates the illumination direction from intensity distribution along manually annotated object boundaries of homogeneous color.

E. Kee and H. Farid [4] extended the above technique to exploiting known 3-D geometry. In the case of faces, a dense grid of 3-D normal improves the estimate of illumination direction. For this purpose, a 3-D face model is registered with the 2-D image using manually annotated facial landmarks.

W. Fan *et al.* [7] proposed a method for estimating 3-D illumination using shape-from-shading. This technique doesn't require 3-D model of the object, which also reduces dependableness of the method.

M. Johnson and H. Farid [6] suggested a method to detect digital image forgeries by utilizing specular highlights in the eyes.

P. Saboia *et al.* [8] extended the above technique in order to classify the images by exploring some additional options. The relevancy of both these approaches is limited by the very fact that images should be available in high resolution and eye should be clearly captured while taking the photographs.

S. Gholap and P.K. Bora [9] proposed physics –based illumination cues to image forensics.The authors explored inconsistencies in secularities based on dichromatic reflectance model.

X. Wu and Z. Fang [5] assume a purely diffuse reflectance and train a mixture of Gaussians to select a proper illuminant color estimator. The angular distance between illuminant estimates from selected regions can then be used as an evidence for forgery.

A. Gijsenij *et.al.* [10] Introduced a pixel wise illuminant estimator which allows to segmentan image into regions illuminated by various illuminants. These illuminated regions which are distinct have sharp transitions from different illuminant shades.

C. Riess and E. Angelopoulou [2] proposed a different method by using physics-based color constancy algorithm that operates on partially specular pixels. Here the image is segmented in order to estimate the illuminant color locally per segment.

Z. Qu *et al.* [12] described a completely automatic method for detecting digital image splicing forgeries base on the sharp splicing boundaries. The novelty of the proposed method that an OSF based edge sharpness measure, a visual saliency guided feature extraction method and also a hierarchical classifier used to splicing detection problem.

T. Carvalho *et al.* [11], proposed method for detecting forged images of people that exploit light inconsistencies in the color of the illumination of images. This method is machine learning-based and requires minimal user interaction.

Overview of previous work on forgery detection based on Illumination inconsistencies.

Year	Authors	Proposed Model/Method	Merits	Demerits
2007	M. Johnson and H. Farid	Computes illumination descriptor in 2-D plane.	This method assumes nearlyLambertian surfaces for both forged and original areas.	System might not work when object does not have a compatible surface.
2007	M. Johnson and H. Farid	Spliced image detection by creating environment map from eyes that embodies the illumination in the scene.	Environment map provides a rich source of information about the lighting.	Works only for high resolution image of eye.
2008	S. Gholap and P.K. Bora	Dichromatic reflection model is used to examine inconsistencies.	Physics- based illumination cues to image forensics.	Less applicability in real world scenarios.
2009	Z. Qu *et al.*	OSF based edge sharpness measure, a visual saliency guided feature extraction method and also a hierarchical classifier is used to splicing detection problem.	Completely automatic method for detecting digital image splicing forgeries.	A drawback of this is that the edge sharpness cues now used will fail when concealing measures, such as blur, is useful.
2010	C. Riess and E. Angelopoulou	Physics based color constancy algorithm is used that operates on partially specular axis.	Illuminant map is generated to find the manipulated region.	Visual judgment of illuminant map can be misleading.
2010	E. Kee and H. Farid	Extended the approach of M. Johnson and H. Farid [3] to exploiting known 3-D geometry.	3-D normal improve estimate of illumination direction.	Highly resoluted images are required.
2011	X. Wu and Z. Fang	Mixture of Gaussians is trained to select a proper illuminant color estimator.	Purely diffuse reflectance (i.e., specular-free).	Requires manual selection of reference block.
2011	P. Saboia *et al.*	Detect forgeries using eye specular highlight.	Extended the approach of M. Johnson and H. Farid [6] to automatically classify the extracted features.	Limited by the fact that people's eyes must be visible and available in high resolution.
2012	A. Gijsenij *et.al.*	Pixel wise illuminant estimator	Multiple regions of segmented image are are illuminated by distinct illuminants.	Results of multiple illuminant estimators are require.
2013	T. Carvalho *et al.*	Detect forged images that exploit light inconsistencies in the color of the illumination of images.	Machine learning based and requires minimal user interaction. Also provide crisp statement on authenticity of the image.	Methods that operate on illuminant color are inherently prone to estimation errors.
2014	P.K Boraet al.	Exposing the image forgeries based on illuminant estimation from human skin highlights formed by the colour variation on the nose tip.	The dichromatic reflection model is utilized to obtain the illuminant colour estimate from human skin highlights.	Alternative methods to find the illuminant colour are require.
2014	H. U. Neenu and J. Cheriyan	Illumination inconsistencies and resampling properties are used for detecting forged images.	This method can be used inforensic and medical applications to check genuinity of images.	Speed and size of classifier in both tarining and testing phase.

P.K Bora *et al.* [13] proposed a novel method that detects the illuminant colour mismatch among different persons in a composite image. The dichromatic reflection model is utilized to obtain the illuminant colour estimate from human skin highlights. The illuminant colour obtained is quantified using chromaticity coordinates. It is then matched against that of different persons in the composite image to detect the forgery.

H. U. Neenu andJ. Cheriyan [14] evinced a method which incorporates both the illumination inconsistencies and resampling properties for detecting forged images. This technique can be used in medical as well asforensic applications to check the genuinity of image.

II. CONCLUSION

In this paper, we presented review of methods for detecting altered or doctored images of people using the illuminant color classification mechanism. Many color based or geometry based methods are reviewed to detect tampering based on illuminant color. In above techniques, the first step is to determine the illuminant estimator followed by feature selection and classification. Here intermediate representation called illuminant map is created. The interpretation of these maps is left to human experts. Whereas, relying on visual assessment by humans can be misleading, because their visual system is quite clumsy at judging illumination environments in pictures. So, it is suggested to transfer the tampering decision to an objective algorithm. Moreover, there is great need of problem specific illuminant estimator. A machine learning based illuminant estimator particularly for faces is required.

REFERENCES

[1]. G.K. Birajdar and V.H. Mankar, "Digital image forgery detection using passive techniques: a survey," Digital investigation, vol. **10**, no. 3, pp. 226-245, 2013.

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

[3]. M. Johnson and H. Farid, "Exposing digital forgeries in complex lighting environment," *IEEE Trans. Inf. Forensics Security,* vol. **3**, no. 2, pp. 450-461, June 2007.

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

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

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

[7]. W. Fan, K. Wang ,F. Cayre and Z. Xiong, "3-D lighting based image forgery detection using shape-from-shading, " in proc. Eur. Signal Processing Conf. (EUSIPCO), pp. 1777-1781,Aug 2012.

[8]. 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),* pp. 1937-1940, 2011.

[9]. S. Gholap and P.K Bora, "Illuminant color based image forensics," in Proc. *IEEE Region 10 Conf*., pp. 1-5, 2008.

[10]. 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.

[11]. T. Carvalho, C. Riess , E. Angelopoulou, H. Pedrini and A. Rocha, "Exposing digital forgeries by illumination color classification", *IEEE Transaction on Information Forensics and Security*, vol. **8**, no. 7, pp. 1182 – 1194, July 2013.

[12]. Z. Qu, G. Qiu, and J. Huang," Detect Digital Image Splicing with Visual Cues", LNCS 5806, pp. 247–261, 2009.

[13]. P.K. Bora, S. Gholap and K. Francis, "Illuminant colour based Image Forensics using mismatch in human Skin highlights," *IEEE 20th National Conf. on Communications*, pp. 1-4, March 2014.

[14]. H.U. Neenu and J. Cheriyan, "Image forgery detection based on illumination inconsistencies & intrinsic resampling properties," *IEEE International Conference on Magnetics, Machines & Drives*, pp. 1-6, July 2014.