International Journal of Current Engineering and Technology
©2015INPRESSCO®, All Rights Reserved

E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

Review Article

Novel Methods for Digital Image Authentication by Detecting Traces of Demosaicing and Illuminant Color Inconsistencies

Shweta P. Kachhawal[†*] **and Avinash P. Wadhe**[†]

[†]SGBAU, Amravati, India

Accepted 15 March 2015, Available online 20 March 2015, **Vol.5, No.2 (April 2015)**

Abstract

Nowadays there's great accessibility of tools for the acquisition and process of transmission signals. With this refined and cheap image editing software, it's changing into more easier task to tamper with digital pictures. Therefore, currently pictures can't be thought of trustworthy proof. To cope with these problems, understanding the sort of image manipulation is vital. This paper presents an summary of machine learning approach that exploits refined inconsistencies within the color of the illumination of pictures and distinguishes between computer generated and photographic image. The technique is applicable to photographs containing two or additional individuals and needs no knowledgeable interaction for the tampering decision. To achieve this, the data is taken from physics and statistical based illuminant estimator on image regions of comparable material. For differentiating the PRCG and PIM, a completely unique approach is to concentrate on the image textures, we have a tendency to acknowledge that pictures from digital cameras that contain traces of resampling as a results of employing a color filter array with demosaicing algorithms.

Keywords: *Digital tampering, demosaicing, resampling, illuminant map, color inconsistencies, Digital forgery*

1. Introduction

In the recent years digital transmission devices like cameras, mobile-phones, etc. has enhanced the chance of generating digital audiovisual information without any time, location, and network-related constraints. The good functioning of those devices enable copying, editing, and distributing the multimedia system information with very little effort. As a result, security of digital pictures became a lot of harder; because of the potential various origins and also the potential alterations that might are operated.

In the past few years, various image tamper detection techniques have been proposed a number of these techniques target detecting a selected style of tampering operation like re-compression, cloning, splicing, resizing. Another category of techniques attempt to detect the presence of generic image manipulation operations that will be indicative of tampering like filtering, down-sampling, up-sampling, compression, rotation, etc.(C. Riess, *et al*, 2010).

One of the issues digital image forensics techniques attempt to solve is that the identification of the source of a digital image. That means to check by what approach a digital image has been created, e.g., camera, scanner, generative algorithms, etc. Attainable solutions to the problem of image source identification could include one amongst the below approaches:

1. Verifying and evaluating the image statistics that are inherent to real-life sceneries and objects.
2. Detecting, classifying and measure the qualities of abstraction structures (i.e., color, texture and edge structures) in a picture.
3. Characteristic signatures to find traces of certain kinds of operations utilized in image generation process by potential sources.

In this paper, the foremost common type of image manipulation i.e. image composition is taken into account. Now days, it's tough to differentiate between photorealistic computer generated images (PRCG) from photographic images (PIM). Here the strategy is used to find traces of demosaicing within the image as a result of resampling. In this paper, the techniques for police investigation traces of demosaicing and finding inconsistencies in color of illuminant is reviewed. The primary technique establishes the traces of resampling and second focuses on inconsistencies of the color of image.

2. Background

There are numerous potential approaches for authenticating the safety of a digital image. The one among the implemented technique for image alteration is watermarking. With watermarking, a picture is

*Corresponding author **Shweta P. Kachhawal** is M.E 2nd Year (CSE) student and **Avinash P. Wadhe** is working as Assistant Professor altered to hold an authentication message by the image capture device. Unfortunately, this methodology needs coordination between the insertion and extraction of the watermark (Andrew C. Gallagher, *et al*, 2013).

After this approach, statistical strategies are also used to characterize the distinction between PRCG and PIM. In this technique, geometric and physical features also are effective for classifying between PRCG and PIM. Even supposing this method is effective, the imperfections like dirt, smudges, and nicks that are pervasive in real scenes are troublesome to simulate (Andrew C. Gallagher, *et al*, 2013). As a result of these factors, the stastical distinction between real scene and computer generated is negligible.

Researchers introduced another technique named interpolation that resampled the image and finds the statistical traces of resampling that are embedded within the image signal itself. In conjunction with analysis, the EM algorithm are used to recover the correlations between neighboring pixels that are introduced through interpolation. This approach effectively works for detection candidate forged image regions and is robust to JPEG compression. Some researchers exploit image sensor imperfections to match images to specific cameras. These approaches demonstrate a way to exploit the natural watermarks that are inserted into images as a results of necessary image processing (Sintayehu Dehnie).

Basically Illumination-based methods for forgery detection are either geometry-based or color-based. The projected ways use the direction of the incident light for exposing digital forgeries. In (E. Kee, *et al,* 2010), authors extended this approach to exploiting better-known three-D surface geometry. In the case of faces, a dense grid of 3-d normals improves the estimate of the illumination direction. To attain this, a 3-d face model is registered with the 2-D image using manually annotated facial landmarks. However this reduces the flexibility of algorithm. After this, technique is proposed to spliced image detection by exploiting specular highlights in the eyes. This technique is restricted by the very fact that people's eyes should be visible and obtainable in high resolution.

Some physics-based illumination methods are introduced for image forensics. The authors examined inconsistencies in specularities supported the dichromatic reflectance model. However Specularity segmentation on real-world pictures is difficult. In [3], to overcome all on top of issues, authors projected a special approach by employing a physics-based color constancy rule that operates on partly specular pixels. in this approach, the automated detection of highly specular regions is avoided. The authors propose to section the image to estimate the illuminant color locallyper segment. Recoloring every image region according to its local illuminant estimate yields a so-called illuminant map. the most drawback of this technique is an expert is left with the tough task of visually examining an illuminant map for proof of change of state.

For overcoming all drawbacks, Tiago José De Carvalho *et al* and Andrew C. Gallagher *et al*, projected new ways i.e tracing the resamples of demosaicing and illumination color inconsistencies.

3. Literature Survey

Tiago José de Carvalho *et al.* planned forgery detection technique that exploits refined inconsistencies within the color of the illumination of pictures. This method is applicable to only composite pictures. The authors combined the attributes of each physics and statistical-based illuminant estimator to apply on image region of same material. Here, authors made user interaction minimal by extracting texture- and edge-based features by making use of machine-learning approach for automatic decision-making.

Andrew C. Gallagher, Tsuhan Chen explain a concept that images taken from camera can contain traces of resampling as results of using a color filter array with demosaicing algorithms. It distinguishes photorealistic computer graphic images and photographic images captured with a camera.

C. Riess and E. Angelopoulou explain image authenticity by considering illumination color as a new indicator. The authors planned a technique in which the user selects illuminated areas for further investigation. The illuminant colors are regionally estimated, effectively decomposing the scene in a map of differently illuminated regions. If a picture has been manipulated, the transition between these illuminants should consequently be disturbed.

The author H. Farid and M. J. Bravo explained three ways that show that the human visual system is unable to discover inconsistencies in shadows, reflections, and planar perspective distortions. They have described computational strategies that may be applied to discover the inconsistencies that seem to elude the human visual system. The These results of their work recommend that care should be taken once making judgments of image legitimacy based mostly solely on visual inspection.

E. Kee and H. Farid used inconsistencies in the lighting model of image as an proof of manipulation. Whereas making a composite image, its vital to maintain the lightning conditions. The authors describe how to estimate the total 3-d lighting environment in images of individuals. For extracting the desired 3-d surface normals, they match 3-d models to an image of a person's head and automatically align this model to an arbitrary head pose. Lighting inconsistencies in a picture are then used as proof of manipulation.

Micah K. Johnson and Hany Farid, used lightning inconsistencies in a photograph as a proof of tampering. Here authors show a way to approximate complex lighting environments with a low-dimensional model and the way to estimate the model's parameters from one image.

Anderson Rocha et al. introduces the subject areas that come under the sphere of digital image forensics.

The topics like source camera identification, forgery detection, etc.

Sintayehu Dehnie described technique to differentiate pictures captured by a digital camera from laptop generated images. This approach is predicated on the fact that image acquisition in a photographic camera is essentially different from the generative algorithms deployed by computer generated image.

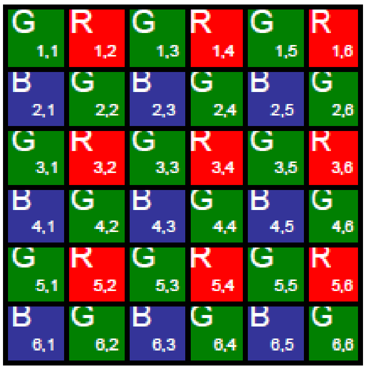
Shweta P *et al* reviewed completely different video forensics techniques. This methods shows however digital video can be manipulated and to a way to notice these tampering. The techniques like detecting Re-Projected Video, detecting Duplication, detecting Double MPEG Compression and detecting Double quantization, are reviewed.

4. Novel Techniques Of Image Authentication

In this paper, two strategies are reviewed for authenticating the image. The primary one is to detect the traces of resampling as a results of demosaicing. And second is to search out illumination inconsistencies within the image. These methods are explained in detail as follows.

4.1 Detecting Traces of Demosaicing

Recently in digital imaging technologies raised new issues and challenges regarding the integrity and authenticity of digital pictures. Digital images can now be simply created, edited and manipulated without leaving any obvious traces of such operations. These capabilities undermine the credibility of digital images in all aspects. Mostly all digital cameras contain an image sensor with a color filter array, for instance, the Bayer filter array shown in Figure 1. A filter is positioned over every photosite, sensitizing it to either the red, green, or blue element of the incident light. Sometimes other color filter array patterns and filters are used, the Bayer is the most common (Andrew C. Gallagher, *et al*, 2013).

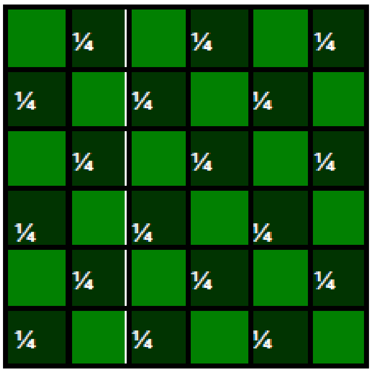


G 1,1	R 1,2	G 1,3	R 1,4	G 1,5	R 1,6
B 2,1	G 2,2	B 2,3	G 2,4	B 2,5	G 2,6
G 3,1	R 3,2	G 3,3	R 3,4	G 3,5	R 3,6
B 4,1	G 4,2	B 4,3	G 4,4	B 4,5	G 4,6
G 5,1	R 5,2	G 5,3	R 5,4	G 5,5	R 5,6
B 6,1	G 6,2	B 6,3	G 6,4	B 6,5	G 6,6

Fig.1 Bayer Filter

The raw image from the image sensor contains solely a single signal value at every pixel position. This component value further corresponds to only a single color element (red, green, or blue within the case of the bayer filter array). Typically, a demosaicing algorithmic rule also known as color filter array interpolation, is applied to the raw image to estimate the pixel value for every color element. The interpolation can either be linear or adaptive. In demosaicing algorithm, missing color values are determined from a weighted linear combination of neighboring pixels, and the sum of the weights is one. The interpolation of this variety leaves a sign that can be reliably detected.

In this technique, only the green pixel values of the Bayer pattern is taken into account shown in Figure 2, every missing green component value can be interpolated from its four nearest neighbors using bilinear interpolation.



🟩	¼	🟩	¼	🟩	¼
¼	🟩	¼	🟩	¼	🟩
🟩	¼	🟩	¼	🟩	¼
¼	🟩	¼	🟩	¼	🟩
🟩	¼	🟩	¼	🟩	¼
¼	🟩	¼	🟩	¼	🟩

Fig.2 When demosaicing is performed with linear interpolation, the interpolated green pixels have lower variance than the original green pixels. The spatial pattern of variances is the basis for detecting the presence of demosaicing(Andrew C. Gallagher, *et al*, 2013).

In Figure 2, the green channel is partitioned into two interleaved quincunx patterns, one corresponding to the original green pixel locations, and the different corresponding to the estimated green picture element locations with lower variance. This analysis oversimplifies the demosaicing and omits the nonlinear image processing for the purpose of illustration. The vital purpose to acknowledge is that demosaicing introduces periodic patterns into the image signal. In a sense, demosaicing may be a sort of passive watermarking, as a result of the signal process necessitated by the image sensor leaves an indication in the image. By extracting and recognizing these periodic signals embedded within the image, the source of the image is surmised.

The technique for detecting traces of demosaicing firstly applies a high pass filter then the variance of every diagonal is estimated. Fourier analysis is employed to find periodicities in the variance signal, indicating the presence of demosaicing.

4.2 Illumination Color Classification Method

Images are widespread means of communication and lots of people rely on them, thus it is necessary that their authenticity should be proved. As the field of image process and its applications has grown and extended to large area, there's an increase in the accessibility of image editing software also. due to the easy handiness of digital editing tools, alteration, and manipulation became very simple and as a result forgery detection becomes a complex and threatening drawback. Due to this, a large range of doctored or edited pictures area unit circulating in our media of communication. This can deceive the viewer, and forces him to simply accept or agree on the contents of the image.

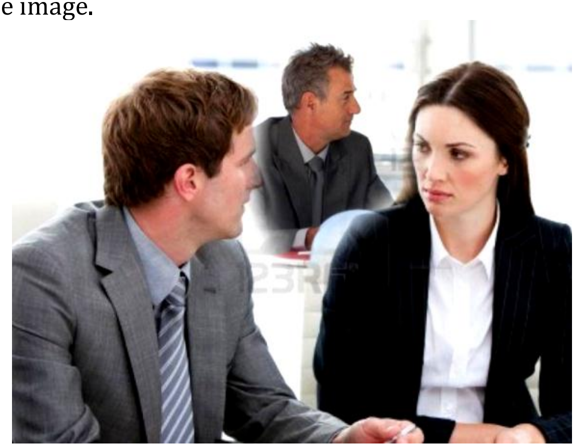


Fig.3 Is this image an authentic one? An example spliced image involving multiple human faces

Splicing or image composition is a sort of forgery that can create a single composite image of individuals from two or additional images (Anderson Rocha, *et al*, 2009). The above figure Fig.1 is an example within which the person in the middle is an inserted one. The splicing is one among the harmful image manipulation technique. Based on the actual fact that no two pictures taken for splicing have same lighting conditions, the illuminant extract of the image can be used for splicing detection; i.e, the amount of light incident on the faces chosen from different pictures to create a composite image is not identical. Though editing the image content is straightforward, it's difficult or highly not possible to adjust the illuminant conditions comparable to other image taken for splicing. Most of the image editors doesn't concentrate or notice the difference in image illuminancy. Therefore the illuminant estimates of the image can be a powerful tool in forensic analysis of junction detection.

The authors proposed that illuminant estimates from local image regions will be analyzed by human experts to detect the illumination inconsistencies (C. Riess, *et al*, 2010). This is very difficult, as most of the illumination options elude the human visual system.

The necessary contributions of this methodology are as follows:

1) Creating images maps of pictures.
2) Introducing an integrated approach of feature extraction (texture –cum- edge features).
3) Minimizing human interaction in tampering decision making.
4) Semi – automated Forgery detection.

The projected methodology of forgery detection can be organized into five main elements.

- Local illuminant Estimation(IE)
- Interactive Face Extraction
- Extraction of illuminant features
- Distance measure of paired faces
- Classification

Conclusion

In this paper, a unique approach to differentiate between photographic images and photorealistic computer generated images is delineated. Rather than focusing on characteristics of the scene itself, exploit the image process necessitated by the camera hardware. The foremost cameras image sensors contain a color filter array and demosaicing used to be wont to produce three-color pictures. Demosaicing acts as a sort of passive watermarking that leaves a trace embedded within the image signal. once traces of demosaicing are detected, we have a tendency to surmise that the image may be a photo graphic (rather than computer generated) image.

Additionally a new technique for detecting forged images of people using the illuminant color estimates is reviewed here. Two separate illuminant estimators are used: gray world estimator and physics based illuminant estimator known as inverse intensity – chromaticity space. The illuminant maps are treated as texture maps. The edge information is additionally extracted. So as to explain the texture –cum-edge patterns, an integrative algorithm gabor physicist local binary pattern, HOG edge descriptor and SASI descriptor is projected. These complementary cues are employed in machine learning based mostly classification.

The projected system requires only a minimum human interaction in forgery detection. User interaction is required only to select the bounding boxes of the human faces on the image. The ultimate decision on image forgery is automated to eliminate the requirement for a human expert to take tampering decision.

References

Tiago José De Carvalho, Christian Riess, Elli Angelopoulou, Hélio Pedrini, Anderson de Rezende Rocha (2013), Exposing Digital Image Forgeries by Illumination Color Classification © *IEEE* , 1556-6013

Andrew C. Gallagher, Tsuhan Chen (2013), Image Authentication by Detecting Traces of Demosaicing @ *IEEE* , 978-1-4244-2340-8/08

C. Riess and E. Angelopoulou (2010), Scene illumination as an indicator of image manipulation, *Inf. Hiding*, vol. 6387, pp. 66–80

H. Farid and M. J. Bravo (2010), Image forensic analyses that elude the human visual system, in *Proc. Symp. Electron. Imaging (SPIE*

E. Kee and H. Farid (2010), Exposing digital forgeries from 3-D lighting environments, in *Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Dec*

Micah K. Johnson, Hany Farid (2007), Exposing Digital Forgeries in Complex Lighting Environments,© *IEEE*, 1556-6013/$25.00

Anderson Rocha, Walter Scheirer, Terrance Boult, Slome Goldenstein (2009), *Vision Of The Unseen : Current Trends And Challenges In Digital Image And Forensics © ACM* 0000/2009/0000-0001

Sintayehu Dehnie, Digital Image Forensics For Identifying Computer Generated And Digital Camera Images

Shweta P. Kachhawal and Prof. Avinash P. Wadhe (2014), Study Of Different Video Forensics Techniques in *International Journal of Computer, Information Technology & Bioinformatics (IJCITB)* ISSN: 2278-7593, Volume-2, Issue-2