International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-3)

Research Article | **March 2014**

Review of Detection of Digital Image Splicing Forgeries with illumination color Estimation

Ms. Sushama G. Rasse
Dept. of Computer Engineering, University of Pune
P.K. Technical Campus, Pune, India

Abstract—

Recently advanced image processing tools and computer graphics techniques make it straightforward to edit or modify digital images. In court, for police agencies, for insurance or media companies, this raises the challenge of discriminating original images from malicious forgeries. Particular region from an image is pasted into other image with purpose to create image splicing. Image splicing is a common type of image tampering (manipulation) operation. The image integrity verification as well as identifying the areas of tampering on images without need to any expert support or manual process or prior knowledge original image contents is now days becoming the challenging research problem. In this paper, we are focusing on authenticity of images and are based on concept of using illumination color estimation. Recently new method introduced for efficient forgery detection particular for faces in images. The illuminant color is estimated using the physics based method as well as statistical edge method which make the use of inverse intensity-chromaticity color space. The estimate of illuminant color is extracted independently from the different mini regions. For the classification used the Support Vector Machine (SVM) approach. In this paper our main goal is to take review of different methods for digital image forgeries detection.

Keywords— Digital images, estimation errors, forgeries detection, image splicing, Illuminant Color Estimation, SVM.

I. INTRODUCTION

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 the no difficulty in their acquisition, division and storage is such that they are more and more exploited to convey information. But digital images are easy to manipulate because of the availability of the powerful editing software and sophisticated digital cameras. Image processing experts can easily access and modify image content and therefore its meaning without leaving visually detectable traces. 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 start, the manipulation is just improve the image's performance, but then many people started to change the image's content, even to gain their ends by these illegal and immorality methods. Based on the above reasons, it is important to develop a credible method to detect whether a digital image is tempered, so-called digital image forgery.

Digital imaging resulted into many real life benefits, but at same side it's vulnerable to many threats of crimes. To check whether image is real or forged? , it is very difficult task. In fact, the security concern of digital content has arisen a long time ago and different techniques for validating the integrity of digital images have been developed. These 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 authenticity is established by verifying if the true signature matches the retrieved signature from the test image [3] [4] [5]. This approach is limited due to the inability of many digital cameras and video recorders available in the market to embed extrinsic fingerprints [6]. Further the drawbacks of intrusive methods used as motivation for non-intrusive method [6] in order to validate the authenticity of digital images. These techniques exploit different kinds of intrinsic fingerprints such as sensor noise of the capturing device or image specific detectable changes for detecting forgery. There are many challenges in blind techniques, for instance, reducing false positive rates (i.e., an authentic image being detected as a forged image), making the system fully automated, localizing the forgery, detecting forgery of any type of image format (compressed or uncompressed), increasing the robustness and reliability, etc.

Image splicing is to create a new image from two or more images, and it is far and wide used for image forgery. Image splicing detection is a main difficulty in image forensics. However there are very hardly any solutions to this problem .An given below example of a digital forgery is shown in Figure 1. As the newspaper cutout shows, three different photographs were used in creating the composite image: Image of the White House, Bill Clinton, and Saddam Hussein. The White House was rescaled and blurred to create an illusion of an out-of-focus background. Then, Bill Clinton and Saddam were cut off from two different images and pasted on the White House image. Care was taken to bring in the speaker stands with microphones while preserving the correct shadows and lighting. Fig. 1 is, in fact, an example of a very realistic looking forgery.


INTERNET

Spies turn to high-tech info ops

PCs, Internet used for manipulating images, public opinion

ALTERED IMAGE

BY DANIEL VERTON

Federal intelligence agencies are studying ways to use computers and the Internet, rather than just leaflets and radio broadcasts, to shape and disseminate information designed to sway public opinion in the world's hot spots.

As part of its so-called "perception management" program, the intelligence community has for decades created misinformation to trigger political change without direct political or military involvement in countries where the United States has vested interests, such as Iraq and North Korea.

Acting on congressional recommendations to bolster research and development in information technology, intelligence agencies are turning to PCs to develop more sophisticated means of manipulating and delivering digital photos, video clips and recorded sound to portray fictitious events in hopes of provoking desirable outcomes.

Altered Egos

The top photo, of a fictitious meeting between President Clinton and Saddam Hussein, was generated by digitally altering and combining elements from three photos, shown below the altered image. Intelligence agencies plan to use similar techniques to create images and then disseminate them via the Internet in their efforts to influence events in foreign countries, such as Iraq.

Fig. 1 Example of a Digital Forgery

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 conditions is hard to achieve when creating a composite image [1]. In this paper we are taking the review of digital image forgeries detection and their different methods. In section II, we are discussing illuminant inconsistencies. In section III, different methods are discussed those are presented by various researchers to provide crisp statement on the authenticity of an image.

II. ILLUMINATION INCONSISTENCIES

In blind image forgeries detection, analysis 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 [2] presented a different approach by using a physics-based color constancy algorithm that operates on partially specular pixels. In this approach, the automatic detection of highly specular regions is avoided. The authors propose to segment the image to estimate the illuminant color *l*ocally per segment. Recoloring each image region according to its local illuminant estimate yields a so-called illuminant map. Implausible illuminant color estimates point towards a manipulated region. Unfortunately, the authors do not provide a numerical decision criterion for tampering 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.

Fig. 2 Example of the influence of illumination on the perceived object color. The same scene is shown, once exposed to white illumination, once exposed to illuminants that approximate illumination at night.

Color is widely used in computer vision, but in a very basic, primitive way. One reason for employing 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 not unlikely: the spectrum of sunlight changes over the daytime, shadows can fall on the object, or artificial light is switched on. Fig. 2 shows two examples for different color appearances. The pictures are part of the dataset. The scene is once exposed to relatively neutral (white) light, and once to illuminants that approximate the environment light at night. Thus, for robustness, methodologies that employ color should explicitly address such appearance 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 method do not require training data and are applied to any image.

A. Statistical generalized gray world estimates

The generalized gray world approach by Joost van de Weijer, Theo Gevers, and Arjan Gijsenij [12], they investigated

edge-based color constancy. The method is derived from the gray-edge hypothesis which assumes that the average edge difference in a scene is achromatic. In contrast to existing methods, which are based on zero-order structure of the image, this method is based on the higher order structure of images. Furthermore, we introduce a framework of color constancy based on low-level image features which includes the known algorithms (gray-world, max-RGB, Minkowski norm) as well as the newly proposed gray-edge and higher order gray-edge algorithms. The quality of the various instantiations of the framework is tested on two large data sets of images recording objects under a large number of different light sources.The derivative operator increases the robustness against homogeneously colored regions of varying sizes. Additionally, the Minkovski norm emphasizes strong derivatives over weaker derivatives, so that specular edges are better exploited.

B. physics-based inverse-intensity chromaticity space estimates

Statistics-based methods require many surface colors and become error prone when there are only a few surface colors. In contrast, dichromatic-based methods can successfully handle uniformly colored surfaces but cannot be applied to highly textured surfaces, since they require precise color segmentation. R. Tan, K. Nishino, and K. Ikeuchi[11] introduces a single integrated method to estimate illumination chromaticity from singlecolored and multicolored surfaces and require only uneven highlight region without segmenting the colors within them. This method gives relationship between illumination chromaticity and image chromaticity. Advantages of method are the capability to deal with either a single surface color or multiple surface colors, color segmentation surrounded by highlight regions and intrinsic camera characteristics are not mandatory. Also, this method does not use strong constraints on illumination, which several existing color constancy methods, such as a blackbody radiator, use.

III. REVIEW OF DIGITAL IMAGE FORGERY DETECTION

In this section we are present the different methods those are for digital image forgeries detection with their advantage and problem.

H. R. Chennamma [8], Lalitha Rangarajan, Portions of the image is correlated with each other with respect to the imaging device. Such correlations will be disturbed in spliced images. We have used an intrinsic camera parameter, namely lens radial distortion, for the detection of image splicing. Inconsistency in the degree of lens radial distortion across the image is the main evidence for the detection of spliced images. In this paper we propose a novel passive technique (with no watermark or signature) for detecting copy-paste forgery by quantitatively measuring lens radial distortion from different portions of the image using line-based calibration.

Zhenhua Qu, Guoping Qiu, and Jiwu Huang [9] described a completely automatic method for detecting igital 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. They explain that a trustworthy hierarchical classifier can be trained with the discriminative features extracted from the first few fixations predicted with a visual attention model with edge sharpness as visual cues and localizing splicing boundaries A drawback of this is that the edge sharpness cues now used will fail when concealing measures, such as blur, is useful.

Johnson and Farid[10] proposed spliced image detection by exploiting specular highlights in the eyes . 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.

Y. Ostrovsky, P. Cavanagh, and P. Sinha, authors in [7] find that once the geometrical regularity of the previous displays is removed, the visual system is remarkably insensitive to illumination inconsistencies, both in experimental stimuli and in altered images of real scenes. Whether the target is interpreted as oddly illuminated or oddly pigmented, it is very difficult to find if the only cue is deviation from the regularity of illumination or reflectance. Our results allow us to draw inferences about how the visual system encodes illumination distributions across scenes. Specifically, they suggest that the visual system does not verify the global consistency of locally derived estimates of illumination direction.

Tiago Carvalho, Christian Riessy Elli et al. [1], 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. The method is valid to a broad range of images and requires no expert interaction for the tampering decision (provides crisp statement on authenticity of an image). To get this, they include hint (cue) from physics as well as statistical-based illuminant estimators on image regions of comparable material. From these illuminant estimates they mine (extract) texture- and edge-based features feeding a machine learning approach for automatic decision-making. They used support vector machine to classify these features. This method requires images of people with minimum two faces and prefers semiautomatic method for face extraction.

IV. CONCLUSION AND FUTURE WORK

The authenticity of an image is major research challenge in the field image forensic for real world events. The image integrity verification as well as identifying the areas of tampering on images without need to any expert support or manual process or prior knowledge original image contents is now days becoming the challenging research problem. Thus to solve

this problem recently some more techniques were presented and new techniques will be developed to make better and harder to detect fakes (for exposing photographic frauds). In this paper we have discussed different methods of detection for digital image forgery as well as illumination inconsistencies and illuminant map. For the future work we suggest to work over improved new method with efficient skin detection methods.

ACKNOWLEDGEMENT

I would like to express the deepest appreciation to guide Dr.S. Singh and to authors Tiago José de Carvalho, Christian Riess, Elli Angelopoulou, Hélio edrini and Anderson de Rezende Rocha for their beneficial information and knowledge.

REFERENCES

[1] Tiago José de Carvalho, Student Member, IEEE, Christian Riess, Associate Member, IEEE, Elli Angelopoulou, Member, IEEE, Hélio Pedrini, Member, IEEE, and Anderson de Rezende Rocha, Member, IEEE, *"Exposing Digital Image Forgeries by Illumination Color Classification"*, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 7, JULY 2013

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

[3] Yeung MM, *"Digital watermarking"*, ACM Communications 1998; 41(7):30–3.

[4] Rey C, Dugelay JL. *"A survey of watermarking algorithms for image authentication"*, EURASIP Journal on Applied Signal Processing; 2002: 613–21.

[5] Zhang C, Cheng LL, Qiu Z, Cheng LM, *"Multipurpose watermarking based on multiscale curvelet transform"*, IEEE Transactions on Information Forensics and Security December 2008; 3(4):611–9.

[6] Farid H,*"Image forgery detection – a survey"*, IEEE Signal Processing Magazine March 2009; 5:16–25.

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

[8] H. R. Chennamma, Lalitha Rangarajan *"Image Splicing Detection Using Inherent Lens Radial Distortion"* IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6, November 2010.pp 149-158.

[9] Zhenhua Qu, Guoping Qiu, and Jiwu Huang,*" Detect Digital Image Splicing with Visual Cues"*, LNCS 5806, pp. 247–261, 2009

[10] 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

[11] R. Tan, K. Nishino, and K. Ikeuchi, "Color constancy through inverse- intensity chromaticity space," *J. Opt. Soc. Amer. A*, vol. 21, pp. 321–334, 2004.

[12] J. van de Weijer, T. Gevers, and A. Gijsenij, "Edge-based color constancy," IEEE Trans. Image Process., vol. 16, no. 9, pp. 2207–2214, Sep. 2007.