International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 3, Issue 5, September-October 2014 **ISSN 2278-6856**

Survey on Technique for Illegal Modification Detection

Ms.Swapnali Somnath Pangre[1], Prof.Dr.S.S.Sane[2]

[1] Student of Master in Computer Engineering,
Department of Computer Engineering
K. K. Wagh Institute of Engineering Education & Research, Nashik
Savitribai Phule Pune University, Pune

[2] Head of Department
Department of Computer Engineering
K. K. Wagh Institute of Engineering Education & Research,Nashik
Savitribai Phule Pune University, Pune

Abstract

Digital images are easy to manipulate and edit due to availability of powerful image processing and editing software like picasa, Photoshop. Nowadays, it is possible to add or remove important part from an image without leaving any obvious traces of tampering. Verifying digital images and validating their contents, and identifying forgeries is one of the critical challenges for governmental and nongovernmental organizations and departments. The image integrity verification as well as identifying the areas of tampering on images without need of any expert support or manual process or prior knowledge of original image contents is now days becoming the challenging research problem. The method as in [16] deals with authenticity of images and is based on concept of using illumination color estimation. Recently a new method is also reported for efficient forgery detection particularly for faces in images , that estimates illuminant color 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. The method employs SVM for classification. The technique is capable of handling images containing two or more people and needs no expert interaction for detection of tampering.

Keywords: Digital Image, Image modification/Forgery, Color constancy, Forgery detection, Illuminant color, skin detection

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 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. 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 [1]. In this paper we are taking the review of digital image forgeries detection and their different techniques .In section II, we are talk about illuminant inconsistencies. In section III, different techniques are discussed those are offered by various researchers to provide hard statement on the authenticity of an image.

2. 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 [2] 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. 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. Figure 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.

Figure 1 : Color illumination

Kobus Barnard [17] 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 [18] 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. 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%). Otherwise, when the chromatic difference is less than 1 and the scene can be considered to contain one (approximately) uniform light source. Figure 2 shows the multiple light source images

Figure 2 : Multiple different light sources

2.1 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 technique is derived from the gray-edge hypothesis which believes that the average edge diversity in a picture is achromatic. Quite

the opposite to existing techniques, which are based on zero-order structure of the image, this method is based on the higher order structure of images. In addition, launch 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 different 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 unstable sizes. Moreover, the Minkovski norm highlights strong derivatives over fragile derivatives, so that specular edges are better exploited.

2.2 physics-based inverse-intensity chromaticity space estimates

Statistics-based schemes require many surface colors and become error prone when there are only a few surface colors. Quite the opposite, dichromatic-based methods can successfully handle consistently colored surfaces but cannot be applied to highly textured surfaces, as they need precise color segmentation. R. Tan, K. Nishino, and K. Ikeuchi[11] introduces a single integrated scheme to estimate illumination chromaticity from single colored and multicolored surfaces and require only uneven highlight region without segmenting the colors inside them. This technique gives relationship between illumination chromaticity and image chromaticity. Benefits of techniques are the capability to deal with either multiple surface color or a single surface colors, color segmentation enclosed by highlight parts 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.

3.Review of Digital Image Forgery Detection

Illumination-based methods for forgery detection are either geometry-based or color-based. In geometry-based schemes center of attention is on detecting inconsistencies in light source spots between particular objects in the picture [5]–[11]. Color-based schemes search for inconsistencies in the interactions between object color and light color [2], [12], [13]. Johnson & Farid showed that under some simplifying assumptions, arbitrarily complex lightning environments can be approximated with a low-dimensional model[7]. They showed how the parameters of a reduced version of their model can be estimated from a single image and how that model can be used to detect consistencies and inconsistencies in an image. Further, the efficacy of this approach on a broad range of simulated images, photographic images, and visually plausible forgeries were tested. In each case, the model parameters was well approximated, from which differences in lighting can typically be detected. There are, however, instances when different lighting environments give rise to similar model coefficients—in these cases, the lighting differences are indistinguishable Kee and Farid further extended this approach to exploiting known 3-D surface geometry[9]. Their approach removes the ambiguities in the earlier techniques and hence allows for a more powerful forensic analysis. Alongwith the 3-D estimation where the model was derived by collecting a set of 3-D laser scanned faces and projecting them into a lower-dimensional linear subspace 3-D model registration was done by maximizing an objective function over the camera intrinsic and extrinsic parameters that aligns the 3-D model to the image of the face. Their technique involved registering a 3-D face model with the 2-D image using manually annotated facial landmarks. But that technique cannot be extended to arbitrary object even though a 3-D model can be generated for it. Gholap and Bora [12] put forth the physics-based illumination cues to image forensics. They represented the colors of pixels around specular highlights in each object of the image in the r-g plane by straight dichromatic lines. If these lines intersect at points not close to one another, an evidence of forgery is shown. However this method does not perform well in the photographs involving the human skin as the cluster of human skin color lies near that of the illuminant colour. Moreover in order to easily identify the chromaticity lines in color space, one should first obtain a rough estimate of the specular region. But the specularity segmentation on real world images is challenging [15]. Additionally, specularities have to be present on all regions of interests, which limits the methods applicability in real world scenarios. To avoid the problem in [15], Wu and Fang[13] assume purely diffuse (ie. Specular- free) 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 indicator for tampering. But the method requires the manual selection of a reference block where the color of the illuminant can be reliably estimated. Wu and Fang implicitly create illuminant maps and require comparison to a reference part of image. However, different choices of reference parts of image lead to different results and make the method error-prone. Andrew C.[19] proposed new approach for forgery detection he describe a novel approach for image forgery problem. Rather than focusing on the statistical differences between the image textures, Author identify that images from digital cameras contain traces of resampling as a result of using a color filter array with demosaicing algorithms. Author identify that estimation of the actual

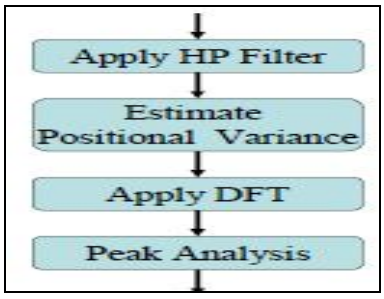

Figure 3: Forgery detection using DFT

demosaicing parameters is not essential; rather, detection of the existence of demosaicing is the key. The in-camera

processing (rather than the image content) distinguishes the digital camera photographs from computer graphics. Figure 3 show the working. Jiayuan Fan, Hong Cao, and Alex C. Kot,[21] proposed a new scheme to compare statistical image noise features with three selected EXIF header features, which are strongly related with camera shot settings. In addition of these noise features, this scheme exclusively disqualified the sharp image area to diminish the undesirable crash caused by different image contents on features. Also through includeing the second-order image noise features and sequential floating forward selection, author derived a set of noise features that are interrelated with a target EXIF feature and simultaneously, the correlation is delicate to image manipulations. By inventing each EXIF feature as a slanted average of its selected noise features, author engaged a least squares solution to solve the regression weights from the intact images. These weights agree to estimate the target EXIF feature parameters from the selected noise features.It is hard to beat proposed system by simply recalibrating the three EXIF values on influenced images as it is tough to meet the three EXIF-image limitations linked with split, secure speed and ISO, concurrently. Table 1, Shows the comparison Comparison of different Digital Image Forgery Detection Tools / Techniques / Algorithms [22].

Table 1: Comparison of different Digital Image Forgery Detection Tools / Techniques / Algorithms

Sr. No.	Digital Image Forensic Tools / Techniques / Algorithms	Works for	Domain	Merits	Demerits
1.	Detecting Lighting Inconsistencies	Effective on both synthetically generated images and natural photographs. Manipulations in images in this technique may require the creation or removal of shadows and lighting gradients	Efficiently work for Infinite Light Source (3-D), Infinite light Source (2-D), Local Light Source (2-D) and Multiple Light Sources.	This method assumes nearly Lambertian surface for both the forged and original areas and might not work when the object does not have a compatible surface, when pictures of both the original and forged objects were taken under approximately similar lighting conditions.	This system also may not work during a cloudy day when no directional light source is present.
2.	Detecting Inconsistencies through Lateral Chromatic Aberrations	Efficient on detecting tampering in visually plausible forgeries.	This approach for detecting tampering is effective when the manipulated region is relatively small.	This approach is efficient for detecting digital tampering in synthetic and real images.	This model fails to estimate Longitudinal Chromatic aberrations and other forms of optical distortions.
					This approach also fails when the manipulated region is relatively very large.
3.	Detection By Classification of Textures in Copy-Move Forgery	Effective on both synthetic and real images.	This method is limited to one particular case of forgeries, when a certain part of the image was copied and pasted somewhere else in the same image (e.g. to cover an object).	Efficient for detecting forgery in small copy areas.	It is very difficult to discover tampered areas in images. Also, Exhaustive search technique used in detecting copy-move forgery is quite computationally expensive.
4.	Principal Component Analysis (PCA) in Duplicated Image Regions	Efficient on plausible / credible digital forgeries	An efficient technique that automatically detects duplicated regions in a digital image.	Good for minor variations due to additive noise and lossy compression.	May fail to detect considerable large changes. Little doubt is there that counter-measures will be created to foil this technique

4.CONCLUSION AND FUTURE WORK

Techniques and methodologies for validating the authenticity of digital images and testing for the presence of tampering and manipulation operations on them have recently attracted attention. detect forgery in the digital images is one of the challenges of this exciting digital age. The sophisticated and low-cost tools of the digital age enable the creation and manipulation of digital images without leaving any detectable traces. As a end result, the validity of images can't be taken for granted, especially when it comes to legal photographic evidence. Thus, the problem of establishing image authenticity has become more complex with easy availability of digital images and free downloadable image editing software leading to diminishing trust in digital photographs. Another common manipulation in tampering with portions of the image is "copy-move". Spotting digital fakes by detecting inconsistencies in lighting is another method.To improve the accuracy in future we can use the different technique such as color constancy and skin detection.

5.ACKNOWLEDGEMENT

I am thankful to my guide Prof.Dr.S.S.Sane,for his guidance and encouragement . Their expert suggestionsand scholarly feedback had greatly enhanced the effectiveness of this work.I would like to express the deepest appreciation 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] 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

[22] Kusam, Pawanesh Abrol and Devanand "Digital Tampering Detection Techniques: A Review" BIJIT - BVICAM's International Journal of Information Technology

AUTHOR

Ms.Swapnali Pangre received the Diploma degree from K.K.Wagh Polytechnique MSBTE in 2007 and B.E. degrees in Computer Engineering from K. K. Wagh Institute of Engineering Education & Research Savitribai Phule Pune University in 2010. Currently,she is working toward the M.E. degree at the . Savitribai Phule Pune University,Pune. Her main interests include digital forensics, pattern analysis, data mining, machine learning ,Information Security and image processing.

Prof.Dr.S.S.Sane Vice Principal, Professor & Head of Dept. of Computer Engineering, K K Wagh Institute of Engineering Education & Research, Nashik