International Journal of Engineering Trends and Technology (IJETT) – Volume 18 Number 6 – Dec 2014

Exposing Digital Image Forgeries by Illumination Color Classification

Ms. Shraddha R Asati [#1], Mr. P.R.Pardhi [*2]

M.Tech Scholar, CSE Department, SRCOEM, Nagpur, India[1]

Assistant Professor, CSE Department, SRCOEM, Nagpur, India[2]

Abstract— **For years, photographs have been used to document space-time events and they have often served as evidence in courts. Photographers are able to create composites of analog pictures, but this process is very time consuming and requires expert knowledge. Today, however, advanced digital image editing software makes image alterations straightforward. These challenges our trust in photographs and, in particular, questions pictures as evidence for real-world events. In this paper, we examine one of the most common forms of photographic operation, well-known as image composition or splicing. In this work, we make an significant step towards reducing user interaction for an illuminant-based tampering decision making. We offer a new semiautomatic method that is more reliable than previous approaches. In this method we propose the method to detect the forensic in the photography. For that here we use the SVM classifier for the forensic detection. Initially we identify the illuminant map in the image. We find the face from the photography. For the face detect here we use the violo john method. After face detection we identify the GLCM (Gray Level Co-Occurance Matrix). In GLCM is the statistical information of the image such as energy, entropy, correlation sum of energy and sum of correlation are calculated. And also we extract the LBP feature. The extracted feature will pass to the SVM classifier for the training. SVM is stands for Support vector machine. It is a binary classifier. It is a kernel based learning classifier. The trained classifier will predict about the image whether it is original or forensic image.**

I. INTRODUCTION

Lots of digital document are generated by multiple devices and spread by magazines, websites television and newspapers. In all these Communication channels, images are a important tool for communication. And, it is not difficult to use computer graphics and image processing techniques to operate images. Image forgery means manipulation of digital image to conceal some meaningful or useful information of the image. There are some cases where it is difficult to identify the edited region from the original image. So the question is how image forgery is performed? Advanced digital image editing software makes image alteration easy. The easy availability of digital editing tool makes manipulation and alteration very easy and as a result forgery detection becomes a difficult problem.

In this paper, we discuss one of the most important forms of photographic manipulation, known as image composition or image splicing. Image is forgered by composition of the original image that is known as analog picture. As evidence in court forgered image plays an important role. One such example is shown in Fig. 1, is a modified image in which there are group of girls. The girl on the right hand side is inserted.

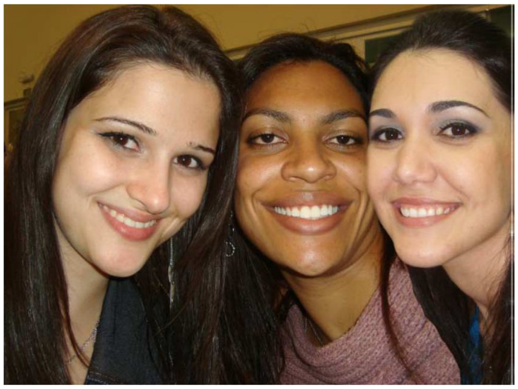

Fig.1. Example of a spliced image involving people.

A. Forgered Image

Today digital images play very vital role in areas like forensic investigation, insurance processing, intelligence services, surveillance systems, medical imaging and journalism. With the improvement of technology and availability of fast computing resources, it is not very easy to manipulate or forge the digital images. Before coming to the discussion of forgery detection methods; it is necessary to know about the different types of tampering done with various digital images. There are many ways to classify the image tampering based on different points of view. Generally; we can say that the most frequently performed operations in image tampering are:

- Hiding or removing a region in the image.
- Adding a different object into the image.
- Misrepresenting the important image information.

Copy move image tampering is one of the commonly used techniques to hide or manipulate the content of the image. Some part of the same image or some new image is pasted on another part of image. To identify the region of some other image statistical methods may work but if the region pasted belongs to the same image then it is not easy to detect this forgery. Many approaches have been suggested to detect this type of forgery.

II. RELATED WORK

Illumination-based approaches for forgery detection are either color-based or geometry-based. Geometry-based approaches focus at identifying inconsistencies in light source positions between specific objects in the scene. Color-based approaches examine for inconsistencies in the interactions between object color and light color. Two approaches have been suggested that usage the direction of the incident light for exposing digital forgeries. Johnson and Farid suggested a method which calculates a low-dimensional descriptor of the lighting environment in the image plane (i.e., in 2-D). It calculates the illumination direction from the intensity distribution along physically annotated object boundaries of similar color.

Kee and Farid extended this method to manipulating known 3-D surface geometry. In the instance of faces, a dense grid of 3-D normals improves the estimate of the illumination direction. To do this, a 3-D face model is registered with the 2-D image using physically annotated facial landmarks.

Johnson and Farid also suggested composite image detection by exploiting specular highlights in the eyes. In a subsequent extension, Saboia et al. automatically classified composite images by extracting extra features, such as the viewer position. The applicability of both methods, however, is somewhat restricted by the fact that people's eyes must be visible and available in high resolution.

Gholap and Bora presented physics-based illumination cues to image forensics. The authors observed variations in specularities based on the dichromatic reflectance model. Specularity segmentation on realistic images is challenging. Therefore, the authors require physical annotation of specular highlights. Additionally, specularities have to be present on all areas of interest, which bounds the method's applicability in real-world scenarios.

To avoid this problem, Wu and Fang adopt purely diffuse (i.e., specular-free) reflectance, and train a mixture of Gaussians to choose a appropriate illuminant color estimator. The angular distance to illuminant estimates from selected regions can then be used as an indicator for tampering. Unfortunately, the technique requires the physical selection of a "reference block", where the color of the illuminant can be consistently estimated. This is a important restriction of the technique.

Riess and Angelopoulou followed a different method by using a physics-based color constancy algorithm that works on partially specular pixels. In this method, the automatic finding of highly specular regions is avoided. The authors suggest slicing the image to estimate the illuminant color locally per segment. Recoloring every image region giving to its local illuminant estimate yields a so-called illuminant map. Improbable illuminant color estimates point towards a worked region. Unfortunately, the authors do not offer a numerical decision criterion for tampering detection. In the field of color constancy, descriptors for the illuminant color have been widely studied. Most research in color constancy focuses on consistently illuminated scenes containing a single dominant illuminant. Though, in order to use the color of the incident illumination as a sign of image tampering, we require various, spatially-bound illuminant estimates. So far, limited work has been done in this direction.

Ebner discussed an early approach to multi-illuminant estimation. Assuming smoothly blending illuminants, the author proposes a diffusion process to recover the illumination distribution. Unfortunately, in practice, this approach over smooth's the illuminant borders. Gijsenij et al. offered a pixel wise illuminant estimator. It permits segmenting an image into regions illuminated by different illuminants. Differently illuminated regions can have crisp changes, for example between sunlit and shadow areas. Although this is an interesting approach, a single illuminant estimator can constantly fail.

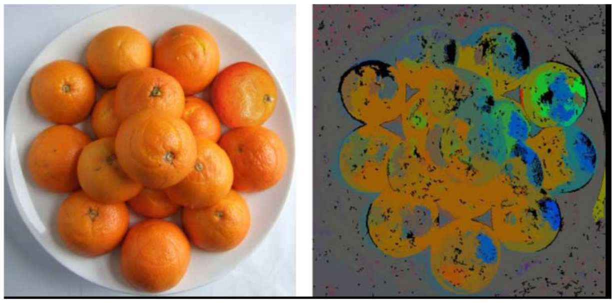

Fig.2. Example of illuminant map that directly shows an inconsistency.

Hence, for forensic purposes, we select a scheme that combines the results of various illuminant estimators. Previously, Kawakami et al. suggested a physics-based method that is custom-tailored for discriminating shadow/sunlit areas. In this work, we consider the limit to outdoor images overly limiting. In this work, we build upon the ideas by and. We use the comparatively rich illumination information provided by both statistics-based color and physics-based constancy approaches. Decisions with respect to the illuminant color estimators are totally taken away from the user, which distinguishes this work from previous work.

III. PROPOSED WORK

In this method we propose the method to detect the forensic in the photography. For that here we use the SVM classifier for the forensic detection. Initially we identify the illuminant map in the image. We find the face from the photography. For the face detect here we use the violo john method. After face detection we crop the face image and calculate the canny edge and HOG feature. The technique counts occurrences of gradient orientation in localized portions of an image. This method is similar to that of edge orientation histograms. The method extracts invariance to geometric and photometric transformations for object orientation. After that we identify the Statistical analysis of structure Information (SASI). In SASI is the statistical information of the image such as energy, entropy, correlation sum of energy and sum of correlation are calculated. The extracted feature will pass to the SVM classifier for the training. SVM is stands for Support vector machine. It is a binary classifier. It is a kernel based learning classifier. The trained classifier will predict about the image whether it is original or forensic image.

IV. EXPECTED RESULTS

The regular images have been taken for the analysis of the project. The probable results are from both the original and edited images.

V. CONCLUSIONS

In this approach, new technique for detecting forged images of people using the illuminant color has been discussed. The illuminant colors a physics-based method and using a statistical gray edge method which exploits the inverse intensity chromaticity color space has been estimated. This illuminant map is treated as texture maps. An information on the distribution of edges on illuminant maps are extracted.

In order to define the edge information, a new algorithm based on the HOG descriptor and edge-points, called HOGedge is proposed. Respectable results are also achieved over internet images and under cross-database training/testing. The proposed method requires only a least amount of human interaction and provides a crisp statement on the authenticity of the image. Additionally, it is a major progress in the exploitation of illuminant color as a forensic cue.

REFERENCES

[1] Tiago Jose de Carvalho,Christian Riess,Elli Angelopoulou and Helio Pedrini "Exposing Digital Image Forgeries By Illumination Color Classification" IEEE Trans. Inf. Forensics Security ,Vol. 8, no. 7, pp. 1182 - 1194, July 2013.

[2] R. Kawakami, K. Ikeuchi, and R. T. Tan, "Consistent surface color for texturing large objects in outdoor scenes," in Proc. IEEE Int. Conf. Comput. Vision, 2005, pp. 1200–1207.

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

[4] 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.

[5] J. Lukas, J. Fridrich, andM.Goljan, "Digital camera identification from sensor pattern noise," IEEE Trans. Inf. Forensics Security, vol. 1, no.2, pp. 205–214, Jun. 2006.

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

[8] S. Bianco and R. Schettini, "Color constancy using faces," in Proc. IEEE Comput. Vision and Pattern Recognition, Providence, RI, USA, Jun. 2012.

[9] 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.

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

[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.

[13] 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.