"IMAGE FORENSIC ANALYSES THAT ILLUMINATION PROCESSES THE HUMAN VISUAL SYSTEM"

[1]SWAPNIL DHARME
NUVA College of Engineering & Technology, Kalmeshwar, Nagpur
swapnildharme@gmail.com
[2]POOJA THAKRE
NUVA College of Engineering & Technology, Kalmeshwar, Nagpur

ABSTRACT: *Digital Photo images are everywhere, on the covers of magazines, in newspapers, in courtrooms, and all over the Internet. We are exposed to them throughout the day and most of the time. Ease with which images can be manipulated; we need to be aware that seeing does not always imply believing. We propose methodologies to identify such unbelievable photo images and succeeded to identify forged region by given only the forged image. Formats are additive tag for every file system and contents are relatively expressed with extension based on most popular digital camera uses JPEG and Other image formats like png, bmp etc. We have designed algorithm running behind with the concept of abnormal anomalies and identify the forgery regions. Today, Powerful digital image editing software makes image modifications straightforward. This undermines our trust in photographs. In this paper, one of the most common forms of photographic manipulation, known as image composition or splicing is analyzed. A forgery detection method that exploits subtle inconsistencies in the color of the illumination of images. The proposed approach is machine-learning based and requires minimal user interaction. The technique is applicable to images containing two or more people and requires no expert interaction for the tampering decision. Here, the existing work can be extended by using advanced face detection method using skin tone information and edges. A lighting insensitive face detection method based upon the edge and skin tone information of the input color image is proposed. From these illuminant estimates, we extract texture- and edge-based features which are then provided to a machine-learning approach for automatic decision-making.*

***Keywords*:** JPEG, Illumination, detection, forgery

1. INTRODUCTION

Image processing is a wide concept and in basically here, the digital image processing is discussed. On analyzing this, one of the most common forms of photographic manipulation known as image composition or splicing is found. An image is forge red by splicing the original image that is called as analog pictures [1]. So that the forge red image plays as a vital role in courts for evidence. By having the forge red image many rumors has been arised. The forgery image is not viewed be different from the original image. To differentiate both the images a SVM classifier is used.

Figure1. How can one assure the authenticity of a photograph? Example of a spliced image involving people.

There are two processes which are used to detect the images whether it is forge red or real one. Trained examples are stored in the database and are put into SVM classifier [5].

The images in the support vector machine are used to classify the real image and forge red image. So by following all the steps which are described in the list of the modules, a forge red image is detected. A brief explanation is given in every segment for which they are used and demonstrate how the forgery picture is detected [6]. Based on the fact that no two images 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 images to create a composite image is not the same. Though editing the image content is easy, it is difficult or highly impossible to adjust the illuminant conditions comparable to other image taken for splicing. Most of the image editors does not concentrate or notice the difference in image illuminancy. Therefore the illuminant estimates of the image can be a powerful tool in forensic analysis of splicing detection. Reiss and Angelopoulos [7] proposed that illuminant estimates from local image regions can be analyzed by human experts to detect the illumination inconsistencies. This is very challenging, as most of the illumination features eludes the human visual system. To minimize or to fully eliminate the need of human experts in digital image forgery detection, the system should be automated [8]. The introduction of a classification scheme that functions based on machine learning can accomplish this task. The classification scheme categorizes the images into two families: consistent and inconsistent based on the estimated illuminant conditions and texture – cum – edge features.

2. RELATED WORK

These image forgery detection approaches can be divided into two categories: 1) active and 2) passive-blind. The active approach may focus on data hiding (e.g. watermarking, steganography) and digital signatures which is based on prior information about the image [2]. On the other hand, the passive approach on image forgery detection does not require any prior information of image to be investigated. It is based on the fact that editing the image content may result in uneven distribution of image features. (e.g. statistical changes). The forgery detection techniques that are based on illuminant estimation can fall on two categories: 1) geometry – based and 2) color based Geometry based methods focus on inconsistencies in lighting whereas color based methods describes how chromaticity of an object varies with different intensities of light. It was Johnson and Farid who proposed that illuminant inconsistencies can be used for splicing detection. Kee and Farid [5] extended this approach to analyze the 3-D surface geometry of the objects in the image. Johnson and Farid also showed that by simplifying some assumptions made on estimating lighting conditions, the complex lighting environment can be approximated and represented in low dimensional model. Then the parameters of the low dimensional model can be estimated and used in detecting the inconsistencies in lighting. It relies on acquiring multiple images of the same scene as the complex light source direction identification is very difficult using a single image. Johnson and Farid [9] and Saboia *et al.* [11] proposed image splicing forgery detection using the specular highlights on the eye of the people in images. These methods have limited application as it requires that eyes of the people should be clearly visible. Another method for splicing forgery on images involving reflective surfaces on scene was proposed by O'Brien and Farid [8]. It is based on the assumption that reflective surface is flat and linear projection. It has limited application and ineffective when the reflective surface is curved. Riess and Angelopoulos [3] proposed a new approach for color constancy. It is a physics – based color constancy algorithm that exploits the inverse intensity – chromaticity color space. It segments the image regions and estimates the dominant illuminant color for each region. They did not provided the results of illuminant estimates to an objective algorithm. So the analyses of extracted illuminant features are left to human experts. Manual analysis on illuminant features is more error prone and time consuming. This is a drawback of this method.

3. METHODOLOGY AND IMPLEMENTATION OF DETECTING DIGITAL IMAGE FORGERY

.

Photo image forgery is classified in to two categories. The first class of image forgeries includes Images tampered by copying one area in an image and pasting it onto another area. It is called as Copy-Move Forgery or Cloning. The second class of forgeries is copying and pasting areas from one or more images and pasting on to an image being forged. The image processing community formally refers to this type of image as an image "composition," which is defined as the "digitally manipulated combination of at least two source images to produce an integrated result". It is also called as Copy-Create Image Forgery.

After applying JPEG image compression algorithm the result will be obtained in the following form:

3.1 METHODOLOGY BASED ON JPEG COMPRESSION ANALYSIS AND ALGORITHM FOR FORGERY DETECTION

Block-based processing is a popular technique used in image processing where the image is broken into sub-parts or equal squares. Each block is considered as a sub-image. This method is allows recursive type processing, with the sub-processing resembling a "divide and conquer" approach. Block-based processing is useful because the calculations performed are influenced by only the information present in that particular block. Block-based processing is employed in image compression. JPEG compression is block-DCT based, and a popularly used image compression technology. The compression standard set forth by the International Standards Organization

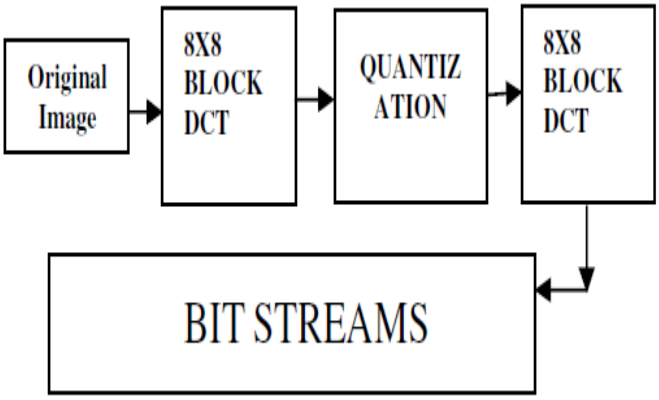

Figure 2: Block Diagram JPEG Compression

3.2 METHOD BASED ON DIRECTION FILTER USING JPEG IMAGE ANALYSIS

General forgery detection methods are based on JPEG compression threshold which work for only JPEG image format. Today digital cameras support other image formats also. For this reason we propose novel methodology for photo forgery detection based on standard deviation based edge detection that detects the edges present in all directions. The main steps of proposed algorithms are based on Image Edge Detection and tampering localization.

Figure 3: Random Selection of Global Threshold Setting and Evaluation used in Jpeg compression algorithm for Photo Forgery Detection

4. EXISTING SYSTEM

In existing, many methods have been proposed for detecting the forged images. Tiago jose de carvalho proposed in [1] that illumination-based methods for forgery detection are either geometry-based or color-based [6] [7] [8] has been used. Geometry-based methods focus at detecting inconsistencies in light source positions between specific objects in the scene has been used. Color-based methods search for inconsistencies in the interactions between object color and light color [2] has been used. An early approach of multi-illuminant estimation has been done. In this smoothly blending illuminants used a diffusion process to recover the illumination distribution. By exploring with this pixel wise illuminant estimator is used. It allows segmenting an image into regions illuminated by distinct illuminants. Differently illuminated regions can have crisp transitions, for instance between sunlit and shadow areas. The issues of the existing system are it over smooth's the illuminant boundaries. And it does not scale well on smaller image regions. A single illuminant estimator always fails.

5. PROPOSED SYSTEM

We will try to design a new system for solving all the problems occurs in the existing system. We used here new approaches for images with well implementation

6. CONCLUSION

This paper focuses on methods to detect digital forgeries created from multiple images called as copy-create image forgeries. Some forgery images that result from portions copied and moved within the same image to "cover-up" something are called as copy-move forgeries. Therefore, the experimental design and analysis herein focuses on copy-create and copy-move image forgeries. A crafty individual, who wants to perfect an image forgery, with time not a factor, can usually give any detection method trouble. If image tampering occurs in a compressed then JPEG Block methodologies is to support and predict forgery region along with different image format at the same time uncompressed image and then that image is converted to the JPEG image format, the JPEG Block Technique will fail to capture evidence of tampering. This conversion process destroys all proof of tampering since the original tampering does not affect any JPEG blocks. Additionally, any image tampering performed on an image prior to an image size reduction will eliminate detectable anomalies for the direction filter technique.

Though the proposed system is developed to detect the splicing on images containing multiple faces, it can also be used to detect splicing done on other scene objects. The proposed system requires only a minimum human interaction in forgery detection. User interaction is needed only to select the bounding boxes of the human faces on the image. The final decision on image forgery is automated to eliminate the need for a human expert to take tampering decision. The illuminant estimate can be a powerful forensic tool; however it is prone to estimation errors. Further improvements can be achieved when advanced color constancy algorithms are used for illuminant estimation. This is the subject of future work.

7. REFERENCES

[1] T.J. Carvalho, C. Riess, E. Angelopoulo, H. Pedrini, and A. Rocha "Exposing Digital Image Forgeries by illumination Color Classification", IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1182–1194, July 2013.

[2] Anderson Rocha, Walter Scherer, Terrance Boult, Slome Goldenstein "Vision of the Unseen: Current Trends and challenges in Digital Image and Video Forensics", ACM – Computer Survey Paper Vol 5, 2010.

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

[4] 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.

[5] E. Kee and H. Farid, "Exposing Digital Forgeries from 3-D Lighting environments", in Proc. IEEE Int. Workshop on Inform. Hiding, 2007, pp. 311 – 325.

[6] 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.

[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] 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.

[9] 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.

[10]. 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.

[11]. 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.

[12] 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.

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

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

[15]. 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.