IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP 10-13
www.iosrjournals.org

Analysis of Digital Image Splicing Detection

P.Sabeena Burvin, PG scholar, J.Monica Esther, Asst Prof,
Department of Information Technology, Francis Xavier Engineering College, Tirunelveli
Department of Information Technology, Francis Xavier Engineering College,Tirunelveli.

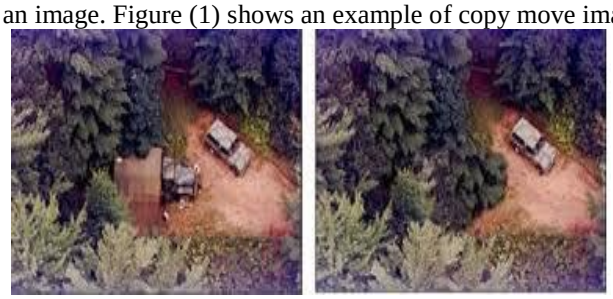
Abstract: *The availability of photo manipulation software has made it unprecedentedly easy to manipulate images for malicious purposes. One of the most common forms of digital image or photographic manipulation operation is known as image splicing or image composition. It is a process that's crops and paste regions from same or separate sources. In this paper, we analyze various automatic image forensic techniques for detecting digital image splicing.*

Keywords: *image forensic, image forgery, image composition, image retouching, copy-move image forgery*

I. Introduction

Digital Image Forgery Detection is an important field in Image Processing, because digital images are used in many social areas like in courts where they are used as evidence. In information channels like newspapers, magazines, websites and televisions, digital images are powerful tool for communication. Unfortunately, it is easy to use computer graphics, image editing software and image processing techniques to manipulate the images. These manipulated images create some unwanted problems in information channels.

Basically there are three different types of digital image forgery: Copy-Move image forgery, Image Splicing image forgery and Image Retouching image forgery. In Copy-Move image forgery, one part of the image is copied and pasted on other part of the same image [1]. In other words, the source and destination of the modified image originated from the same image. This is usually done in order to conceal certain details or the duplicate certain aspects of an image. Figure (1) shows an example of copy move image forgery.



1a) Original image 1b) Forged image

Figure1. An example of copy move image forgery

In Image Splicing, two images are combined to create one tampered image or it is a technique that involves a composite of two or more images, which are combined to create a fake image [2]. Figure (2) shows an example of image splicing image forgery.

2a) Original image 2b) Forged image

Figure2. An example of image splicing image forgery

3a) Original image 3b) Forged image

Figure3. An example of image retouching image forgery

In Image Retouching, the images are less modified. It just enhances some features of the image. There are several subtypes of digital image retouching, mainly technical retouching and creative retouching [3]. Figure (3) shows an example of image retouching image forgery.

II. Image Splicing

In this paper, we analyze about image splicing image forgery. Image splicing is a common form of digital image manipulation or image forgery. It is one such type of tampering; Image splicing is also called as image composition. The basic definition of image splicing is a process that crops and paste regions from same or separate sources. The following figure (4) shows one of the example form of image splicing process and its steps [4].

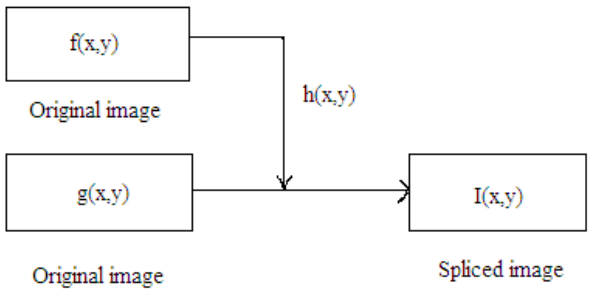
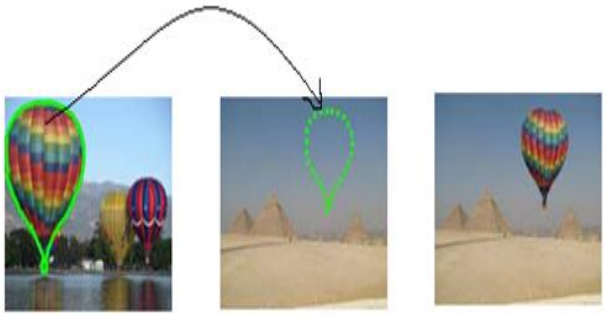


Figure4. The steps of image splicing, f(x, y) and g(x, y) are original images, h(x, y) is a part of f(x, y) which is insert into g(x, y) and generate spliced image I(x, y). Perhaps f(x, y) and g(x, y) is the same image.



5a.Source image 5b.Target image 5c.Composite image

Figure5: The Process of Image Splicing Forgery

As shown in above figure (5), by coping a spliced portion from the source image (5a) into a target image (5b). One can create a composite picture (5c) or scenery to cheat others with the help of state-of-art image editing software [5], even non-professional users can perform splicing without much difficulty.

III. Analysis of Image Splicing Detection

Zhehua and Guoping proposed an automatic detection framework to identify a spliced image, which is fully based on Human Visual System model in which visual saliency and fixation are used as a forensic cue [6]. This technique provides a convenient way to locate splicing boundaries, but this system needs some training for users.

Servinc and Ismail proposed a method based on the neighbor bit planes of the image. The basic idea is the correlation between the bit planes as well as the binary texture characteristics within the bit planes will differ between an original and a spliced image, which is considered for detecting splicing [7]. This method

provides better performance at both stronger and weaker level of manipulation, but in order to identify the spliced image this method requires various image forensic detectors.

Farid method consider the fact that while creating a digital composite image the matching of lightning conditions of digital image is difficult between the individual photographs[8], this inconsistencies in lighting can be used as a factor for detecting digital tampering. But the main drawback with this approach is it is not applicable for indoor images.

Alin and Farid proposed a method to detect the spliced image by detecting traces of resampling. When creating digital forgeries, it is often necessary to scale, rotate or distort a portion of an image. This process involves resampling the original image onto a new lattice, which resampling rates used for exposing digital forgeries [9]. This method offers a complementary approach to authenticating digital images, but it's only applicable for uncompressed TIF &JPEG image with minimal compression.

Alin and Farid again proposed an automatic method for detecting traces of digital tampering in lossless & lossy compressed image by using color Filter Array[10], Most digital cameras employ a single sensor in conjunction with a CFA, where the missing color samples are interpolated from these recorded samples to obtain a three channel color image. This interpolation introduces specific correlations which are likely to be destroyed when tampering with a digital image. As such, the presence or lack of correlations produced by CFA interpolation can be used to declare it as a forgery. This technique works in the absence of any digital watermark or signature to authenticating digital images, but this will not be the case in practical.

Johnson and Farid proposed a method based on the specular highlights that appear on the eye are a powerful cue to shape, color and location of the light source [11].Inconsistencies in these properties of light can be used as evidence of tampering. It can applicable to arbitrary objects, but this method only determines the direction to the light source within one degree of ambiguity.

Riers & Angelopoulou proposed illumination color as a new indicator to distinguish the original and manipulated image [12]. The basic idea is that if an image has been manipulated, the transition between the illuminants should be disturbed. The disturbed illuminants can be used as a best indicator for identifying image authenticity; but it requires the original image for comparison process.

Feng and chang proposed a fully automatic spliced image detection method, which is based on consistency checking of camera characteristics among different areas in an image [13], From each area using geometric invariants camera response functions (CRF) is determined. The boundary between the authentic or spliced regions is segmented by classifiers. This method provides high performance, but the rate of detection of splicing is not to the expected level.

Chennamma & Lalitha proposed a detection method based on the spherical lens which introduces radial distortion [14]. This radial distortion parameter estimated and their consistency is verified for the detection of splicing. The efficiency of this method depends on the resolution of the images.

Eric and Hany put forth a method which estimates the lightning conditions of the digital composite image in 3-D environment and the same estimate is used as a evidence for detecting tampering [15]. This method is very powerful in tampering analysis.

Farid & Bravo proposed an automatic detection method for identifying faked pictures without the involvement of HVS (Human Visual System) [16], which shows the visual system is remarkably improper to detecting geometric inconsistencies in shadows, reflection and perspective distortion. But the process of detection is time consuming.

Xuemin & Zhen locate the splicing area by exploiting illuminant color inconsistency [17]. This method detects image splicing and also locates the spliced region, is not applicable for indoor images and original image is necessary to find the duplication or manipulation.

Pravin, Sudha and Ser proposed a novel method for detecting image splicing using discrepancies in motion blur. In which they used motion blur estimation through image gradients in order to detect inconsistencies between the spliced region and rest of the image [18]. This method needs very less human intervention, improves robustness and efficiency.

Shinteng & Tszan proposed a fast and effective forgery detection technique for copy-move and image splicing forgery, which focuses on JPEG format image and detect both image forgeries [19]. This method is mainly used to find the Copy-and-Paste operation of image regions from one image onto another.

James F.O'Brien & Harry proposed a new forensic technique has emerged to detect geometric or statistical inconsistencies that result from specific forms of Photographic manipulation [20], but the human visual system is needed to identify the corresponding points on objects and it's reflections.

Pan, Xing & Lyu describes a method based on the fact that the images from different origins tend to have different amount of noise introduced by the sensors [21]. They proposed an effective method to expose image splicing by detecting the inconsistencies in local noise variances. But the main this method is not able to detect the entire tampered region.

Kekre, Misha, Pallavi, Shede & Gupta proposed a new method based on image hashing, which is used to generate hash value for each image in the database [22], these hash values can be used for content based image retrieval, image database indexing, image authentication and also avoiding & mitigating the tampering of digital images. The only limitation of this technique is the original image is needed for find duplication.

Zahra Mohamadian and Ali Akbar pouyan proposed a method to detect forgery in digital images in uniform and non-uniform regions in which Zernike moments based detection approaches is used to detect flat copied regions [23]. If the images are rotated, scaled or distorted this method will fail to identify the forged image.

Munkhbaatar & Rhee proposed a blind forgery detection scheme using compatibility metrics based on edge blur and lightning directions [24]. The edge blur width is used to identify the discontinuities of edge in spliced image and the lightning directions are used to enlighten the image composition.

IV. Conclusion

Nowadays image splicing image forgery is becoming a common way the anti-social people are using to create the fake photographs and misusing them. So it is necessary to identify such kind of image manipulations. So many researches have already been carried out on image splicing. But the existing methods of detecting image splicing undergo the following challenges: original image is essential for revealing tampering, forgeries with indoor image and image resolution. We have analyzed several methods proposed in research papers to detect image composition to insist the necessity for image splicing detection. This field is still growing and a lot of research is needed to make Digital forensic more promising.

References

[1]. Prof. Unmukh Datta & Chetna Sharma, "Analysis of copy-move image forgery detection"; International journal of advanced research in computer science & electronics engineering(IJARCSEE), volume 2, issue 8, august 2013.

[2]. Types of digital image forgery, Available. https://www.google.co.in/?gfe_rd=cr&ei= HWocU7zx IOOD8Qf8wIDgCw#q=Types+of+digital+image+forgery.

[3]. http://www.slideshare.net/ahlamansari/image-forgery-and-security

[4]. Zhen zhang,ying zhou, jiquankang & yaan ren, "Study of digital image splicing detection", zhang zhen 660126.com, china.

[5]. http://www.ee.columbia.edu/ln/dvmm/downloads/AuthSplicedDataSet/AuthSplicedDataSet.htm.

[6]. Zhenhua Qu, Guoping Qiu, and Jiwu Huang.(Jan 8-10-2009) "Detect Digital Image Splicing with Visual Cues", 11th International Workshop, IH 2009, Darmstadt, Germany.

[7]. Bayram.S, I. Avcibas, B. Sankur, and N. Memon, (2005) "Image manipulation detection with binary similarity measures", in Proc. Eur. Signal Processing Conf. (EUSIPCO), vol. I, pp. 752–755.

[8]. Johnson and Hany, (2005) "Exposing digital forgeries by detecting inconsistencies in lighting", in Proc. ACM Workshop on Multimedia and Security, New York, NY, USA, pp. 1–10.

[9]. Hany Faridy and Alin C. Popescu, (Feb 2005) "Exposing Digital Forgeries by Detecting Traces of Re-sampling", Signal Processing, IEEE Transactions on (Volume:53 , Issue: 2).

[10]. Alin C. Popescu and Hany Faridy , (Oct 2005) "Exposing Digital Forgeries in Color Filter Array Interpolated Images", Signal Processing, IEEE Transactions on (Volume:53 , Issue: 10).

[11]. Johnson.M.K, (2007) "Exposing Digital Forgeries Through Specular Highlights on the Eye", 9th International Workshop on Information Hiding, Saint Malo, France.

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

[13]. Yu-Feng Hsu and Shih-Fu Chanhge, (2007) "Image Splicing Detection Using Camera Response Function Consistency and Automatic Segmentation", ICME, page 28-31, IEEE.

[14]. Chennamma.H.R and Lalitha Rangarajan, (Nov 2010) **"**Image Splicing Detection Using Inherent Lens Radial Distortion", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6.

[15]. Eric Kee and Hany Farid, (Dec 2010) "Exposing Digital Forgeries From 3-D Lighting Environments", Information Forensics and Security (WIFS), 2010 IEEE International Workshop.

[16]. Hany Farid and Mary J. Bravo, (2010) "Image Forensic Analyses that Elude the Human Visual System", SPIE THE INTERNATIONAL SOCIETY FOR OPTICAL ENGINEERING; Volume (7541); Media Forensics and Security conference.

[17]. Xuemin Wu, Zhen Fang, (2011) "Image Splicing Detection Using Illuminant Color Inconsistency", Third International Conference on Multimedia Information Networking and Security.

[18]. Pravin Kakar, N. Sudha, and Wee Ser, (Jun 2011) "Exposing Digital Image Forgeries by Detecting Discrepancies in Motion Blur", IEEE Transaction on Multimedia, Vol. 13, No, 3.

[19]. Shinfeng D. Lin and Tszan Wu, (2011) "An Integrated Technique for Splicing

[20]. and Copy-move Forgery Image Detection", 4th International Congress on Image and Signal Processing.

[21]. O'Brien and H. Farid, (Jan 2012) "Exposing photo manipulation with inconsistent reflections", ACM Trans. Graphics, vol. 31, no. 1, pp. 1– 11.

[22]. Xunyu Pan, Xing Zhang and Siwei Lyu, (April 2012) "Exposing Image Splicing with Inconsistent Local Noise Variances ", Computational Photography (ICCP), 2012 IEEE International Conference.

[23]. Kekre.H.B, Halarnkar.P.N and Shende.P, (Jan 2013) "Digital Image Forgery Detection Using Image Hashing", International Conference on Advances in Technology and Engineering (ICATE).

[24]. Zahra Mohamadian and Ali Akbar pouyan, (2013) "Detection of duplication Forgery in Digital Images in Uniform and Non-Uniform Regions", 15th International Conference on Computer Modelling and Simulation, UK.

[25]. Munkhbaatar Doyoddorj, Kyung-Hyune Rhee, (May 2013) "A Blind Forgery Detection Scheme Using Image Compatibility Metrics", Industrial Electronics (ISIE), 2013 IEEE International Conference on 28-31.