2321-8045 Science Park Research Journal Vol-1, Issue-8, 12th Sept 2013

PRIMARY ARTICLE

# Image Forgery Detection And Source Identification

Mahale Vivek Hilal[1],Ashok T.Gaikwad[2] And Charansing N. Kayte[3]

## ABSTRACT

With the ease of digital image manipulation, image forgery has become a common concern. The fast development of commercial image editing software's such as Adobe Photoshop dramatically increases the amount of doctored photographs circulated every day. First, various image forgery detection techniques are classified and then its generalized structure is developed. To restore the traditional trustworthiness on digital photos, image forensics analyses that can reliably tell the origin, integrity and authenticity of a given image are urgently needed. we propose several new image forensics tools. These forensics tools help expose common image forgeries, especially those easy-to-make forgeries, which can hardly be seen directly by human eyes.

**KEYWORDS :**

Digital Image Forensic .image Authentication. Forgeries Detection Sensor Noise

## INTRODUCTION

Photo manipulation has become more common in the age of digital cameras and image editing software[1][2]. There are two main interests, namely source identification and forgery detection. Source identification focuses on identifying the source digital devices (cameras, mobile phones, camcorders, etc) using the media produced by them, while forgery detection attempts to discover evidence of tampering by assessing the authenticity of the digital media (audio clips, video clips, images, etc)[1][2]. The tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our e-mail in-boxes, doctored photographs are appearing with a growing frequency and sophistication. Over the past five years, the field of digital forensics has emerged to help restore some trust to digital images. Digital watermarking has been proposed as a means by which an image can be authenticated[3][4]. Forensic tools that help establish the origin and authenticity of such digital images are essential to a forensic examiner[5, 6]. Identification of forged regions can prove to be vital when digital images are presented in court as evidence or scanned checks are used in banks. In this paper, I review several techniques and methods of image forgery detection and source Identification[2]. The past few years have seen a growth of research on passive digital image forgery detection which can be categorized at three levels (similar to those mentioned in [5]):

**1.Low Level.** Methods at this level use statistical characteristics of digital image pixels or DCT coefficients. For example, demosaicing or gamma correction during the image cquiring process will bring consistent correlations of adjacent pixels, whereas tampering will break up this consistency. Investigating double JPEG compression for tampering detection is an example of using statistical characteristics of DCT coefficients. Using a model of authentic images which tampered images do not satisfy for forgery detection also belongs to this level.

**Mahale Vivek Hilal[1], Ashok T.Gaikwad[2] And Charansing N. Kayte[3]**

From

[1]Department Of Computer Science , IMIST,Aurangabad

[2]Director, IMIST,Aurangabad

[3]Dept. of Digital and Cyber Forensic, Government Institute Of Forensic Science Aurangabad

Te Article is published on September 2013 issue & available at www.scienceparks.in

DOI: 10.9780/23218045/182013/32

In short, no semantic information is employed at this level.

**2.MiddleLevel.** At this level,we detect the trace of forgery operation which has some simple semantic information, like splicing1 caused sharp edges, blur operation after splicing and inconsistencies of lighting direction, etc.

**3.High Level.** i.e., semantic level. Actually, it is very hard for computer to use semantic information to do forgery detection because the aim of forgery is changing the meaning of image content it originally conveyed. But, sometimes it still works. For example, it does not make sense to have an image in which George W. Bush is shaking hands with Osama bin Laden.

As we know, at least in recent years, computers still have difficulties in high level image analysis. Nevertheless, they can be helpful in middle level and low level analysis. Actually, they are better than human at these two levels [5].

## IMAGE TAMPERING

To detect image tampering, we should know about image tampering operation itself first. In [8], the author divided digital forgery operation into six different categories: compositing, morphing, re-touching, enhancing, computer generating and painting. In fact, almost all state-of-the-art tampering detection technique aims at compositing operation. With powerful image editing tool (e.g. Photoshop or lazy snapping [7]), compositing tampered images is much easier and can result in much more realistic images. It always involves the selection, transformation, composition of the image fragments and the retouching of the final image [8].

Here, we want to emphasize that a tampered image means part of the content of a real image is altered. This concept does not include those wholly synthesized images, e.g. images completely rendered by computer graphics or by texture synthesis. In other words, an image is tampered implies that it must contain two parts: the authentic part and the tampered part [9].

## Low Level Digital Image Forgery Detection

Just like the roles of steganography and steganalysis, tampering creators and detectors are opponents. Since it is not hard to use digital image edit tool to make a sophisticated tampered image, which means less trace of tampering operation can be seen from content of the tampered image, many tempering detection algorithms have to focus on imaging process and image statistical characteristics.

## Middle Level Digital Image Forgery Detection

As we know, some image tampering operation will leave some semantic cues that can be used for us to detect forgery, such as splicing caused edges which are sharper and less smooth than other original edges in image. And sometimes there are inconsistencies of lighting direction in the composited image.

## DISCUSSIONS AND CONCLUSIONS

There is a growing need for digital image forgery detection. Many techniques, some of which were introduced in this paper, have been proposed to address various aspects of digital image forgery detection. We can find that most proposed forgery detection methods aim at detecting inconsistencies in an image, and the majority of them belong to the low level category. Although many of these techniques are very promising and innovative, they have limitations and none of them by itself offers a definitive solution [10].

Therefore, we can hope that as more detection tools(source) are developed it will become increasingly more difficult to create convincing forgery digital images. Besides, as the suit of detection tools expands we believe that it will become increasingly harder to target attack each of the detection schemes [7]. However, there are several issues requiring attention when we want to propose new approaches.

## REFERENCES

1.S.Murali, Govindraj B. Chittapur , Prabhakara H. S and Basavaraj S. Anami3,"Comparison And Analysis Of Photo ImageForgery Detection Techniques".

2.Dr.kayte Charansing N.,Vivek Hilal Mahale,Dr. Ashok T.Gaikawad, "A survey on digital image forgery detection

techniques and forensic methods"

3.I. J. Cox, M. L. Miller, and J. A. Bloom, Digital Watermarking. San Francisco,CA: Morgan Kaufmann, 2002.

4.S. Katzenbeisser and F. A. P. Petitcolas, Information Techniques for Steganography and Digital Watermarking. Norwood, MA: Artec House, 2000

5.N. Khanna, A. K. Mikkilineni, A. F. Martone, G. N. Ali, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, "Asurvey of forensic characterization methods for physical devices," Digital Investigation, vol. 3, pp. 17–28,2006.

6.N. Khanna, A. K. Mikkilineni, G. T. C. Chiu, J. P. Allebach, and E. J. Delp, "Forensic classification of imaging sensor types," Proceedings of the SPIE International Conference on Security, Steganography, and Watermarking of Multimedia Contents IX, vol. 6505, no. 1. SPIE, 2007, p. 65050U.

7.Lin, Z., Wang, R., Tang, X., Shum, H.Y.: Detecting doctored images using camera response normality and consistency. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition, vol. 1, pp. 1087–1092 (2005)

8.Farid, H.: Creating and detecting doctored and virtual images: Implications to the child pornography prevention act. Technical Report TR2004-518, Department of Computer Science, Dartmouth College (2004)

9.Li, Y., Sun, J., Tang, C., Shum, H.: Lazy snapping. In: International Conference on Computer Graphics and Interactive Techniques, pp. 303–308. ACM, New York (2004)

10.Gloe, T., Kirchner, M., Winkler, A., B¨ohme, R.: Can we trust digital image forensicsfi In: Proceedings of the 15th international conference on Multimedia, pp. 78–86.ACM, New York (2007)