Scientific Journal Impact Factor (SJIF): 3.518

International Journal of Modern Trends in Engineering and Research

IJMTER

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

A SURVEY ON IMAGE FORENSICS BASED ON DIGITAL WATERMARKING

Rahulsingh G. Bisen[1] And Vinayak G. Kottawar[2]

[1,2]Department of CSE, M.G.M's C.O.E.,Nanded

Abstract— This paper presents a framework for digital image forensics which one of the category of Digital Forensics. There are two main parts in Digital Image Forensics, namely source identification and forgery detection. Digital watermarking used in image forensics has been extensively studied. This paper briefly provides introduction to digital image forensics, process of image forgery creation and various ways to detect image forgery. Then it describes why digital watermarking should be used in image forensics, what existing problems are and what the possible solutions are.

Keywords— Image forensic; digital watermarking; region selection; 2-D or 3-D transformation; compositing or matting

I. INTRODUCTION

Digital Forensics is the discipline that combines elements of law and computer science to collect and analyze data from computer systems and storage devices in a way that is admissible as evidence in a court of law. Multimedia Forensics has become study of various researchers from last few years. The multimedia supplied by websites mainly contains images, audio and video. In recent years image is considered as one of the favorite message carrier. In general, image can contain the most intensive information, which takes up to 98%. Digital images have been widely used in the network environment such as news report, intelligent information collection and so on. Image Forensics has become very important from last few years as in today's digital age, the creation and manipulation of digital images is made simple by digital processing tools with the emergency of high quality and high precision image processing equipments such as high pixel digital camera, high resolution printer, scanner, and copier, and the application of image editing software's such as Adobe Photoshop, Microsoft Paint and Paint Shop Pro, it becomes very easy to obtain and modify a digital image.that are easily and widely available. There are two main parts in digital image forensics:

1. **Source identification:**
   Source identification deals with identifying the source of images (such as cameras, mobile phones, camcorders, etc.)

2. **Forgery detection:**
   Forgery detection deals with discovering the evidence of tampering the images by accessing the authenticity of the digital media

II. PROCESS OF IMAGE FORGERY

As shown in the figure 1, the process of image forgery creation involves following steps:

- Selecting a image,
- Applying transformation,
- Composition of the image fragments and
- Retouching of the final image.

The process of image forgery creation begins with selecting a region or extracting a fragment or 3D object from the image. Then appropriate transformation technique (2Dor 3D) is applied on an image. This transformed image fragment is then fused into another image by using techniques such as matting or composting. Lastly, the image is retouched to remove the remaining artifact.

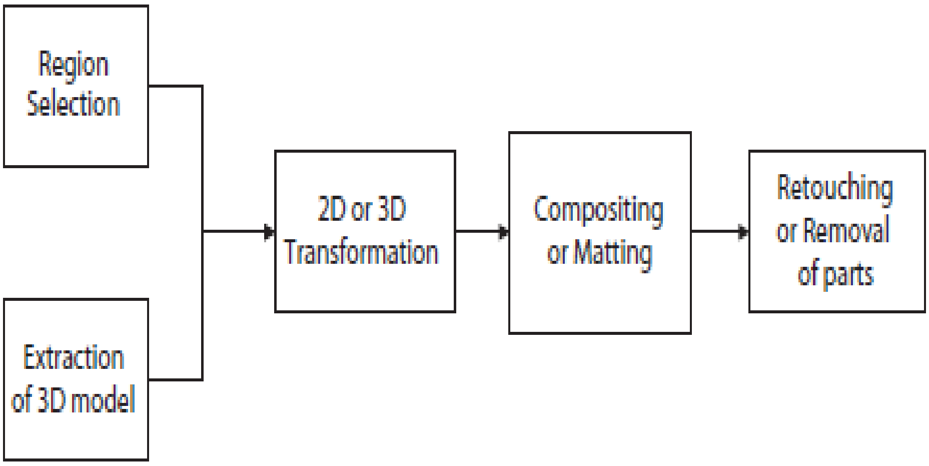

Figure 1. The process of image forgery creation

The following two figures (see Figure 2 and Figure 3) show Image forgery that can be created by forgers using the above technique:

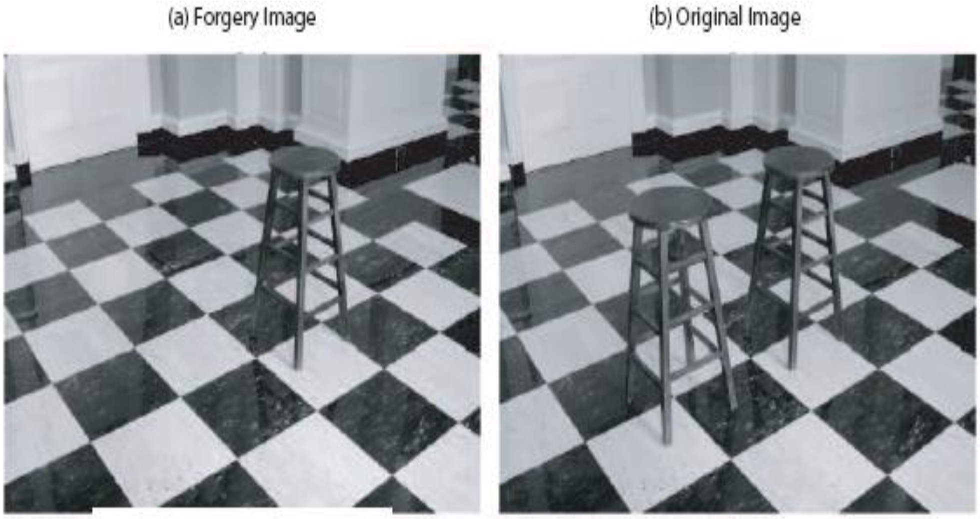

Figure 2. Example of image forgery

(a) Forgery image (b) original image

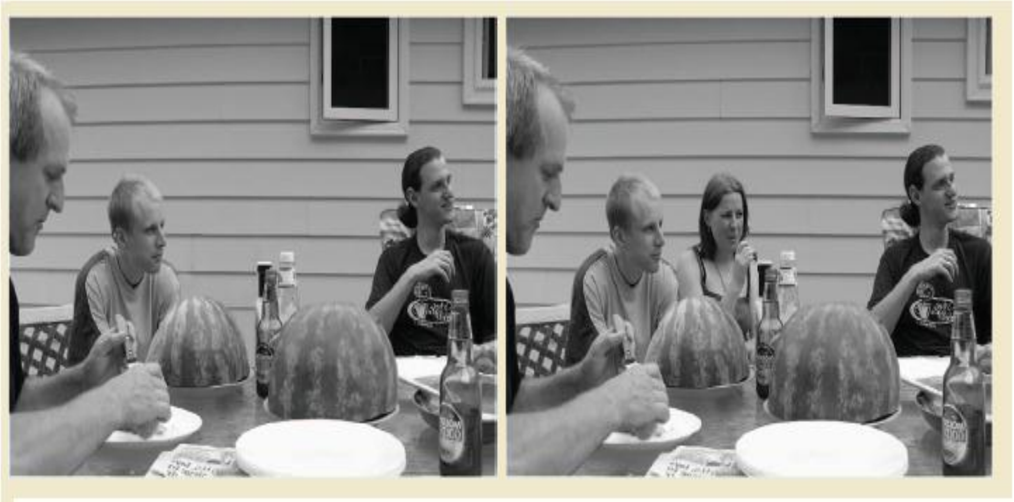

*Figure 3. Another e*xample of image forgery

III. METHODS OF IMAGE FORGERY DETECTION

There are various methods to detect forgery in images in digital image forensics. Some of these methods are as follows:

- Using JPEG Quantization Table.
- Using Chromatic Aberration
- Using Camera Response Function (CRF)
- Using Robust Matching

3.1 Using JPEG quantization table

Nowadays, generally all images use JPEG compression technique which is also known as lossy compression. Each compressed image has its own quantization table. Whenever an image is tampered and it is saved with different format other than its source format then quantization tables of source image and tampered image will be different. Instead of tampering complete image, if only some part of image is tampered and it is composted back to original image then also quantization table of source image and tampered image will be different. This difference can be exploited by comparing the quantization tables of an image and database of photo editing softwares for signs of tampering. The weakness of this method is that, when an image generated by digital camera is tampered or edited using editing software then there will exist double JPEG compression problem. This is because camera output image is JPEG compressed image and image edited with editing software is also compressed with JPEG format leading to double JPEG compression problem [3].

3.2 Using chromatic aberration

Chromatic aberration is a type of distortion in which there is a failure of a lens to focus all colors to the same convergence point. It occurs because lenses have a different refractive index for different wavelengths of light. It is the expansion or contraction of a colour channel with respect to one another resulting in a misalignment of the colour channels. Chromatic aberration is generally caused due to displacement of pixels in colour channel. The average angular error between displacements of pixels in colour channel is computed by using two parameters: local and global model parameters. If the average angular error exceeds a certain threshold, it is likely that aberration has been inconsistent across the image due to forgery. The weakness of this method is that, for image with little or no spatial frequency contents such as image with large and uniform part of sea, it very difficult to estimate chromatic aberration. [4]

3.3 Using camera response function (CRF)

Camera response function (CRF) is a form of camera signatures which can be extracted from a image and provides a basis for image forensics. This method suggests image splicing can be detected using geometry invariants and camera response function (CRF). In this method following steps are performed:

- Suspected splicing boundary is identified manually
- On the either side of this boundary geometry invariants from pixels are computed
- Geometry invariants are then used to estimate the CRF
- The CRFs from each region are then checked for consistency with each other
- The image is said to be authentic if the data from one region fits well to the CRF from another region and spliced otherwise.

The weakness of this method is that, its accuracy is high only for uncompressed images whereas for JPEG compressed images this method does not woks well. [5],[6].

3.4 Using robust matching

This method can be used to detect certain types of image forgery such as copy – move attack. In this forgery, a part of an image is cloned or duplicated elsewhere in the same image, usually to conceal some important features. In this method, matching is carried out between blocks of size AxA in a same image to detect exact replicas for uncompressed images. Whereas for JPEG compressed images, robust representation consisting of quantized DCT coefficients is used. The weakness of this method is that, it does not identify correct matching segments in flat, uniform areas such as the sky. [7].

IV. IMAGE FORENSIC AND DIGITAL WATERMARKING

Image forensics based on watermarking is an interdisciplinary of digital watermarking technology and image forensics. It involves image processing, information theory, digital communications, cryptography, multimedia technology etc. It can be also used to determine ownership of works, judge the authenticity of the image, and even point out the tampered area. Many researchers on the digital watermarking technology begin the research of image forensics technology. In recent years, the research on the application of digital watermark in the image forensics has been highlighted. The applications of digital watermarking in image forensics currently can be broadly divided into two categories:

- Embedding the watermarking in the process of JPEG compression [10],[11],[12].
- Embedding watermarking information after the photo saved as JPEG format [13],[14].

Image forensics can be done in two ways – one is active forensics and another is passive forensics. Digital watermarking technology is mainly used in active forensics to embed the authentication information previously into the original digital image; hence the authentication information can be used as the evidence of forensic analysis when the image has been invaded. Passive digital image forensics is a forensic analysis of digital image with the condition that the image has not been interfered with embedded watermark. As Digital images have been widely used in the network environment and high quality and high precision image processing equipments such as high pixel digital camera, high resolution printer, scanner, and copier, and the application of image editing softwares such as Adobe Photoshop, Microsoft Paint and Paint Shop Pro can easily modify a digital image, watermark can be embedded in a digital image in advance. Then by using active forensics photo source determination, classification, copyright protection and authenticity certification can be detected. But there are many problems to achieve the purpose of image forensics by adding the digital watermarking to images.

V. EXISTING PROBLEMS AND POSSIBLE SOLUTIONS IN IMAGE FORENSICS BASED ON WATERMARKING

There are three main problems in image forensics based on digital watermarking which are mentioned as following-

- Text images possess small watermark embedding capacity as compared to normal colour images. Hence it is difficult to guarantee the invisible watermark of the text image compared to that of commercial images
- The purpose of digital image forensics is divided into two categories - judging the source of the images and judging the authenticity of the images. To simultaneously achieve these two main purposes digital image forensics is difficult.

Majority of digital cameras in the market do not have technology to add watermarks to the digital image. Hence to embed the watermark information during the digital image forming process is the major issue to use digital watermarking in image forensics.

To overcome the above mentioned problems of using digital watermarking in image forensics following possible solutions can be studied:

1. **Adaptive algorithm for image forensics:**
   - Analyze the special features of the general colour images and special text image
   - Design algorithms to automatically identify image type after the statistics and analysis of the image features.
   - Then design different watermarking algorithms according the characteristics of colour images and text images, and automatically select the appropriate watermarking algorithm to embed watermarking information.
2. **The research on dual watermark embedding algorithm:**
   - Study robust digital watermarking and fragile digital watermarking algorithm respectively.
   - Explore appropriate classification criterion by analyzing the characteristics of different regions of image.
   - So the watermark embedded at different regions and different levels, the image authentication and ownership authenticity certification can be achieved at the same time.
3. **The establishment of prototype system:**
   - Construct a prototype system according to the algorithms for image forensics based on the DSP or FPGA development platform.
   - Test the main technical indicators, and analyze the test results

VI. CONCLUSION

Out of various fields of digital forensic, digital image forensic has become very vital field of research from last few years. The main function of image forensics is to assess the authenticity and the origin of images. The image forensics based on watermarking can be used to determine ownership of works, judge the authenticity of the image, and even point out the tampered area. There are various existing problems in this field that can be overcome by selecting any one of the possible solutions.

REFERENCES

[1] Zhou Guojuan, Lv Dianji, *"*An Overview of Digital Watermarking in Image Forensics*"* 2011 IEEE Fourth International Joint Conference on Computational Sciences and Optimization.

[2] Tran Van Lanh, Kai-Sen Chong, Sabu Emmanuel, Mohan S Kankanhalli, "A Survey on Digital Camera Image Forensic Methods".

[3] H. Farid, "Digital Image Ballistics from JPEG Quantization", Technical Report, TR2006-583, Dartmouth College, Computer Science

[4] M. K. Johnson and H. Farid, "Exposing Digital Forgeries Through Chromatic Aberration", In ACM Multimedia and Security Workshop, Geneva, Switzerland.

[5] Y.-F. Hsu and S.-F. Chang, "Detecting Image Splicing Using Geometry Invariants and Camera Characteristics Consistency", In ICME, Toronto, Canada, July 2006.

[6] Z. . Lin, R. Wang, X. Tang, and H.-Y. Shum, "Detecting doctored images using camera response normality and consistency," in CVPR, 2005, pp. 1087–1092

[7] J. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", Proc. of DFRWS 2003.

[8] T.-T. Ng, S.-F. Chang, C.-Y. Lin, and Q. Sun, "Passive-blind Image Forensics", In Multimedia Security Technologies for Digital Rights, W. Zeng, H. Yu, and C. –Y. Lin (eds.), Elsvier, 2006.

[9] Jessica Fridrich, "Digital Image Forensics", IEEE Signal Processing Magazine March 2009

[10] LIU Cai, DU Shi-pei. The Reality Authentication of Digital Photograph Based on Digital Watermarking, Journal Of Engineering Graphics,2005,26(4):73-75.

[11] C hi Kin Ho and Chang-Tsun Li, Semi-Fragile Watermarking Scheme for Authentication of JPEG Images.Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on .2004 , Volume: 1,Page(s): 7 – 11

[12] Zhishou Zhung, A Novel Lossy-To-Lossless Watermarking Scheme For Jpeg2000 Images. Image Processing, 2004. ICIP '04. 2004 International Conference on . 2004 , Volume: 1,Page(s): 573 -576

[13] L i Yaqin, Zhou Defu. Application of the Digital Watermark Technology in Watermarking Digital Camera. OFFICE AUTOMATION. 2009(5),156:40-43

[14] ZHENG Ji-wu WANG Ling LIU Hui. Digital Photograph's Authentication Technique Based on Digital Watermark, Computer Simulation. 2008,25(8):231-233,274