DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4541

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

STUDY OF IMAGE TAMPERING AND REVIEW OF TAMPERING DETECTION TECHNIQUES

C.Rajalakshmi
Research scholar Dept.of Computer science
M.S.University,India

Dr.M.Germanus Alex
Prof &Head Dept. of Computer science
Kamarajar Government Arts College Surandai
India.

Dr.R.Balasubramanian
Prof &Head Dept.of Computer Science & Engg.
M.S.University,India

Abstract: Nowadays photo manipulation made easier to play with the image files even by a layman. The Combining certain elements to create the unique image that can convince even the most experienced set of eyes. Time to time various detection techniques are developed to identify the image tampering operation over images. In this paper, first, various methods of tampering the image are discussed and the various detection techniques are surveyed. Finally, concluded the comparative study with some parameters.

Keywords: Digital forensics, Tamper detection, Copy move, SIFT

1. INTRODUCTION

The oxford dictionary defines the word image as the optical appearance of something produced in mirror or through a lens. Image may be formed by other types of radiant energy and devices. However, optical images are most common and are most important. A digital image is a numerical representation of a two dimensional image. Digital images are electronic snapshot taken of a scene or scanned from documents such as photographs, manuscript, printed texts, and artwork. Today's technology allows digital media to be altered and manipulated in ways that were simply impossible 20 years ago [1]. In spite of the various professional experts and software tools available worldwide, it is easier to manipulate an image without leaving any clue. With an amount of increase in image forgery and their consequences, it is very essential for the development of new image forgery detection techniques. For this purpose, a review of existing tampering detection techniques is essential for the development of new techniques as presented in this paper.

2. COMMON TAMPERING TOOLS

The process of creating fake image has been tremendous ally simple with the introduction of powerful graphics editing software such as adobe Photoshop, GIMP, Corel paint shop etc. Some of which are available for free. Photoshop is amazing tool for altering reality. Like any tool it can be used for the forces of both good and evil. GIMP is a cross platform image editor available for GNU/LINUX, OSX, windows and more operating systems. It is free software. Paint shop pro (PSP) is a raster and vector graphics editor for Microsoft window. Apart these some other tools like photos cape, creative cloud, Picasa, paint shop pro, pixir, Aperture, ACD see, serif, affinity, snap seed, and so on are available photo editing tools for manipulating an image.

3. TAMPERING METHODS

Photography lost its innocent many years ago. Only a few decades after Niepce created the first photograph in 1814, photographs were already being manipulative. Tampering can be innocent or evil. Innocent Tampering does not change the content of the image but change image's quality. Innocent tampering included various operations such as contrast brightness, adjustment, zooming, and rotation and so on. The evil tampering aims to modify the content of the image. The evil tampering includes.

Cloning (copy/paste)

a) Original image

b)Tampered image

Copy move forgery is created by copying and pasting content within the same image [2].

Image splicing

a) Original image

b)Tampered image

Image splicing is an image editing method to copy a part of an image and paste in to another image [3].

Image resembling

This operation can be used to shrink or enlarge the size of an image or part of an image. Image reduction, zooming and scaling methods are mentioned in [4].

Image forensics method

The author Henry farid in his book, [5] digital forensics, classify the forensics as camera based forensics, pixel based forensics, statistical based forensics, statistical based forensics, Geometric based forensics and physics based forensics

Digital image forensic

1.Format based forensics	2.Camera based forensics	3.Pixel based forensics	4.Statistical based forensics	5.Geometric based forensic	6. Physics based forensics
Fourier based JPEG Double JPEG JPEG Ghost	Color filter array Chromatic aberration Sensor noise	Resembling Cloning Thumbnails	PCA LDA	Calibration Reflection shadow	2D Lighting 2Dlight Environment 3DLight Environment

4. FORMAT BASED TECHNIQUES

The transformation of a forged image for the purpose of compression and other applications can make the forgery detection a very challenging task. JPEG compression to make forgery detection is very difficult. The JPEG standard does not enforce any specific quantization table or Huffman code. Camera and software engineers are therefore free to balance compression and quality to their own needs and tastes. The specific quantization tables and Huffman codes needed to decode a JPEG file are embedded into the JPEG header. The JPEG quantization table and Huffman codes along with other data extracted from the JPEG header have been found to form a distinct camera signature which can be used for authentication.

5. CAMERA BASED TECHNIQUES

Camera-based techniques focus on detecting the traces of tampering by exploiting the artifacts introduced by various stage of the imaging process. Chromatic aberration, color array, camera response, and sensor noise imperfections are all be used to estimate different camera artifacts. Under this class of techniques, the specifications of the camera capturing the image are used to identify tamper. These methods are mostly based on the analysis of sensor, color filter array interpolations, and lens aberrations. Most digital cameras capture color images using a single sensor in conjunction with an array of color filters. As a result, only one third of the samples in a color image are captured by the camera, the other two thirds are interpolated. This interpolation introduces specific correlations between the samples of a color image when creating a digital forgery these correlations may be destroyed or altered. In [5] describe the form of these correlations and propose a method that quantifies and detects them in any portion of an image when tampering with an image, the color aberrations are often disturbed and fail to be consistent across the image. In [5] describe how to exploit these aberrations for forensic analysis.

6. PIXEL-BASED TECHNIQUES

Pixel-based techniques are based on detecting the statistical anomalies introduced at the pixel level during the forgery process. These techniques also analyze pixel-level correlations that arise from a specific form of tampering either directly spatial domain or in some transformed domain. These techniques are the most common ones found in practice.

7. STATISTICAL BASED FORENSICS

Principal component analysis (PCA) [6] is the classic approach to reducing the complexity of analyzing high-dimensional data by projection into a lower-dimensional linear subspace. PCA projects data onto axes of maximal data variance. In so doing, the dimensionality of data is reduced while minimizing the loss of information or

distortion. Linear Discriminate Analysis (LDA) is the standard approach to multi-class classification. LDA projects data onto a linear subspace so that the within-class scatter (specifically, the within-class variance) is minimized and the across-class scatter is maximized.

8. GEOMETRIC-BASED TECHNIQUES

In authentic images, the principal point (the projection of the camera center onto the image plane) is near the center of the image. When a person or an object is moved or translated in the image (copy-move), or two or more images are combined together (splicing), it becomes difficult to keep the image principal point in its correct perspective. Thus, by applying projective geometry principles, robust forgery detection algorithms can be developed. The multitude of approaches discussed above show that the problem of forgery detection is a multidimensional one. Depending upon the particular forgery attack a given image is subjected to; some detection techniques can provide excellent results while others can be completely useless. Among these approaches, the most common and practical ones are the pixel based techniques. This class of techniques does not require any a priori knowledge about the type of transformation the image was subjected to, nor does it require information about the image acquisition process. One of the earliest surveys commonly cited in the literature is the paper published H. Farid, [1], which was later followed by a series of surveys, written by different researchers[7].

9. PHYSICS-BASED TECHNIQUES

Natural photographs are usually taken under different lighting conditions. Thus, when two or more images are spliced together to create the forged image, it is often difficult to match the lighting conditions from the individual photographs. Therefore, detecting lighting variations in an image can be used as evidence of tampering.

Based on image, the forgery methods are classified as

1. Detection of tampering performed in a single image (copy move).
2. Detection of tampering performed in a more than one image (image composition).
3. Independent tampering detection (single or composite or both).

Analyses of image tampering detection techniques

i) Copy move forgery

Table 1

Title of the paper	**Image operation**	**Tamper detection techniques**
Digital image tamper detection techniques- A comprehensive study [8]	Retouching, spelling ,copy-paste, cropping, cloning	Edge blurring
Digital image tampering- A threat to security[9]	Copy move, resize, image splicing, noising, blurring	Laplace filter, PCA, DCT,DWT,SVD
Digital image tamper detection tools[10]	Copy move, resize, image splicing, noising, blurring	Laplace filter, PCA, DCT, DWT, SVD
Tampering and copy move forgery detection using SIFT feature[11]	Copy move, block, feature based methods.	,PCA,DCT,DWT,SIFT

Table 2

Image splicing & copy move forgery detection[12]	Copy move splicing	Multiscale WLD,LBP,LLB,SVM
Efficient copy move forgery detection for detection for digital images[13]	Copy move, image splicing	Statistical & block characteristics
Survey of image forgery detection[14]	Copy move, splicing ,resize, cropping cloning	Pixel, format, camera physically, geometric based.
Comparison and analysis of photo image forgery detection techniques [15]	Copy move, copy **create**, copy paste	JPEG compression analysis, edge detection, localization
Image forgery detection A survey[16]	Copy move	JPEG compression, block based

Table 3

Detection false captioning using common sense reasoning[17]	Distorting, deletion, insertion, photo montage false captioning	AI(detection duplication). Segmentation classification(ROI)

Detecting image splicing using merged features in chromo space[18]	Image splicing local/global blurring compression and resize	DCT SRM,CASIA V2 dataset
Image forgery detection based on semantic[19]	Copy move	Framework semantic ontology commonsense knowledgebase
Copy move image forgery detection using mutual information[20]	Copy move	Region duplication

Table 4

Title of the paper	**Operation**	**Tamper detection techniques**
copy move image forgery detection method using steerable pyramid transform and texture descriptor[21]	Copy move	SPL,LBP
Copy move forgery detection based on patch match[22]	Copy move	Localization
Improving the detection and location of duplicated regions in copy move image forgery[23]	Copy move	SIFT MIFT localization

ii) Splicing detection techniques

Traces are left in the anatomy of an image when simple splicing operation is performed. Bincoherence features are used to note these traces and later successfully applied in [24] [25] [26] [27].

iii) Independent tampering detection techniques

Independent of image forgery is done in single or composites, all digital images are to be stored in any standard format such as JPEG one of the most interplead compression techniques. If an image is hybrid of two JPEG images trace of different compression could be exposed. In[28] expose these type of forgeries.

10. BEST APPROACH IN FORENSICS DETECTION TECHNIQUES

There are multiple techniques which can resolve these tampering issues to some extent depending on certain criteria. The methods discussed above are reliable to some extent but possess some limitations. These limitations are overcome by SIFT based detection technique.). Nowadays, local visual features(e.g SIFT,SURF, GLOH, etc.) have been widely used for image retrieval and object recognition, due to their robustness to several geometrical transformation (rotation, scaling), occlusions and clutter. More recently, attempts have been made to apply these kinds of features also in the digital forensics domain; in fact, SIFT features have been used for fingerprint detection shoeprint image retrieval, and also for copy move detection. It is a robust technique and is used in many areas. SIFT is also used in tampering detection of various transformations, (rotation, scaling, position etc).Expertimental results of various techniques shows that approaches used SIFT algorithm are the best and suitable for image forgery detection.

Splicing identification using SIFT algorithm

a) Original image

b) alter image

c) Extraction of feature points

d) Match points between image a & b

e) Display of original image

11. FUTURE SCOPE AND CONCLUSION

This paper mainly reviewed the different methods of image forensics. A wide range of tools and techniques are available to look in to digital images to verify the authenticity and integrity. Although the challenge still remain for techniques that are robustness of the existing techniques and confidence in the accuracy of the results achieved by these techniques. The available techniques are suitable for specific type of forgery only. There is no technique available to find out all type of tampering done in an image. Nowadays SIFT based forensics methods are proposed by many researchers. In my view in SIFT algorithm segment of the host image needs best approaches to enhance the accuracy of the forgery detection result. Future work will be mainly dedicated to investigating how to improve the clustering phase by means of an image segmentation process.

12. ACKNOWLEDGMENT

The authors would like thank the reviewer for their valuable comments.

REFERENCES

[1] Henry Farid " Image forgery detection survey " , IEEE SIGNAL PROCESSING MAGAZINE, March 2009.
[2] M.Ali Qureshi, M. Deriche "A review on copy move forgery detection techniques" IEEE 2014.
[3] Splicing.Available:http://www.ee.columbia.edu/in/ dvmm/trustfoto/projs/splicing/homepage-splicing.png
[4] A. Piva "An overview on image forensics" , ISRN Signal Processing 2013.
[5] Henry Farid " survey of Image forgery detection", Dartmouthu College.
[6] A.C. popescu and H. Farid, "Exposing digital forgery by detecting duplicated image regions", 2014
[7] T.VanLanh.K.S.Chong, S. Emmanuel,"survey on digital camera image forensic methods" ICME07,2007.
[8] Minati mishra, Flt. Lt. Dr. M C. Adhikary,"Digital Image tamper DetectionTechniques", 2013
[9] Deepika Sharmal, Pawanesh Abroal2 ," Digital Image Tampering", 2013
[10] N.Anantharaj "Tampering and Copy move forgery detection using shift Feature,2014
[11] Sahar Qasim Seleh," Tampering and Copy move Forgery Detection using shiftfeature"2012
[12] Somayeh Sadeghi, Hamid A. Jalab, and Sajjad Dadkhah," Efficient copy move forgery"2012
[13] Yongzhen ke, Weidong,"Imageforgery detection based on semantic" 2014
[14] G. Muhammad, Riyadh, "Copy move image forgery detection using streerable"2013
[15] Cozzolino, Napoli,"Copy move forgery detection based on patchmatch" 2014
[16] Sangwon lee, David A. Shamma, Bruce Gooch, "Image forgery detection A survay",2009
[17] D.G.Lowe, "Distinctive image features from scale invariant key points". Int. journal of computer vision vol 60 , no 2 pp.91-110,2004
[18] V. Christlen,C. Riess, J.Jordan,C.Riess, and E.Anegelopouou "An Evaluation of popular Copy Move Forgery detection approach" Dec, 2012
[19] R.Achanta , A. Shaji, K. Smith, A. Lucchi, P.Fua, and S. Susstrunk,"SLICsuperpixel compared to stateof the arts superpixelmethod", 2012
[20] I. Amerini, L. Ballan,R.Caldelli, A. Del Bimbo,AND g. Serra, "A State based forensic method for copy move attack detection and transformation recovery",2011
[21] P. Kakar and N. Sudha, "exposing postprocessed copy paste forgeries through transform-invariant feature" ieee vo no7, 2012
[22] Arun Anoop M "Review on image forgery detection"2015
[23] X. Pan am D S Lyu "Detection image region duplication using SIFT Feature" USA 2010
[24] V.Lu.A.L. Varma "Forensis hash for multimedia information" 2011
[25] H.J. Lin C.N Wang andY T Kao "Fast copy move forgery detection" 2009
[26] S.J Ryu MJ lee and H.K.Lee "Detection of copy rotate move forgery detection detection techniques" 2010
[27] Shi Y. Q chen C, Chen W, " A natural image model approach to splicing detection" ACM MMSEC07,2007.
[28] Farid H, "Exposing digital forgery from jpeg ghosts", IEEE Transaction on information forensics and security 2009.