International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Survey on Copy Move Image Forgery Detection Using Wavelet Transform

Akanksha Namdeo[1], Anish Vishwakarma[2]

[1]Rungta College of Engineering and Technology, Department of Electronics Engineering, Kohka-Kurud Road, Bhilai 490024, India

[2]Rungta College of Engineering and Technology, Department of Electronics and Engineering, Kohka-Kurud Road, Bhilai 490024, India

Abstract: ***Editing of images are very common these days. The process of creating fake images has been very simple with the introduction of powerful computer graphics. Such tempering with digital images is known as image forgery. With the advancement of the digital image processing software and editing tools, a digital image can be easily forged. The detection of image forgery is very important because an image can be used as legal evidence, in investigations, and in many other areas. The pixel-based image forgery detection aims to verify the authenticity of digital images without any prior knowledge of the original image. There are many different ways for tampering an image such as splicing or copy-move, resampling an image that are resize, rotate, stretch, addition and removal of any object from the image. In this we have discussed various pixel-based techniques for image forgery detection.***

Keywords: Forgery Detection, Dydic Wavelet Transform,Discrete Wavelet Transform,SVD,Image Forencics..

1. Introduction

Digital Image forgery is the process of altering or manipulating a digital image with an intention to mislead others by representing the changes as true copies of the original. The advancement in technology introduces us many digital image editing softwares such as Photoshop, Gimp Fireworks etc. which helps in editing the images without making any visible traces of forgery. So the maintenance of integrity and authenticity of digital images is a major problem. The main goal of this paper is:

- to introduce various ways of image forgery detection;
- to review some existing techniques in pixel-based image forgery detection;
- to provide a comparative study of existing algorithms with their merits and demerits.

Digital image forgery detection techniques are classified into active and passive approaches. In the active approach, the digital image requires preprocessing of image such as watermark embedding or signature generation, it limits their application in practice, Unlike the watermark and signature-based methods, the passive techniques are not need any digital signature to be generated or to embed any watermark. Passive image forgery detection techniques roughly can be divided into five categories:

1.Pixel-based image forgery detection: Pixel-based techniques detect statistical anomalies introduced at the pixel level Pixel-based techniques emphasize on the pixels of the digital image. This is one of the most common forgery detection techniques. These techniques are categorized into four types.

a) Copy move
b) Resampling
c) Splicing
d) statistical

2. Format-based image forgery detection: format-based techniques leverage the statistical correlations introduced by a specific lossy compression scheme. Format based techniques are another type of image forgery detection techniques. These are based on image formats mainly in the JPEG format. These can be divided into three types. If the image is compressed then it is very difficult to detect forgery but these techniques can detect forgery in the compressed image.

a) Jpeg Quantization
b) Double Quantization
c) Jpeg Blocking

3. Camera-based image forgery detection: camera- based techniques exploit artifacts introduced by the camera lens, sensor, or on-chip post-processing. Whenever we capture an image from a digital camera, the image moves from the sensor to the memory of camera and it undergoes a series of processing steps, quantization, colour correlation, white balancing, filtering, and JPEG compression. These processing steps starts with capturing to end with saving the image in the memory may vary on the basis of camera model and artifacts of camera. These techniques work on this principle. These techniques can be divided into four categories.

a) Chromatic aberration
b) Color filter array
c) Camera response
d) Sensor noise

4. Physical environment-based image forgery detection: physical environment-based techniques explicitly model and detect anomalies in the 3-D interaction between physical objects, light, and the camera. Consider the creation of a forgery showing two movie stars, rumored to be romantic seans, walking down a sunset beach. Such an image might be created by splicing together individual images of each movie star. In doing so, it is often difficult to exactly match the lighting effects under which each person was originally photographed. Differences in background lighting across an image can then be used as evidence of tampering. These algorithms work on the basis of the lighting environment under which an object or image is captured. Background

lighting is very important for capturing an image. These techniques are divided into three categories.
a) Light detection 2-D
b) Light detection 3-D
c) Light Environment

5. Geometry-based image forgery detection: Geometry-based techniques make measurements of objects in the world and their positions relative to the camera. Grooves made in gun barrels impart a spin. These grooves introduce somewhat distinct markings to the bullet fired, and can therefore be used to relate a bullet with a specific handgun. As the same spirit, several image forensic techniques have been developed that specifically model artifacts introduced by various stages of the imaging process. Geometry-based techniques made measurement of objects in the world and their position relative to the camera. Geometry-based image forgery techniques are divided into two categories.
a) Principal Point
b) Metric Measurement

2. Comparison Table

There are so many different techniques have been proposed for the implementation of Detection of Forgery on Images to give better performance than previous work. Some previous works are shown below.

S.NO.	*Paper Title*	*Method Used*	*Tempering Detection Type*	*Advantages /Disadvantages*
1	Copy-move forgery detection using dyadic wavelet transform	Dy wt	This method is based on image segmentation and similarity detection	Effectively detected tampering on the image where the background is simple.
2	Copy-Move Image Forgery Detection Using Local Binary Pattern and Neighborhood Clustering	LBP and neighborhood clustering	This paper proposed copy-move image forgery detection method is evaluated using types of original and Forged images.	The performance of the methods degrades when the pasted parts rotation and scaling both.
3	Passive copy move image forgery detection using undecimated dyadic Wavelet transform	Dy WT	Comparison based on Q factor of images.	It utilizes both the LL1 and HH1 subbands to find similarities and dissimilarities between the blocks of the images for robust detection of copy move.
4	Rake transform and edge statistics for image forgery detection	Rake transform and edge statistical	They proposes a novel scheme to image forgery detection to automatically differentiate forged Images from authentic images by using only images.	The proposed method is not give a reliable result because of the insufficient generalization properties.
5	Multi-Scale Local Texture Descriptor for Image Forgery Detection	A Multi-scale local texture Descriptor	SVM with a radial basis function kernel is employed to Detect image forgery detection,	The proposed method Achieved 92.28% accuracy and also Showed toughness against Q factor of JPEG compression.
6	Copy-move forgery detection using multiresolution local binary patterns	Multiresolution local binary patterns	The proposed method is robust to geometric distortions and illumination variations of duplicated regions	Experimental results demonstrated that the proposed approach could even detect duplicated regions with common postprocessing operations including: scaling, JPEG compression, gaussian blurring and AWGN.
7	Identifying Tampered Regions Using Singular Value Decomposition in Digital Image Forensics	SVD	Method is used on Gaussian white noise contamination, lossy JPEG compression.	The experimental results show that the proposed method gives reliableness and robustness against retouching details
8	Copy-move image forgery detection based on sift descriptors and svd-matching	sift descriptors and svd matching	Detection on difficult when the images are undergone some geometric deformations such as rotation, translation, scaling	The combination of both feature-based and block-based different techniques can help and improve the expected results.
9	RGB Digital Image Forgery Detection Using Singular Value Decomposition and One Dimensional Cellular Automata	SVD+ Cellular Automata	It generates the Robust Secret Key for the image authentication	One-Dimensional Cellular Automata to generate the Robust secret key that can be used to protect the Image against the forgery.
10	An Evaluation of Popular Copy-Move Forgery Detection Approaches	Evaluation on DWT	The goal of the paper is to examine which CMFD method to use under different image attributes.	In this paper evaluated the performance of different widely-used features for copy-move forgery detection
11	Splicing Image Forgery Detection Based on DCT and Local Binary Pattern	DCT and Local Binary Pattern	CASIA tampered image detection evaluation database version 1.0 is used.	The experimental results show that the proposed features of the chromatic channel are outforming that of other color channel.
12	Digital image forgery detection and estimation by exploring basic image Manipulations	Resampling and contrast enhancement	In this paper, the method for detecting image alterations Such as re-sampling, contrast enhancement and histogram Equalization has been proposed	The resampling Detection algorithms fail when JPEG compression is performed

13	An efficient expanding block algorithm for image copy-move forgery detection	Expanding Block Algorithm	Forgery Detection has been performed well.	It has been shown that the expanding block algorithm is an effective method for identifying image copy-move forgery.
14	Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis	DCT Coefficient	In this paper propose detecting tampered images by examining the double quantization effect hidden among the discrete cosine trans-form (DCT) coefficients.	In this paper proposed method produces encouraging results, more effort is still needed to improve the accuracy of their approach.

3. Comparison

We have discussed various methods used for image forgery detection proposed by various authors. The aim of all the methods is to detect the forgery in the image but the techniques are different. Table shows the comparison table of the various methods discussed in this paper.

4. Conclusion

In this paper various approaches of pixel-based image forgery detection have been reviewed and discussed. All the above methods and approaches discussed are able to detect forgery. But some techniques are not effective in terms of detecting actual forged region. On the other way some algorithms have a very high time complexity. So, there is a need to develop an efficient and accurate image forgery detection algorithm.

References

[1] J. A. Redi, w. Taktak, and j.-l. Dugelay, "digital image forensics: a booklet for beginners," multimedia tool appl., vol. 51: 133_162, 2011.
[2] Mohd dilshad ansari, s. P. Ghrera1 and vipin tyagi, "pixel-based image forgery detection: a review", IETE journal of education 2014.
[3] Najah Muhammad.; Muhammad Hussain.; Ghulam Muhamma.; George Bebis."Copy-Move Forgery Detection Using Dyadic Wavelet Transform" IEEE conference on imaging and visualization, 2011 Publication year: 2011.
[4] Motasem alsawadi.; Ghulam Muhammad.; Muhammad Hussain.;George Bebis. "Copy-Move Image Forgery Detection Using Local Binary Pattern And Neighborhood Clustering", 2013 IEEE European Modelling Symposium, 2013 Publication Year: 2013.
[5] Ghulam muhammada.; Muhammad Hussain.; George Bebis, "Passive Copy Move Image Forgery Detection Using Undecimated Dyadic Wavelet Transform",Elsevier Digital Investigation 2012 Publication Year: 2012.
[6] Patchara Sutthiwan Yun Q.; Shi1 Wei Su Tian-Tsong Ng, "Rake Transform And Edge Statistics For Image Forgery Detection" IEEE Publication Year: 2010.
[7] Ghulam Muhammad, "Multi-Scale Local Texture Descriptor For Image Forgery Detection" IEEE Publication Year: 2013.
[8] Reza Davarzani.; Khashayar Yaghmaie.; Saeed Mozaffari.; Mey Sam Tapak, "Copy-Move Forgery Detection Using Multiresolution Local Binary Patterns" Forensic Science International, 2013 Publication Year: April 2013 Page(s): 61–72.
[9] Xiaobing Kang.; Shengmin Wei, "Identifying Tampered Regions Using Singular Value
[10] Decomposition In Digital Image Forensics" IEEE International Conference on Computer Science and Software Engineering, 2008 Publication Year: 2008.
[11] Takwa Chihaoui.; Sami Bourouis.; Kamel Hamrouni, "Copy-Move Image Forgery Detection Based On Sift Descriptors And Svd-Matching", IEEE 1st International Conference on Advanced Technologies for Signal and Image Processing on march,2014 Publication Year: 2014 Page(s): 17-19.
[12] Dr. Mohammad V. Malakooti.; Ahmad Pahlavan Tafti.; Faezeh Rohani.;Mohammad Amin Moghaddasifar, "RGB Digital Image Forgery Detection Using Singular Value Decomposition And One Dimensional Cellular Automata".
[13] Vincent Christlein.; Christian Riess.; Johannes Jordan.; Corinna Riess.; Elli Angelopoulou, "An Evaluation Of Popular Copy-Move Forgery Detection Approaches" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 6, December,2012 Publication Year: 2012.
[14] Amani A. Alahmadi.; Muhammad Hussain.; Hatim Aboalsamhl.; Ghulam Muhammadl, George Bebis, "Splicing Image Forgery Detection Based On Dct And Local Binary Pattern" Publication Year: 2013.
[15] S. Devi Mahalakshmi .; K. Vijayalakshmi .; S. Priyadharsini, "Digital Image Forgery Detection And Estimation By Exploring Basic Image Manipulations" Elsevier Digital Investigation ,2012 Publication Year: 2011 Page(S): 215–225.
[16] Gavin Lynch.; Frank Y.Shih.; Hong-Yuan Mark Liao,"An Efficient Expanding Block Algorithm For Image Copy-Move Forgery Detection" Elsevier Information Sciences,2013 Publication Year: 2013 Page(S): 253–265.
[17] Zhouchen Lin, Junfenghe.; Xiaooutang.; Chi-Keungtang, "Fast, Automatic And Fine-Grained Tampered Jpeg Image Detection Via Dct Coefficient Analysis" Elsevier Pattern Recognition,2009 Publication Year: 2009 Page(S): 2492 – 2501.