National conference on Technology innovation in Mechatronics,Energy Management and Intelligent communication(NCTIMEMIC-2017)

International Journal of Advanced Scientific Technologies , Engineering and Management Sciences (IJASTEMS-ISSN: 2454-356X) Volume.3,Special Issue.1,April.2017

A Survey on Various Detection Methods for Copy Move Digital Image Forgery

Abhila G. K.
MTech Student, Dept of CSE
Lourdes MathaCollege of Science and Technology
Trivandrum,India
gkabhila@gmail.com

Chithra A. S.
Associate Professor, Dept of CSE
Lourdes MathaCollege of Science and Technology
Trivandrum,India
chithra.as@gmail.com

Abstract—Image forgery means manipulation of the digital image.This Manipulated image is used to conceal some meaningful or useful information of the image.There are several kind of digital image forgeries .These types of forgeries can't be identified by naked eyes. One of them is copy move digital image forgery. Copy move forgery(CMF) means copy a couple of regions from the image and paste it somewhere else in the same image.CMF may be performed to cover the truth of the image. so it is essential to identify this type of image tampering. There are lots of CMF detection(CMFD) Schemes to find out these types of forgeries. Commonly there are two classes of CMFD algorithms. one is based on block-wise division and other is based on keypoint extraction. Other detection schemes also exits(for example SURF,SIFT,RANSAC ETC). This paper deals with various methods used for detecting copy move image forgery.

Keywords—Keypoints,Patches,Blocks,Segments.

I. INTRODUCTION

Digital image forensics[1] mainly deals with the problem of certifying the authenticity of an image or its origin. Now a days we come across lots of tampered images in news papers,business,law,military affairs,academic results etc.So it is essential to deal with such tampered images.Here is the importance of digital image forensics to deal with authenticity of the images. The kind of tampering operations(such as copy -move,mosaiking etc)applied to the image is detected by image forensics techniques.The tampering operations generate no visual artifacts in the image.One of the existing types of image tampering is copy-move forgery. The main objective of copy move forgery is to replicate a part of an image which is used to hide an object or to enlarge certain areas, by copy-pasting a set of pixels from an area to another area of the same Image. There are three main branches of digital image forensics.1)Image source identification: This branch deals with which device was used to capture an image from that the authenticity of the image can verified.2)Discrimination of computer generated image: This branch deals with whether an image is natural or synthetic.3)Image forgery detection: This branch deals with if an image has been intentionally modified by human or not.

II.LITERATURE REVIEW

Davide Cozzolino, Giovanni Poggi, Luisa Verdoliva[2]proposed patchmatch based copy move image forgery detection scheme. In this work authors propose a new algorithm for detecting copy move forgery in images.It is based on fast computation of a dense nearest-neighbor field.Here use Patchmatch for identify identical regions in the image.All such algorithms are based on three steps they are1) featuring*:* suitable features are associated with all pixels or with a limited set of keypoints in the image; 2)matching*:* for each pixel of interest, the best matching pixel is located based on the associated features of the image; 3)post-processing*:* the displacement field is filtered and processed to detect actual copy-moved regions.The techniques proposed in the literature can be grouped in two large classes.One class is depending on whether the matching is performed for each pixel and other class is based for some selected keypoints. This preliminary choice impacts heavily on complexity for matching based method.For avoiding this types of complexity authors proposed a new fast and reliable technique for copy-move detection based on the Patchmatch.Patchmatch based scheme is a fast randomized algorithm and also they are iterative in nature.This algorithm finds dense approximate nearest neighbor matches between image patches. Patchmatch is to compute the approximate nearest neighbor field (NNF) of an image.This helps to reduce computational complexities of this algorithm.This PatchMatch looks as the perfect tool to carry out copy-move detection in the forged images . Authors modify the basic algorithm to gain robustness against rotation.This algorithm also has the ability to identify the copy move forgeries under rescaling and resizing operations.For handling rescaling and rotation generalized patchmatch algorithms use nearest neighbors in a four-dimensional space (x, y, θ, s),with θ the rotation angle and s the scale factor. This leads to some complexity, but the resulting algorithm can be still considered relatively fast and accurate.The limitations of this algorithm is to replace SATS, relatively slow with regular fields, with faster techniques.

Swapan Debbarma ,Angom Buboo Singh ,Kh.Manglem Singh [3]proposed Keypoints Based Copy-Move Forgery Detection of Digital Images. In this paper authors use two algorithms namely SIFT and SURF.These algorithms are used for feature extraction and forgery detection in images.Speed and accuracy are two terms which can be used to compare the performance of these two algorithms**.** This SIFT algorithm consists of the following four steps: 1) scale-space extrema detection for the image2) keypoint localization; 3) assignment of one canonical orientations; 4) generation of keypoint descriptors. Initially given an input image.From this input image SIFT features are detected at different scales using a scale-space representation implemented as an image pyramid.By using Gaussian smoothing and subsampling of the image resolution the image pyramid levels are obtained. The local extrema (minimum/maximum) in the scale-space are used to detect the keypoints of the image.After selecting these keypoints are extracted by applying a computable approximation of the Laplacian of Gaussian called Difference of Gaussians (DoG). The SURF algorithm is based on integral image and Hessian matrix approximation.An intermediate image representation known as the “Integral Image”which affect the performance of SURF algorithm. An integral image $I\Sigma(\mathbf{x})$ at a location is $\mathbf{x}=(x, y)$ which represents in the origin and x location the sum of all pixels in the input image formed a rectangular regions**.** Three additions take place to calculate the sum of the intensities in upright of rectangular region of the image after the integral image has been computed. Hence, the calculation time is dependent of the image size.SIFT is more accurate for detection of larger keypoints matches compare to SURF.SIFT uses feature vector(128)this makes it run slower than SURF which has only the feature vector dimension(64).The integral image used in SURF reduces the time complexities.SURF and SHIFT methods are good to detect image forgeries in the presence of JPEG compression,Gaussian noise addition etc.The limitations of these algorithms is to fail to detect forgeries in smooth or plain areas of the image.

S. A. Fattah1, M. M. I. Ullah, M. Ahmed, I. Ahmmed, and C. Shahnaz[4]proposed Copy-Move Forgery Detection in Digital Images Based on 2D-DWT(Discrete Wavelet Transform).For detecting copy-move image forgery discrete wavelet transform (DWT) perform two stages of operations.In the first stage 2D-DWT is performed on the forged image and only approximate DWT coefficients are considered. The DWT image is divided into different small blocks.These blocks are of two categories namely overlapping and non-overlapping blocks.A candidate block selection scheme is proposed for reducing the computational burden.This is for non-overlapping blocksIn the second stage, all overlapping blocks are compared with the primarily selected candidate blocks. This paper proposed 2D-DWT based block matching algorithm for copy-move forgery detection. In this method used all three layers of color image are utilized and LL band DWT transformed image is divided into overlapping blocks . Square blocks are used for convenience. To obtain overlapping blocks one pixel shifting method is used. Investigated the effect of changing block size and area of overlaps is in detail it is observed that too large number of pixels which is beneficial in terms of statistical similarity measure for copy move forged images. It may result in misleading information in case of small sized forged images.The computational burden will increased by too small block sizes. Hence a moderate block size is preferred by this method. In order to avoid chances of missing similar regions considering overlapping only by one pixel is preferred.Block-matching procedure is used to extract features from each block and then to find the duplicated blocks based on the similarity in their features.The advantage of this method is that candidate block selection algorithm helps in avoiding the huge computational burden involved in block matching operation. The candidate blocks are matched with all overlapping blocks.As a result high level of detection accuracy is achieved both in case of single and multiple copy-move image forgeries.The limitations of this method is that the proposed scheme produce only satisfactory performance in terms of hit rate, miss rate, and false detection rate.

Mohsen Zandi, Ahmad Mahmoudi-Aznaveh,Azadeh Mansouri[5]proposed a method to overcome the disadvange of show false matches in case of large number of copied regions present in forged images.The authors propose a new approach to overcome this challenging issue. False positive reduction is the result of this method.In this method adaptive thresholding is applied to the matching stages. The duplicated region may be exposed to some distortions due to the result of compression, blurring, rotation, interpolation and so on. The lower similarity will be result due to larger extent of the imposed distortions.The block content may also be effective in degradation amount depending on the level and type of distortion.In this method for achieving more false positive results , high threshold is used for matching regions.If use a low threshold may lead to missing some copied regions.That's why the authors proposed to employ an adaptive threshold to enhance the achieved results.In this method for analyzing the similarity between two copied blocks some factors should be taken into account they are as follows:The block content, Selected features,degradation type and its degree and finally similarity criteria, these are the factors taken into account. In this paper use an adaptive similarity threshold scheme for Copy-move forgery detection(CMFD) algorithm. This method can be used for most of the block-based copy-move forgery detection.The authors proposed that the matching threshold can be adjusted proportional to the standard deviation of the pair block’s intensity for detecting copy move forgeries in digital images.In this algorithm relationship is considered almost linear. The advantage of this algorithm is that the effect of employing adaptive threshold which leads to higher performance in matching step.The limitations of this work is that it is not appropriate to employ forensics techniques performing based on statistical inconsistencies.

AndreaCostanzo,IreneAmerini,RobertoCaldelli[6]proposed the method for detecting copy move forgery based on SIFT keypoint removal and injection.This paper mainly deals with attacks capable of removing SIFT keypoints from images. To trace with these attacks authors proposed three novel forensic detectors,which is used for the identification of forged images. The SIFT keypoints of the images are removed globally or locally . The proposed detectors look for inconsistencies.They mainly deals with inconsistencies like the absence or anomalous distribution of keypoints within the forged image. In this paper the authors first validate the methods on keypoint removal techniques.Then the authors further assess their reliability by devising a counter-forensic attack.This is done by injecting fake SIFT keypoints in the attempt to cover the removal of keypoints from the forged image. The working principles of the SIFT keypoint removal method is called Classification-Based Attack (CLBA).Depending on the grayscale histogram of the neighborhood surrounding keypoints in the pixel domain they are classified on three classes. They are unimodal, bimodal and multimodal classes. Depending on the class, each keypoint is removed by manipulating a small square region in the forged image.The CLBA’s effectiveness is evaluated in terms of keypoint removal rate (KRR).The perceptibility is evaluated in terms of average Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity (SSIM) index between the manipulated and the original neighbourhoods.The advantages of these detectors are effective not only against keypoint removal but also against the injection of fake keypoints.The limitations of this work is that investigating the possibility of recognizing the injection forgery by studying potential anomalies. These studies on the properties of the fake keypoints with respect to the original ones.

Seung-Jin Ryu, Matthias Kirchner, Min-Jeong Lee, and Heung-Kyu Lee[7]proposed a method to detect copy move forgeries by rotation invariant localization of duplicated image regions based on zernike moments.Zernike moments are known for their superior insensitivity to image noise..Zernike moments a perfect building block for detecting copy—rotate—move (CRM) manipulations.This is due to analytical invariance to rotation and robustness to noise of zernike moments. In this paper authors extract Zernike moments from overlapping blocks of a questioned image.Then use their magnitudes as feature representation.The detector employs locality sensitive hashing for block matching.Then removes falsely matched block pairs.It is done by inspecting phase differences of corresponding Zernike moments. In this paper the authors use pixel detection accuracy and pixel false positive rate for a quantitative evaluation of localization performance.This is done at pixel-level. Two factors that affect the performance of detectors.They are the size of the duplicated region and the size of the image under investigation.The small duplicated regions are typically hard to distinguish from incorrectly matched blocks in forged images.The limitations of this work is that detectors which are based on Zernike moments are not capable of localizing duplicated regions,which is underwent strong affine transformations other than rotation and scaling.

III.CONCLUSION

This paper summarizes various detection techniques in the copy move forged images.Done a systematic study on the reliability and accuracy for all the available copy move forgery detection techniques. Some of the copy move forgery detection techniques mainly focus on forged images without any transformations and some concentrate on copy move forgery detection with transformations such as rotation, scaling etc. The limitations of all the copy move forgery detection techniques are discussed as well.

REFERENCES

[1] Jian Li, Xiaolong Li, Bin Yang, and Xingming Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme", IEEE transactions on information forensics and security,issue no.3,page no 507-518,March 2015.

[2] Davide Cozzolino, Giovanni Poggi, Luisa Verdoliva,"Copy-Move Forgery Detection Based on Patchmatch", IEEE international conference on image processing,2014,page no. 5312-5316.

[3] Swapan Debbarma ,Angom Buboo Singh ,Kh.Manglem Singh, "Keypoints Based Copy-Move Forgery Detection of Digital Images", IEEE international conference on informatics,Electronic and vision ,2014,page no.1-5.

[4] S. A. Fattah, M. M. I. Ullah, M. Ahmed, I. Ahmmed, and C. Shahnaz Department of EEE, BUET, Dhaka, Bangladesh2Prime Silicon Technology Inc., Santa Clara, CA,"A Scheme for Copy-Move Forgery Detection in Digital Images Based on 2D-DWT",IEEE international conference on circuits and systems ,2014, Page no 801-804.

[5] Mohsen Zandi, Ahmad Mahmoudi-Aznaveh Faculty of electrical and computer engineering Shahid Beheshti University Tehran, Azadeh Mansouri Faculty of electrical and computer engineering Kharazmi University Tehran, Iran, "Adaptive Matching for Copy-Move Forgery Detection", *IEEE* international workshop on information forensic and security ,2014,page no.119-124.

[6] Andrea Costanzo, Irene Amerini, Roberto Caldelli,and Mauro Barni,"Forensic Analysis of SIFT Keypoint Removal and Injection", *IEEE* transactions on information forensics and security, issue no.9,page no. 1450-1456, September 2014.

[7] Seung-Jin Ryu, Matthias Kirchner, Min-Jeong Lee and Heung-Kyu Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments", IEEE transactions on information forensics and security,issue no.8, page no.1355-1368,August 2013 .