International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-6 Issue-4, April 2017

A Review on Block-Key Point Based Copy Move Forgery Detection

Monisha Mohan, Preetha V.H

***Abstract*: Copy move forgery is a region duplication forgery in which a part of a digital image is copied and pasted within the same image. Many algorithms have been developed for detecting the copy move forgery. Copy move forgery is mainly classified into two types which is block based and keypoint based. The block based method includes PCA, DCT, DWT etc and key point based method includes SIFT and SURF. This paper will include a detail study of different image forgery detection techniques, different tampering techniques and a detailed study of different block based and keypoint based method.**

***Index Terms*: Copy move forgery, DCT, DWT, SIFT, SURF**

I. INTRODUCTION

The availability of affordable and powerful image processing and editing software such as photoshop, make image manipulation relatively easy. Today digital world has changed the format of accessing, manipulating and sharing information however the developments have also given rise to different security problems. With the development of digital cameras and computers as well as software for image editing, the problem of digital image forgery is very serious. Hence inorder to avoid this manipulation in image, image tampering detection is very necessary.

Fig:1- Example of Copy Move Forgery

II. CLASSIFICATION OF IMAGE FORGERY

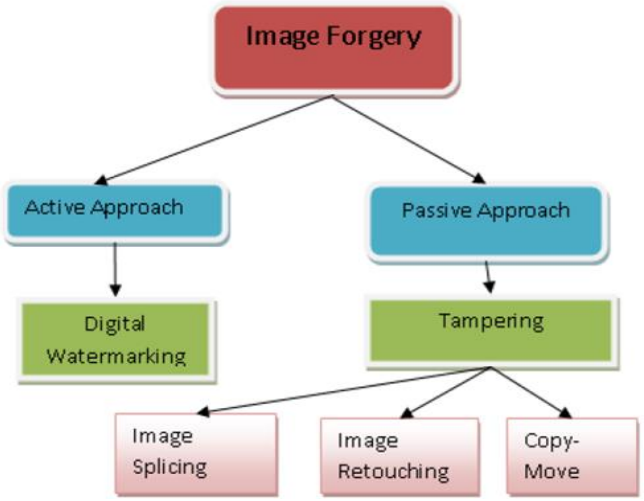

Fig:-2 Classification of Image forgery

To detect if the digital image is authentic or not, it is very important to check the forgery of image. Image forgery is not new technique. According to the previous history it was developed as early as 1840's.Hippolyta Bayard was the first person to create a fake image as recorded by history which is famous for a picture of committing suicide.

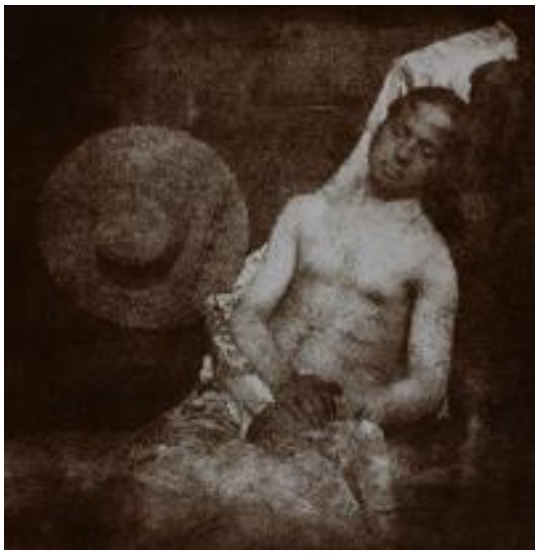

Fig:-3 Self Portrait as A Drowned Man, Direct Positive Print

Digital image forgery does not differ very much in nature compared to conventional image forgery[1].

Manuscript published on 30 April 2017.
***** Correspondence Author (s)
Monisha Mohan, M.Tech Student, Department of Electronics and Communication Engineering, Sree Chitra Thirunal College of Engineering, Trivandrum (Kerala), India, E-mail: monishamohan3633@gmail.com
Preetha V. H, Assistant Professor, Department of Electronics and Communication Engineering, Sree Chitra Thirunal college of Engineering, Trivandrum (Kerala), India, E-mail: vhpreetha@yahoo.com

Instead of using photographs, digital image forgery deals with digital image. The process of creating fake image has been tremendously simple with the introduction of powerful computer graphics editing software such as adobe photoshop, GIMP and corel paint shop.

Digital image forensics has two principle approaches to detect the forgery which is shown in figure 2. First one is active approach which include digital watermarking and signature technique. These are implemented at the time of image acquisition. The authenticity of digital image such as digital signature in the image or encryption of digital image in active approach require special hardware implementation. In the case of digital watermarking it is defined as the process of hiding digital information in the carrier signal that is hidden information should but doesnot need to contain a relation to the carrier signal. Digital watermark may be used to check the authenticity or integrity of the carrier signal to show the identity of its owner.

Second one is passive approach which doesnot require any prior information about the image and only depends on the trace left on the image by different processing steps during image manipulation.

Mainly two methods are used in passive approach. One of which is image source identification which identify the device used for the acquisition of digital image. It will identify whether the image is computer generated or using digital camera. By using this method, the location of forgery in image cannot be determined.

The second method of passive approach is Image Tampering. Normally Image tampering was originated by the earliest of 21st century. At that time, it was used for political propaganda[2]. Image tampering is otherwise known as image manipulation. Image tampering is defined as "adding or removing important features from an image without leaving any obvious trace of tampering". Normally image tampering technique is classified into three types, which are image splicing, image retouching, and copy move.

Image splicing is the oldest technique in which mixtures of two or more images are combined to form a fake image or manipulated image. In image retouching certain facial characteristics of image being enlarged or reduced inorder to make image more attractive. In image cloning or copy move, a part of image or a portion of image is copied and pasted within the same image.

III. COPY MOVE FORGERY

Copy move forgery is a specific type of image tampering where a part of the image is copied and pasted on another part generally to conceal unwanted portion of image. Hence the main aim of this detection of copy move forgeries is to detect the image areas that are the same or extremely similar.

In recent years the detection of copy move forgery has become one of the most actively researched topic in blind image forensics [3]. Copy move forgery technique is widely in the area which poses serious problem of the extent of trust that can be placed in the authenticity of digital content, especially when presented as evidence in court room, for claiming insurance and in the scientific world.

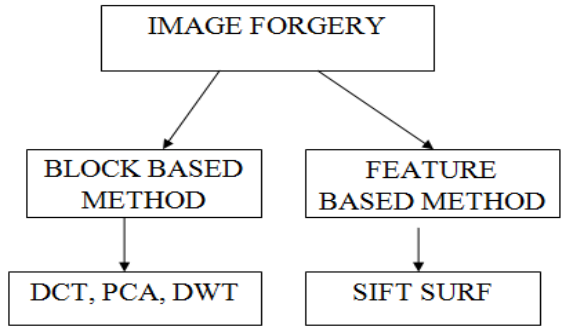

Fig: -4 Block Diagram of Copy Move Forgery

The goal of the paper is to examine the different methods of copy move forgery detection. There are a number of methods that provide a solution for copy move forgery detection. The most widespread technique is copy paste where one part of the image is copied to another part of the same image. Detection of forgery become more difficult when copied part is rotated, cut, extended etc Hence copy paste is also known as copy move forgery.

Mainly copy move forgery is classified into two types. They are block based method and key point based method. In block based copy move forgery method features are extracted from each blocks of image. In this method image is divided into a blocks of size of 16*16 and further more each block is divided into 4 smaller and equal blocks. Nine different features from these blocks are extracted and used for the detection of copy move forgery. Mainly copy move forgery based on Discrete Cosine Transform(DCT), Discrete Wavelet Transform(DWT), Principle Component Analysis(PCA), Singular Value Decomposition(SVD) etc techniques comes under block based method.

The other method is key point based forgery detection which rely on the identification and selection of high entropy image regions. The key point based algorithms usually require two steps for detecting and describing local visual features. In the first step, the localization of the interested point has done. In the second step, the construction of the robust local descriptor is done, such that it should be invariant to affine transformation. Mainly keypoint method is of two types which are SIFT and SURF.

3.1. Block Based Method

In block based method, it was observed that several techniques are good for accurate detection and location of copy move forgery.

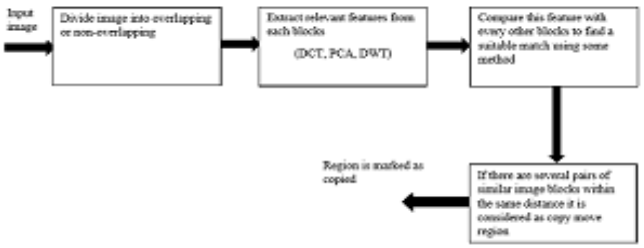

Fig:5 Block Diagram of Block Based Method

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In [4] the author propose a method based on blocks and their features. Features based methods was used to improve the accuracy of detection of false image. The method will uses DCT coefficients and properties of discrete Fourier transformation. Features were compared in order to detect false image and also register the location of region in the image that are manipulated. In [5], the author proposed a method where the image is divided into blocks with a fixed size and discrete cosine transform(DCT) was performed on each block and each block represent DCT coefficients. Each DCT block was represented by a circular block and four properties have been pulled out to reduce the dimensions of each blocks. Feature vectors are sorted lexicographically and duplicated blocks of image are compared with the threshold value.

Passive forensics for copy move forgery image using DCT and SVD was proposed in [6]. A method that has a much higher percentage of detection with the images with such parts were described. Each image is divided into blocks of the same size and DCT is applied to each. The result shows the proposed method can detect image in the figures with same region even when image is further compressed,

In [7] the author proposed a method using DCT binary vectors. The method for false image detection based on the contrast with the help of discrete cosine transform vectors. The image was divided into blocks and for each block, DCT coefficient were calculated. Further feature vectors were created for each block on the basis of DCT components. The proposed method can detect false image when the contrast of the image is changed.

In [8] the paper proposed an improved algorithm based on Discrete wavelet transform(DWT) which is used to detect such cloning forgery. In this technique at first DWT is applied to input image for a reduced dimensional representation. Then the compressed image is divided into overlapping blocks. Lexicographically sorting is performed and duplicated blocks are identified. Due to DWT usage, detection is first carried out on the lowest level image representation. This approach will increase the accuracy of detection process and reduce the time needed for detection process. Block matching appears to be more efficient approach. Utilising such an approach the author [9] proposed a new copy move forgery detection algorithm which slides a b*b block over an N*N image pixel by pixel resulting K=(N-b+1)2 blocks. Each block is column wisely reshaped into a b^2 long row vectors otherwise known as a feature vector and inserted into $k*b^2$ feature matrix. PCA is performed to an appropriate representation of each row of the feature vector matrix. Performing PCA on the feature matrix involve computing the corresponding covariance matrix and obtaining a projection of each block with higher eigen values thereby reducing the dimension of the feature vectors.

3.2 Key Point Based Method

The second technique of copy move forgery is keypoint based method. Keypoint based techniques based on identifying and selecting higher entropy image region. Here feature vectors are extracted per keypoint. Consequently, very few feature vectors are estimated resulting in reduced computational complexity of feature matching and post processing.

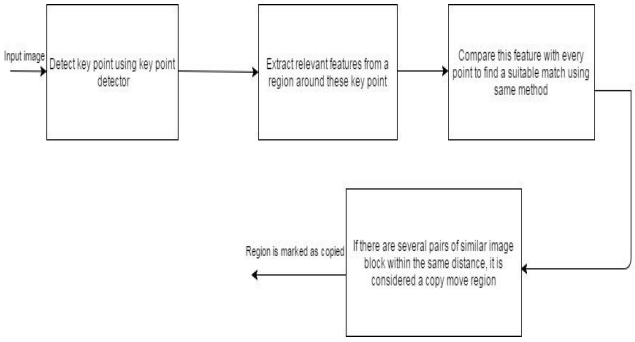

Fig:6 Block Diagram of Key Point Based

The lower number of feature vectors indicate that post processing threshold are also to be lower than that of block based method.

The keypoint based algorithms require two steps for detecting and describing local visual features. In first step, the localization of interest is done. In the second step, the construction of the local descriptors is done which is robust such that it should be invariant to affine transformation. Keypoint based copy move forgery is mostly based on SIFT and SURF. Both methods are based on scaled space.

SIFT was proposed by David Lowe in the year 2004 as a continuation of his earlier work on invariant feature detection. The author proposed a method for detecting distinctive invariant features from images that can be later used to perform reliable matching between different views of an object or scene. The two main key concepts used are distinctive invariant features and a reliable matching. Sift comprised of 4 main steps which are scale space extrema detection, keypoint localization and filtering, orientation assignment and keypoint descriptors. SURF was proposed by Bayetal in 2006 and ensures the high speed in the three of features detection steps: detection, description and matching. The SURF algorithm speeds up the SIFT detection process without scarifying the quality of detected points. The potential keypoint detected by using the Hessian matrix and Non-maximum suppressions. The authors [10] proposed an improved SIFT based algorithm. The local interest points are detected, and the SIFT features for such keypoints are computed. At each interest point, a 128-dimensional feature vector is generated from the histogram of local gradients in its neighborhoods. After this, feature matching based clustering is performed on coordinates of the matched points. After clustering, keypoint matching is done. It mainly concerns with the matching of extracted feature keypoints from SIFT algorithm. Finally, the algorithm determines which geometrical transformation was used on the original portion of the image. For this, Homographic matrix of at least three matched points is computed. This 3x3 matrix is computed using maximum likelihood estimation of the homography. Takwa Chiha. proposed20 a hybrid method based on SIFT and SVD. In this algorithm, the forgery detection is done by identifying the keypoints of an image using SIFT and matching identical features using SVD. Firstly, the image undergoes the SIFT transform and calculates the locations of interest point invariant to scale and orientation. In the second step,

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

features are extracted from detected keypoint sin order to eliminate more keypoints from the list by finding those that are likely to remain stable over transformations. The third stage identifies the dominant orientations for each selected key-point based on its local image patch. In the final stage, a local feature descriptor is computed at each keypoint based on a patch of pixels in its local neighborhood. So, the output of this step is SIFT keypoints that are represented with 128-dimensional descriptor vectors and their locations. The proposed method reduces the number of false points matching problem and is robust to geometrical transformations.

Shivakumar and Baboo proposed [12] an algorithm in which, they have first extracted the SURF features. In the second step, key-point matching is done. After that, a verification step is performed which filters matching pairs that follow a common pattern. The experiments carried out show that the algorithm detects copy-move forgery with a minimum false positive. The algorithm is even robust to rotation, scaling, and Gaussian noise.

Mohammad Hashmi proposed [13] combining SURF and Wavelet Transform. The image is first transformed into wavelet domain. SURF is applied on this transformed image for keypoints detection and feature extraction. The SURF feature descriptor vector is obtained. Because of the multispectral components produced by the wavelet, the features are more predominant. The algorithm finds a match between the descriptor vectors and marks forged regions.

IV. CONCLUSION

Detecting forgery in the digital images is one of the challenges of this exciting digital age As copy-move forgery is one of the most popular image forgery so importance of forgery detection techniques is increasing day by day. As region duplication is performed in copy-move forgery so at least two similar region will be present in tampered image. Copied segment will have similar properties like noise components, dynamic range and color palette maintaining compatibility to rest of the image. Copy-Move forgery detection can be divided into two categories Block-based and Key point based methods.

REFERENCES

1. Snigdha K. Mankar, Prof. Dr. Ajay A. Gurjar, ‘ Image Forgery Types and Their Detection: A Review’, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 4, April 2015
2. Nishtha Parashar and Nirupama Tiwari, ‘A Survey Of Digital Image Tampering Techniques’, International Journal of Signal Processing, Image Processing and Pattern RecognitionVol.8, No.10 (2015), pp.91-96
3. Ardizzone E, Bruno A, Mazzola G. Detecting multiple copies in tampered images. In: Image Processing (ICIP), 2010 17th IEEE International Conference on. IEEE; 2010. p. 2117–20.
4. R. Singh, A. Oberoi, and N. Goel, “Copymove forgery detection on digital images,”International Journal of Computer Applications, vol. 98, no. 9, pp. 17–22, 2014.
5. Y. Cao, T. Gao, L. Fan, and Q. Yang, “A robust detection algorithm for copy-move forgery in digital images,” Forensic science international, vol. 214, no. 1, pp. 33–43, 2012.
6. J. Zhao and J. Guo, “Passive forensics for copy move image forgery using a method based on DCT and SVD,” Forensic science international, vol. 233, no. 1, pp. 158–166, 2013.
7. S. Kumar, J. Desai, and S. Mukherjee, “Copy move forgery detection in contrast variant environment using binary DCT vectors,” International Journal of Image, Graphics and Signal Processing, vol. 7, no. 6, pp. 38–44, 2015.
8. Preeti Yadav, Yogesh Rathore, “Detection of Copy-Move Forgery of ImagesUsing Discrete Wavelet Transform”, International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 04 ,pp. 565-570, April 2012
9. C. Popescu and H. Far id, “Exposing Digital Forgeries by Detecting Duplicated Image Regions,” Technical Report, TR2004-515, Department of Computer Science, Dartmouth College, 2004
10. Swapnil HK, Gawande A. Copy-Move Attack Forgery Detection by Using SIFT. International Journal for Innovative Technology and Engineering IJITEE. 2013;2(5).
11. Chihaoui T, Bourouis S, Hamrouni K. Copy-move image forgery detection based on SIFT descriptors and SVD-matching. In: Advanced Technologies for Signal and Image Processing (ATSIP), 2014 1st International Conference on. IEEE; 2014. p. 125–9.
12. Shivakumar B, Baboo LDSS. Detection of region duplication forgery in digital images using SURF. IJCSI International Journal Computer Science Issues. 2011;8(4).
13. Hashmi MF, Anand V, Keskar AG. A copy-move image forgery detection based on speeded up robust feature transform and Wavelet Transforms. In: Computer and Communication Technology (ICCCT), 2014 International Conference on. IEEE; 2014. p. 147–52.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)