IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 53-58
www.iosrjournals.org

Review on Copy Move Image Forgery Detection Methods

Ameera Beegom J[1], Akhil Paulose[2], Deepa S S[3]
[1]*PG Scholar, College Of Engineering Trivandrum*
[2]*Assistant Professor, Vimal Jyothi Engineering College, Kannur*
[3]*Assistant Professor, College Of Engineering Trivandrum*

Abstract: *In today's contemporary life, digital images have momentous importance because they have become a prominent source of information distribution. However, the increased usage of image changing tools made it easier to forge the contents of a digital image; making the truthfulness untruthful. Many techniques can be used to falsify the digital images. Copy move forgery is a method where a definite part of an image is copied and pasted elsewhere in the same image to cover unwanted part or object. In this writing, we attempted to review some feature extraction methods for copy move forgery detection techniques. The passive technique of digital image forgery tries to identify forgery in digital images without any preceding information and the copy move forgery is a type of passive method. A look at various techniques is also included.*
Keywords: *Passive, Copy move, Forensics, Forgery, Authenticity, Digital image*

I. Introduction

The usage of digital images increases day by day. The image content is changed by using any image editing tools. Thus the image can be manipulated with these tools by simply drag and drop its features or components .These actions can be done by anybody which doesn't need much technical knowledge about this. Therefore, it is essential to authorize the contents of the image. So the aim of image forgery tools is to detect and locate the forgery.

Image Forgery can be perceived by two approaches: Active approach and Passive approach.The concept of watermarking or digital signature or both are used in active approach. But in passive approach the image forgery can be detected without any prior information of the image.Passive approach is classified into three categories:

(i) Copy-move forgery
(ii) Image Splicing
(iii) Image Retouching

(i) **(ii)**

Fig 1. An example of Copy Move Forgery (i) original image (ii)forged image [5]

In the method of copy move forgery one part of the image is affixed into another portion of the same image. Here the aim is to cover some specific thing in the original image using another portion of the same image.But Image splicing means a portion of one image is taken and used on any portion of another image to form a resultant forged image.That is Image splicing is the combination of two or more images which are combined to create a fake image. Image retouching means there is an enhancement or reduces some features of the original image.

The primary objective of Image Forensics techniques is to identify the type of tampering that has been done on the image.There are many methods available for detecting and localizing such forgeries.The detection of Copy Move forgery is categorized into three.Block based, Key point based and brute force based. The simplest approach is brute force based and is detected by using exhaustive search.But, this approach is computationally very expensive.

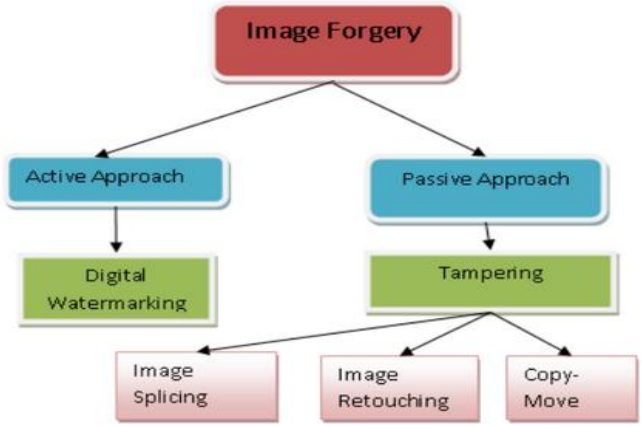

Fig 2. Image forgery methods

The rest of the survey is presented as follows: the key steps of forgery detection are introduced in section II. In Section III, a summary of various techniques in the area of copy move forgery detection is presented. Finally, the concluding remarks and challenges are given in Section IV.

II. Key steps for copy move forgery detection

This section illustrates the basic steps used for detecting the copy move forgery.
Step 1: Preprocessing : This converts the color image into a gray scale image

$$I=0.299R+0.587G+0.114B$$

where R,G,B are three input channels, and I is obtained the gray image.

Step 2: Feature Extraction : Here the feature vectors are identified. In block based method , the image is split into overlapping or non-overlapping blocks of fixed size.From each block of the image, the features are extracted . While in key point based methods, the features are extracted around the keypoints.

Step 3: Matching: This step mainly identifies the duplicated regions of the image. The duplicated regions present in an image can be found in matching step. This can be done by comparing the feature vectors. In block based methods, for placing similar feature vectors to each other lexicographical sorting is applied .The approximate nearest neighbor can be identified by any searching procedure which helps in feature matching for key point based methods.

Step 4: Filtering : The number of false matches can be greatly reduced by using any filtering techniques.

Techniques In Copy Move Forgery DETECTION
The following section describes the various techniques in copy move forgery.

1.Block Based Image Forgery Detection Techniques.

Here the image is split into blocks of equal size to bring out the features of each block. Then these features are compared with each other to find out suitable match. After finding these match, the corresponding block pairs are treated as copy move.

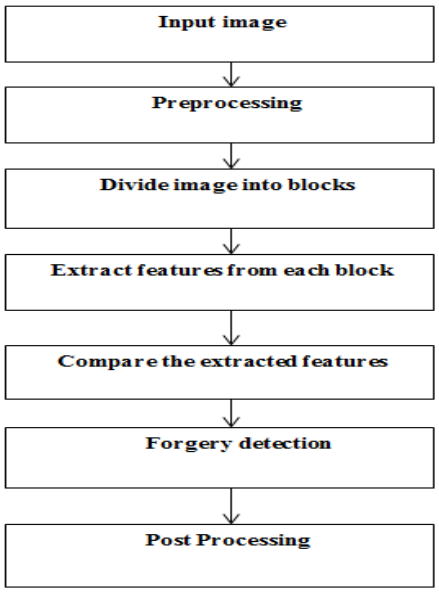

Fig 3: Block based method

For feature extraction , any of the following methods can be used.
Several Block based Copy Move Image forgery detection techniques are described as follows.

Fridrich et al [4] proposed a method for detecting copy move forgery based on DCT.The various steps involved in this method are discussed as follows:

(a) Preprocessing the input image.
(b) Divide the image into blocks of the same size.
(c) For each block, apply DCT.
(d) Create feature vectors and sort lexicographically.If two blocks in input image are same then their corresponding feature vectors will also same.
(e) If the two feature vectors will be same and the distance between two should be more than block size then calculate the shift vector s and increase the count for s where s= (s1, s2) = (x1-x2, y1-y2), (x1,y1) and (x2,y2) are the coordinates of the upper left corner of the similar block pairs.
(f) For each shift vector a counter c is considered and per similar block pairs the counter is increment by 1 as C(s1,s2)= (s1,s2)+1.
(g) If the counter exceeds the threshold value mark the region as duplicated.
(h) Color, the pixels in the forged region to highlight the region duplication.

The Wavelet based region duplication forgery detection was proposed by Wang et al [6]. The detailed steps are explained as below:

(a) Preprocessing the input image.
(b) Split the image into blocks of equal size.
(c) Create feature vectors by applying DWT in each block.
(d) The sorting operation like lexicographic is performed in the rows of feature vectors. Now compare the feature vectors and if two consecutive rows of the vectors are similar, then stores the positions of the identical blocks.
(e) Then calculate the shift vector for a suspected pair of blocks and for each shift vector a counter c is taken and the counter is increment by 1for similar block pairs.
(f) If the counter is exceeding the user defined threshold , mark the region as forged.

In [7] Farid et al presented a technique for copy move forgery detection based on Principal Component Analysis. In this, the length of the feature vector is reduced and also the computational cost is reduced.

2. Key point Based Image Forgery Detection Techniques.

Here the keypoint detector algorithms are used to identify the key points. Then the feature matching is performed by comparing the feature vectors which is extracted from a region around these key points. It extracts feature point using different methods like SIFT, SURF etc without any image subdivision.The approaches like clustering, Euclidean distance, the nearest neighbor etc can be used for feature point matching . A forgery can be

found if matching features are found. The post processing techniques, such as RANSAC can be used for removing false matches.

Various techniques for detecting copy move forgery in images are discussed as follows:

Baboo et al [8] proposed a method for detecting region duplication forgery using SURF. The steps involved in this method are discussed below:

SURF (Speeded Up Robust Features) is used to extract features and it is a robust local feature detector. The feature detector is based on Hessian matrix. For image duplication, any geometric transformations such as scaling and rotation are applied to the image but SURF is invariant to these transformations.

The various steps for SURF detectors and descriptors are explained as follows:

(a)Preprocessing the input image.

(b)Integral Image: Create the integral image representation of the input image.Then the pixel sums over upright rectangular areas can be calculated. The speed up of the calculation of any upright rectangular area can be increased in this way. For any point in an image, the integral image is calculated by the sum of the values between the point and the origin.

(c) Keypoint Detection: For detecting the keypoints in an image,SURF uses Hessian matrix.Then calculate the determinant of Hessian matrix. If it is positive ,the points will be treated as extrema otherwise it will be discarded. The following shows the Hessian matrix representation.

$$H(x,\sigma) = \begin{bmatrix} L_{xx}(x,\sigma) L_{xy}(x,\sigma) \\ L_{xy}(x,\sigma) L_{yy}(x,\sigma) \end{bmatrix}$$

where $Lxx(x,\sigma)$ is the convolution of the Gaussian second order derivative with the image I in point x and similarly others.These derivatives are called Laplacian of Gaussian. In order to create the scale space convolution is applied to image with varying size box filters.SURF uses the below equation for the approximation of the Hessian determinant.

$$det(Happrox)= DxxDyy-(0.9Dxy)^2$$

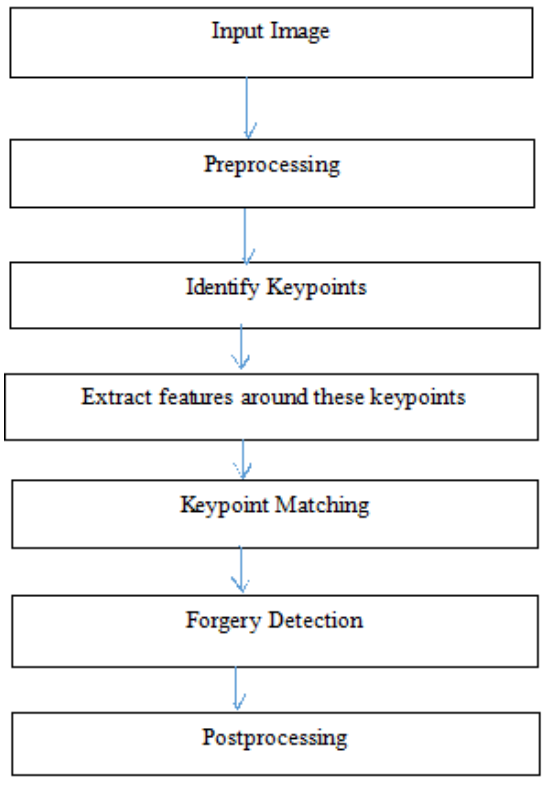

Fig 4: Key point based image forgery

(d)Feature Vector Generation : Around the keypoint construct a square region where keypoint is taken as the center point. Then the square is divided into 4X4 sub squares.After that find the Haar wavelet responses for each of these areas. Each sub region gives 4 responses.

$$Vs=[\Sigma dx ,\Sigma dy, \Sigma|dx|, \Sigma|dy|]$$

where dx is the horizontal response and dy is the vertical response.

(e)Matching : After getting the keypoint and the feature vector, the job is to compare each feature vector with others. Then calculate the dot products between each feature vector with others and take the inverse cosine angles of dot products. After that sorting is applied and store their values and index number.T hen compare the ratio of the nearest neighbor value with a predefined threshold.If it is less than the threshold which means match exists.The resulting SURF is invariant to rotation, scale, brightness .

Lowe [1] proposed a method for detecting copy move forgery using SIFT.The steps involved in this method are discussed below:

Scale Invariant Features Transform (SIFT) is a very efficient method to detect duplicated region. It is not only just scale invariant but also provides good detection results for rotation, illumination and invariant viewpoint changes. The Key-Point extracted by SIFT are invariant to rotation and scaling.

The steps for SIFT detectors and descriptors are explained as follows:

(a)Preprocessing the input image.

(b)Scale-Space Extrema detection : This is based on the different scale of the same image with a scale-spaced function. The image scale space function is defined as:

$$L(x,y,\sigma)=G(x,y,\sigma)* I(x,y)$$

where * is the convolution operator. Thus, $L(x,y,\sigma)$ is obtained by the convolution of a variable scale Gaussian, $G(x,y,\sigma)$ with an input image $I(x,y)$. For efficient detection of keypoints , Difference of Gaussian function $D(x,y,\sigma)$, which can be computed from the difference of two nearby scales separated by a constant multiplicative factor k as:

$$D(x,y,\sigma)=L(x,y,k\sigma)-L(x,y,\sigma)$$

(c)Keypoint Detection : This step used to eliminate the keypoints those had low contrast or poorly localized at on edge. The second order Hessian matrix is used to remove the edge response of the DOG operator.

(d)Orientation Assignment : The magnitude of gradient $m(x,y)$ and orientation $\theta(x,y)$ is calculated as:

$$m(x,y) = \sqrt{(L(x+1,y)-L(x-1,y))^2+(L(x,y+1)-L(x,y-1))^2}$$

$$\theta(x,y) = \tan^{-1}((L(x,y+1)-L(x,y-1))/(L(x+1,y)-L(x-1,y)))$$

An orientation histogram is obtained from the gradient orientation of sample point feature vectors.

(e)Feature vector Generation : The orientation histogram values are used to form feature vectors. Finally, 128 dimension feature vectors are obtained.

(f)Matching: The extracted feature vectors are grouped using any clustering methods. For the matching process, the feature vectors among two clusters are compared. In order to improve the matching efficiency, also calculate the angle between the vectors of any two clusters. If the ratio between angles is less than a predefined threshold , then there a match exists.

Reference no	Feature Extraction Method	Feature Matching Parameter	Performance
[1]	SIFT	Hierarchical clustering	Multiple copied region is detected
[1]	SIFT	Euclidean distance	Give good performance and invariant to scale and rotation of the pasted object.
[2]	SURF	Feature Vector	Fast process, Detect Scaled and rotated object , reduce computational complexity
[4]	DCT	Feature length	Computational complexity is high.Some limitations are there in case of natural images.
[6]	DWT	Feature length	The feature vector dimension reduction, but gives low accuracy if the forged area is at center.

Table 1: Comparison of Various Feature Extraction methods

III. Conclusion

As the copy move forgeries have taken conventional in our daily lives, there is a growing need of passive image forgery detection techniques to address various features of image forensics. Although several methods have been proposed in the field of copy move image forgery detection for certain cases, but a method

which gives a comprehensive solution is still needed. This study presented here a brief review on various techniques in copy move forgery detection.

References

Journal Papers:

[1]. David G. Lowe., *"Distinctive Image Features from Scale-Invariant Key-Points", International Journal of Computer Vision ,2004,60(2), pp.91-1*

[2]. Xu Bo, Wang Junwen, Liu Guangie and Dai Yuewei., *"Image Copy-Move forgery Detection Based on Surf", International Conference on Multi-media Information Networking and Security, 2010 , pp.889-892*

[3]. Mohammad Farukh Hashmi, Aaditya Hambarde., "*Copy move forgery detection using DWT and SIFT", International Conference on Intelligent System Design and applications, 2013, pp.188-193.*

[4]. J. Fridrich, D. Soukal, and J. Lukas, *"Detection of Copy-Move Forgery in Digital Images", in Proceedings of Digital Forensic Research Workshop, August 2003*

[5]. Neha Jadhav, Suvarna Kharat, Punam Nangare,*"Copy-Move Forgery Detection using DCT", International Journal for emerging Technologies and Engineering, Vol 2 Isuue 3 March 2015, ISSN 2348-8050.*

[6]. Wang Y, Gurule K, Wise J, Zheng J. *"Wavelet based region duplication forgery detection." ,Proceedings of the 9th International Conference on Information Technology: New Generatio (ITNG '12); April 2012; IEEE; pp. 30–35.*

[7]. A.C.Popescu and H.Farid, *"Exposing Digital Forgeries by Detecting Duplicated Image , Regions,"Technical Report,TR2004-515,Depart Department of computer Science, Darmouth College, pp.758-767, 2006*

[8]. B L Shivakumar and Lt.Dr.S Santhosh Baboo, *"Detection Of Region Duplication Forgery in DigitalImages using SURF, International Journal Of Computer Science Issues, Vol 8, Issue 4, No 1, July 2011.*

[9]. Swapnil H.Kudke, A.D.Gawande, *"Copy-Move Attack Forgery Detection by Using SIFT," International Journal of Innovative Technology and Engineering (IJITEE), Vol.(5), ISSN 2278-3075, 2013*

[10]. I.Amerini,L.Ballan,R.Caldelli,A.D.Bimbo,and G.Serra, *"A SIFT-based Forensics Method for Copy-Move Attack Detection and Transformation Recovery," IEEE Transaction on Information Forensics and Security, Vol.6, no.3, pp.1099-1110, 2011.*

[11]. V.Christlein,C.Riess, J.Jordan, C.Riess, and E.Angelopoulou, *"An Evaluation of popular Copy-Move Forgery Detection Approaches," IEEE Transactions on Information Forensicsand Security, Vol.7, pp.1841-1854, 2012*