IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p-ISSN: 2278-8735
PP 41-45
www.iosrjournals.org

Gabor Filter – HOG Based Copy Move Forgery Detection

Monisha Mohan[1], Preetha V.H[2]
[1](Mtech student, Department of ECE, Sree Chitra Thirunal college of Engineering, Trivandrum, Kerala)
[2](Assistant Professor, Department of ECE, Sree Chitra Thirunal college of Engineering, Trivandrum, Kerala)

Abstract: *Digital images are used in all places and it is easy to forge and edit because of availability of various image processing and editing software. Copy move forgery is the most common method of image tampering in the case of forged image. Nowadays researchers start studying on detection of different forgery techniques. This paper proposes a block based copy move forgery approach using gabor filter and HOG features. Generally gabor filter is used for texture analysis but it has a disadvantage of having less recognition rate due to almost same value of histogram descriptor. Hence we propose a new method to overcome the disadvantage of gabor filter by using HOG features. The main advantage of this method is better invariance to change in illumination and shadowing, this will capture more copy move forgery compared to conventional methods.*

Keywords: *Copy move forgery, Gabor filter, HOG, Image tampering*

I. Introduction

Nowadays with the availability of powerful digital image processing programs such as photoshop,3D max etc it is relatively easy to create digital forgery from one or multiple images. This will create a serious problem to the extent of trust that can be placed in the accuracy of digital content, especially in cases like presenting a paper in front of courtroom as some evidence. Different photo editing softwares such as Adobe photoshop and some of the complex digital technology are universal and they made the process of manipulating image to form forgery a typical practice and hence digital forgery technique arrived as a result of this. Digital forgery techniques can be classified into two approaches which are active and passive approach. Active approaches are commonly used in watermarking or digital signatures in which we can detect the image is tampered if special information cannot be extracted from that obtained image. Passive approach is entirely different from that of active method. This method is otherwise known as "Blind forgery" which uses the received image only for assesing its accuracy or integrity without any signatures or watermark of the original image from the sender

Fig:1 Original image and forged image

Image tampering is defined as adding or removing relevant features from an image without leaving any information of tampering and hence it is considered as manipulation of image. Image tampering is broadly classified into three categories, they are 1.Image Splicing, 2.Image Retouching and 3.Image CloningImage splicing is the oldest technique in which mixtures of two or more image 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. This paper aims at reviewing the two methods of copy move forgery

detection. The rest of the paper is arranged in the following way. Section2 discuss the literature survey. Section 3 covers the proposed method. Section 4 covers experimental result. In section 5, we summarize the paper.

II. Literature Review

In [1] block based method and there features are proposed. Feature based method were used in order to increase the correctness of detection in tampered image. The proposed method uses DCT coefficients and properties of Discrete Fourier Transform. These features were compared in order to detect the tampered region and to also register the location of region in the image.

In [2] the approach was based on blocks and uses texture of blocks. The main objective of this approach was to determine if the texture was applicable for some applications. In [3] the author for the first time proposed the copy move forgery using DCT on small overlapping blocks. Using DCT coefficients, feature vectors are formed. Feature vectors are sorted lexicographically and similarity between the blocks were analyzed. The author proposed [4] an algorithm which involves 3 steps which are cluster matching, texture analysis and keypoint clustering. Hierarchial tree clustering algorithm is used for clustering the keypoint. The algorithm will propose a texture based analysis to find similar cluster matching. The algorithm is robust for false matches. The main disadvantage of this method is that the algorithm fails if the number of cluster formed is too small or large enough. In paper [5] the author uses both SIFT and DWT. The DWT method is used for the reduction of dimensionality. When DWT is applied to an image it will decompose into 4 parts LL, LH, HL & HH. Considering only any one of the part that is LL, the most information of an image is accompined in this part, and hence SIFT features are extracted from LL part. This will extract the key features and finally find the similarity between various descriptor vectors.

Lowe proposed [6] a new technique which is based on SIFT features which means Scale Invariant Feature Transform which is performed by extracting 128 vectors. SIFT descriptors of copied and pasted region are computed and matched for detecting tampered region. This method is robust against JPEG compression and the method will compute distinct features of local image patches that are not changing to scaling and rotation and are powerful to change in noise, illumination etc. The Kaur A, Sharma R. [7] proposed a novel method to detect the combination of different post-processing operations. The method will uses a mixture of DCT and SIFT. As DCT is strong against the JPEG compression and the Gaussian noise due to robust energy and SIFT is robust against the rotation and scaling. Hence, the proposed method is able to detect the forgery in the images even it has gone under distant post-processing operations. The forgery detection rate is increased as if one method fails to detect the forgery the other succeeds in detecting the forgery.

III. Proposed Work

3.1using Gabor Filter

In image processing, a gabor filter which is named after Dennis Gabor [8] is a linear filter used for edge detection. Frequency and orientation representations of gabor filters are identical to those of human visual system and they have been found to be exactly appropriate for texture representation and discrimination. In the spatial domain, a 2D gabor filter is a Gaussian kernel function modulated by a sinusoidal plane wave. The general form of a 2D gabor filter is expressed as:-

$G\sigma,f,\theta=g\sigma(x,y).\ \exp[2\Pi jf(x\cos\theta+ y\sin\theta)]$

Where

$g\sigma(x,y)=1/2\Pi\sigma^2\ \exp[-(x^2+y^2)/2\sigma^{2]}]$

where $j=\sqrt{(-1)}$,f is the frequency of the sinusoidal wave, ɵ controls the orientation of the function and gσ(x, y) is the Gaussian function with scale parameter σ. The parameters of the Gabor filter are therefore given by frequency f, orientation h, and the scale σ.

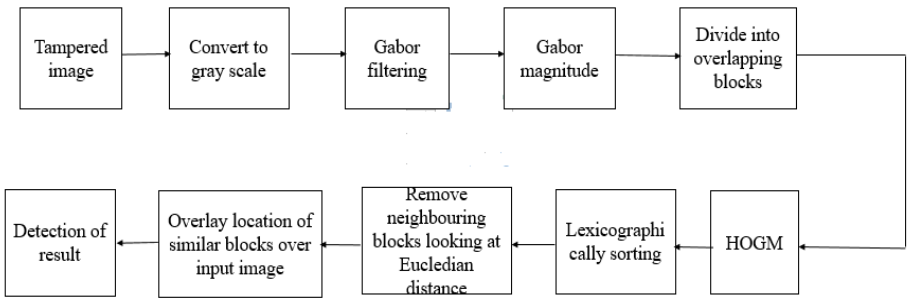

Fig:2 Block diagram Copy move forgery using Gabor filter

In this method , the HOGM scheme extracts the maximum magnitude values of the image from different orientations because the maximum magnitude values shows the orientation of strongest textural information, but the main disadvantage of using this method is less recognition rate due to almost same values of HOGM descriptors. Here multiple parameters to be fine tuned for each image to achieve a decent recognition rate. Gabor filter is widely used for human facial feature extraction alone, restricting the reach of method in copy move forgery detection. The result of Gabor filter image is shown below:-

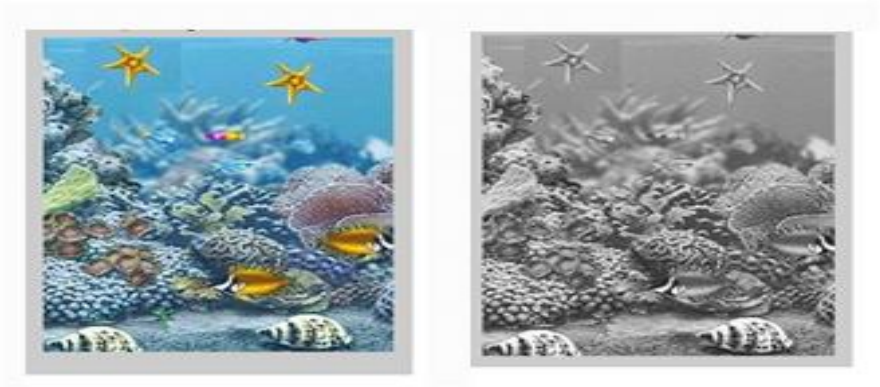

Fig:3 Input image and gray scale image using gabor filter

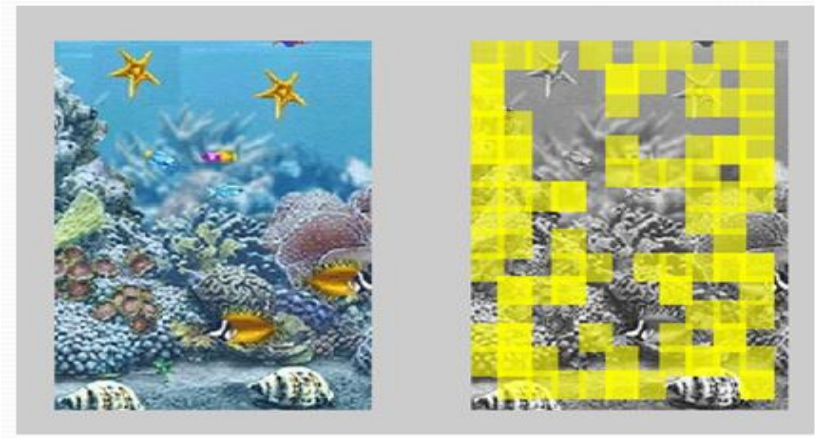

Fig:4 Output result using gabor filter

3.2. Using Hog

The histogram of oriented gradients (HOG) is a feature descriptor used in computer vision and image processing for the intention of object detection. This method counts development of gradient orientation in localized portions of an image. This technique is similar to that of edge orientation histograms, Scale invariant feature transform descriptors and shape contexts but distinction in that is computed on a dense grid of uniformly spaced cells and uses overlapping local contrast normalization for improved accuracy.

Here the main approach of our research is to detect the duplicated region by using HOG features [9]. The tampered image is first converted to gray scale image by using the equation:-

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

Where R, G, B denotes red, green and blue channel of image and I represents the luminance components of YCbCr space. To identify the forged region, the image is divided into overlapping sub-blocks. Histogram of oriented gradients (HOG) is applied to each block for extraction of features. In order to calculate the gradient values, we apply the 1D centered, point discrete derivative mask in both the horizontal(D_X) and vertical (D_Y) direction.

D_X= [-1 0 1]

D_Y= [-1 0 1]

For a given image I, we obtain x and y derivaties using a convolution operation $I_X=I_X*D_X$ and $I_Y=I_Y*D_Y$. The magnitude of the gradient is given by

$$|G|=\sqrt{(I_X^2+I_Y^2)}$$

The gradient orientation is given by

$$\theta=\arctan [I_Y/I_X]$$

In order to resist the illumination and contrast changes, the gradient strengths are locally normalized by grouping the cells to larger spatially connected blocks. After applying HOG to each block, a HOG descriptor matrix of same size of block is arranged to represent each corresponding block. Then the proposed method is arranged lexicographically and then discards the neighbouring block by looking at the eucledian distance. The final step is to overlay similar blocks over the input image. The main advantage of using this method over the previous method is they are invariant to geometric and photometric transformations, since the pixel votes are bilinearly interpolated and hence there will be minimum aliasing.

IV. Experimental Result

The first method which uses gabor filter doesn't detect the forgery due to its less recognition rate. Hence we detect the forgery by using HOG features. Various steps are used for detecting this type of forgery

Fig:5 Input image

Fig:6 Gray scale image

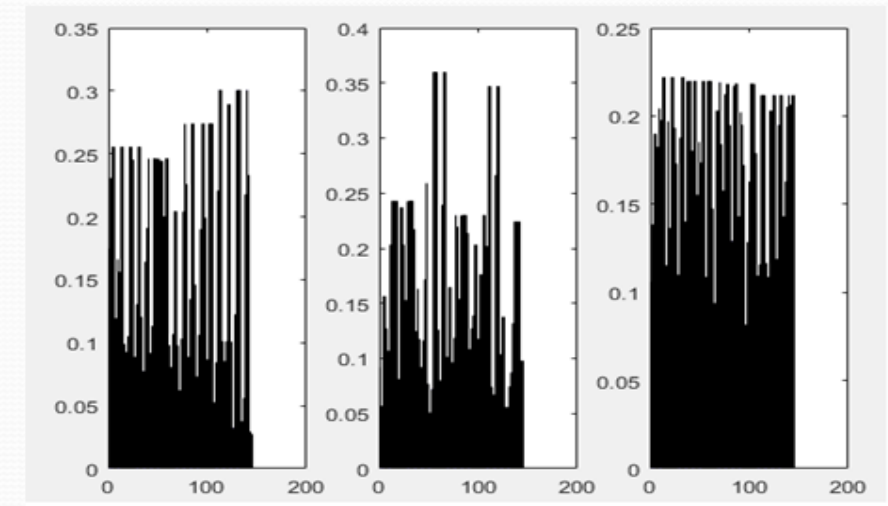

Fig:7 Histogram of oriented gradients of selected blocks

Fig:8 Output result

V. conclusion

Copy-move is a common method for image forgery. It works without any digital watermarks or signature information. In this paper we propose an algorithm using gabor filter and HOG feature for detecting copy move forgery and we had proved a better result of having HOG features other than using gabor filter. This algorithm gave best performance for the detection of copy move forgery and also to detect multiple copy move forgery.

References

[1]. R. Singh, A. Oberoi, and N. Goel, "Copy move forgery detection on digital images," International Journal of Computer Applications, vol. 98, no. 9, pp. 17–22, 2014.

[2]. E. Ardizzone, A. Bruno, and G. Mazzola, "Copy-move forgery detection via texture description," in Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence, pp. 59–64, ACM, 2010.

[3]. J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy-move forgery in digital images," in Proceedings of Digital Forensic Research Workshop, Cleveland, Ohio, USA, August 2003.

[4]. 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.

[5]. Hashmi MF, Hambarde AR, Keskar AG. Copy move forgery detection using DWT and SIFT features. In: Intelligent Systems Design and Applications (ISDA), 2013 13th International Conference on. IEEE; 2013. p. 188–93.

[6]. D.G Lowe, ''Distinctive image features from scale invariant key points", International Journal of Computer Vision, vol.60, no.2,pp. 1053-1056,2009.

[7]. Kaur A, Sharma R. Copy-move forgery detection using DCT and SIFT. International Journal of Computer Application. 2013;70(7):30–4.

[8]. Gul Muzaffer, Ozge Makul, Beste Ustubioglu and Guzin Ulutas, "Copy Move Forgery Detection Using Gabor Filter and ORB", Proceedings of 2016 International Conference on Image Processing, Production and Computer Science (ICIPCS'2016) , London (UK), March 26-27, 2016 pp. 23-29

[9]. Meera Mary Isaac, Dr. M. Wilscy "A Key point based Copy-Move Forgery Detection using HOG features", International Conference on Circuit, Power and Computing Technologies [ICCPCT], IEEE 978-1-5090-1277, 2016