International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-04, Issue-06, Sep 2018

Analysis of Copy Move Image Forgery Detection Using Histogram of Orientated Gradient

Ashok T. Gaikwad

Institute of Management Studies and Information Technology, Aurangabad, (M.S) 431001, India

**Corresponding Author: drashokgaikwad@gmail.com*

Abstract - Nowadays, Digital images are widely used by human in society. Easy availabilities of image editing software and tools images were doctorate by peoples. In this paper, we present algorithm for to detect image forgery detection using HOG (Histogram of Orientated Gradient). First of all, we transferred RGB image to the Grayscale read image. Then Grayscale image is divided to the overlapping block. Apply HOG for extract the features. Then lexicographically sorting and perform the matching process for detect forge region. Then draw the duplicate region. For evaluation of our system we calculate Positive Rate, False Positive Rate and Identification Rate.

Keywords — Forgery, HOG, TPR, FPR

I. INTRODUCTION

Now a day digital images are becomes as main information carrier. The reason is as ampleness of acquisition, distribution and storage of image. Image in News Paper and magazines peoples can accept as a truth, also accept as evidence in court of law. Now a day due to the developed technology peoples can easily access image and editing software which alter or change image meaning. Peoples did manipulation in images for malicious purpose. Image forgery detection has two approaches. First is active [1-3] and second is passive [4-6]. Active image forgery detection needs prior information of image, but in passive image forgery detection there is no need of prior information of image. Active forgery detection method has consisted Digital Signature and Digital Watermark [7]. Passive forgery detection has also two types, first Forgery type Dependent and Forgery Type Independent. Forgery Type Dependent has again two types i.e. Copy – Move Forgery Detection and Image Splicing Detection. Forgery Type Independent has two types Retouching Detection and Lighting Condition.

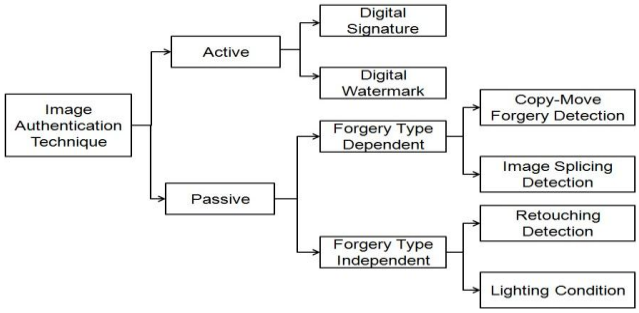

Fig.1image forgory detection methods

Out of these types of forgery in passive forgery Copy-Move is most common used [8]. In Copy-Move forgery one region of image is copied and past another place of same image. In this to detect image forgery is very difficult because pasted part is coming from same image that's why almost statistical properties are matched with the rest part of image. In splicing, object from one image splice with source image.

The article was organized with different section the remaining section was literature survey in the section II . The methodology of the system was covered in the section III. In the section IV conducted with Results and discussion. Finally, the conclusion and future work on section V.

II. RELATED WORK

The copy-move forgery detection is categories Block based and Key point based methods [9]. Mahale Vivek et al. [10] proposed image inconsistency detection using HOG. They did experiment on CoMoFoD dataset. They experiment on 100 and 200 images out of these they were taking 50%original and 50% forge images. They divide their dataset in to train and test and perform preprocessing. Then they apply HOG on both train and test set. Then they were performing matching process by calculating Euclidian Distance using threshold value for detect forge region. For evaluation they were calculating false accepted rate (FAR) and false reject rate (FRR). They conclude that from experiment First they were take 100 (50 original and 50 forge images) images. The system has got 0.63FAR and 0.37 FRR. In second case they were taking 200 (100 original and 100 forge images) the FAR and FRR are 0.77, 0.22 respectively. Amani Alahmadi et.al. [11] discus a novel passive method to detection of image forgery using DCT and local binary pattern. They have done pre-processing on dataset. Then for feature extraction they used LBP& DCT. They were dividing there dataset in training and testing set using SVM classifier. They perform their experiment on CASIA TIDEE V1.0, CASIA TIDEE V2.0

 DOI : 10.18231/2454-9150.2018.0687

and Columbia dataset. They were concluding that they got accuracy 97.5 on CASIA TIDEE V2.0, 97% on CASIA TIDEE V1.0, 97.77 on Columbia dataset. Vivek Mahale et.al [12] proposed a novel method to analysis image inconsistency using Local Binary Pattern (LBP). They propose algorithm to analysis automatically image inconsistency and identify forge region in image. In their work firstly read image from CoMoFoD dataset and then convert into gray scale. Then this grayscale image has divided into overlapping blocks. After that, they apply LBP on each block for feature extraction. This feature array would be shorting by lexicographical sorting algorithm. Then they were calculating Euclidian Distance using threshold value for matching process. Then dark the similar region detected by algorithm. They evaluated there method with calculating True Positive Rate (TPR) and False Positive Rate (FPR) with ROC curve. In this paper, they calculated that TPR and FPR for 2x2, 4x4, 8x8 and 16x16 blocks i.e. True Positive Rate are 0.0142, 0.0301, 0.0517 and 0.0800 respectively, while False Positive Rate for the same blocks are 0.0995, 0.0992, 0.0994, and 0.0997 respectively. Finally conclude that good results are coming on 2x2 block size. They also calculate accuracy i.e. 98.58 %. The some research related to HOG as mention in [15].

III. METHODOLOGY

The figure 2 below shows the propose system which is flow of our experiment work. The detail explanation of propose system is given below:

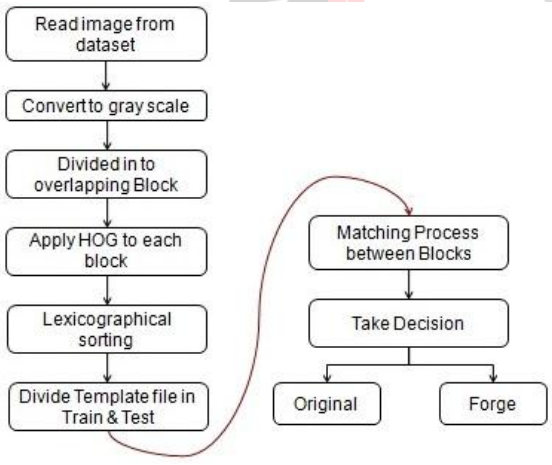

Figure 2: Proposed system

Algorithm1: Automatic Image Forgery detection using HOG

Input: Image for determination of inconsistencies check

Output: Either Original or Forge image

Begin:

Step 1: Read Image from dataset.

Step 2: Convert RGB Image in to Grayscale image and apply Gaussian filter.

Step 3: Divide image into overlapping blocks

Step 4: Compute HOG Features from each block

Step 5: Apply Lexicographical sorting and match similar pairs of blocks

Step 6: Calculate the Euclidean distance between two blocks

Step 7: Take decision using threshold value that image is original or forge

End.

A. *Preprocessing*

In preprocessing first read image and convert it into the grayscale image using formula given below:

$$I = 0.299R + 0.587G + 0.114B \quad (1)$$

Here, R, G and B mean red, green and blue respectively. Then divide image in 2x2 overlapping blocks. Then Initialized a Gaussian filter with sigma = 0.5 * Block Width.

B. *Feature extraction*

The feature extraction process takes the input from pre-processing. Then apply HOG on each block to find descriptor feature. Firstly, HOG was developed by Dalal et al. [13]. After got descriptor feature we sort it using Lexicographical sorting algorithm.

C. *Matching process*

The matching process incorporated block wise manner to determine whether block has Inconsistency, with the help of lexicographical sorting of feature fact. Similar feature are located in different blocks. The mechanism using for matching is Calculate Euclidean Distance between block by block feature vectors using threshold value. If image region was forging then dark it by red colour for highlighting forges area.

IV. RESULTS AND DISCUSSION

The proposed method is evaluated on database COMOFOD [14]. Dataset consist different post processed forgery and original images like BC (Brightness change), CA (contrast adjustments), CR (Color reduce), IB (Image blurring), JC (JPEG compression) and NA (Noise Adding). The database is taken from Video Communication Laboratory (VLC), University of Zagreb, Croatia, and Department of Wireless Communication. The proposed method was evaluated on laptop Intel Core i3, with 4GB Ram and Hardware infrastructure with MATLAB, necessary image processing toolbox. The figure 3 shows the some sample taken from COMOFOD database in to cases original and forge.

 DOI : 10.18231/2454-9150.2018.0687

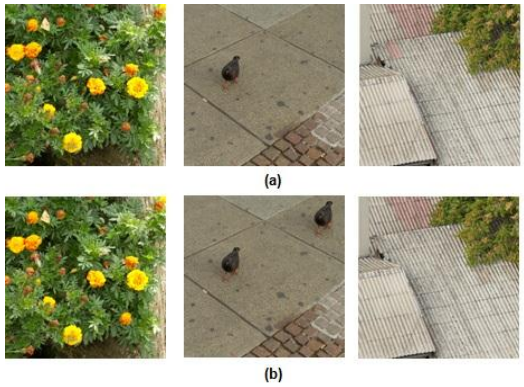

Figure 3 sample image taken from COMOFOD dataset (a) Original (b) Forge

First we perform pre-processing on image then extract the HOG feature and feature vector were sorted by using lexicography algorithm. Then perform matching process and identify forge region in the image. Figure below shows some example of forge image and to detect forge part.

Figure 4 Forge image with exact forge area detect and color that forge area

In the evaluation of our system, we take 6 images (3 original and 3 forge) from each category. There are 6 categories means in one test I take 36 images (18 original and 18 forge). Then I calculate TPR, FPR and Identification Rate. Table 1 show the analysis of image forgery detection with HOG method. Formula of TPR, FPR and Identification Rate is given below.

$$TPR = \frac{TP}{TP + FN}$$

$$FPR = \frac{FP}{FP + TN}$$

Identification Rate = (TP + TN) / (TP+FP+TN+FN) x 100

(4)

In our experiment I was taking 6 images from each class out of this 3 are originals and 3 are forges. Then I will execute algorithm on it then I calculate TP (true positive), FP (false positive), FN (false negative), and TN (true negative) values. From TP, FP, FN, and TN values I calculated TPR, FPR, and Identification Rate, which is shown in table 1.

As per our expriment we drow a ROC curve of identification rate for each sample in each class indivisiuly as shown in figure 5.

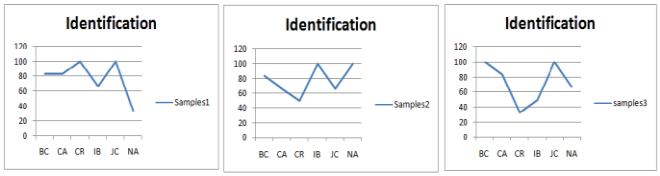

Figure 5: ROC curve of identification Rate of each class of three samples

V. Conclusion and Future Scope

In this paper was focused on image forgery detection using Histogram of Orientated Gradient method. The proposed system run on CoMoFoD data set. By used all categories of images for the experimental work for sample 1 the 36 images out of these 6 from each class forge and original. The identification rate reach to 100% in CR and JC category image, 83.33% in BC and CA category image, 66.66% in IB and 33.33% in NA category of images.In sample 2 also 36 images out of these 6 from each class forge and original. The identification rate was gave of 100% in IB and NA category image, 83.33% in BC category image, 66.66% in CA and JC, and50% in CR category of images. In sample 3 also the 36 images out of these 6 from each class forge and original. The identification rate was gave 100% in BC and JC category image, 83.33% in CA category image, 66.66% in NA, 50% in IB, and 33.33% CR category of images.The future of this work may be extending to compare with other techniques which improve the performance of our work.

References

[1] Cheddad, A., Condell, J., Curran, K., &McKevitt, P. (2010). Digital image steganography: Survey and analysis of current methods. Signal processing, 90(3), 727-752.

[2] Rey, C., &Dugelay, J. L. (2002). A survey of watermarking algorithms for image authentication. EURASIP Journal on Advances in Signal Processing, 2002(6), 218932.

[3] Yeung, Minerva M., Digital watermarking: marking the valuable while probing the invisible. Communications of the ACM ; 41(7): 31-35 (1998).

[4] Yeung, M. M. (1998). Digital watermarking: marking the valuable while probing the invisible. Communications of the ACM, 41(7), 31-35.

[5] Mahdian, B., &Saic, S. (2008). Blind authentication using periodic properties of interpolation. IEEE

 DOI : 10.18231/2454-9150.2018.0687

Transactions on Information Forensics and Security, 3(3), 529-538.

[6] Zhang, Z., Ren, Y., Ping, X. J., He, Z. Y., & Zhang, S. Z. (2008, July). A survey on passive-blind image forgery by doctor method detection. In Machine Learning and Cybernetics, 2008 International Conference on (Vol. 6, pp. 3463-3467). IEEE.

[7] Birajdar, G. K., &Mankar, V. H. (2013). Digital image forgery detection using passive techniques: A survey. Digital Investigation, 10(3), 226-245.

[8] Mushtaq, S., & Mir, A. H. (2014). Digital image forgeries and passive image authentication techniques: A survey. International Journal of Advanced Science and Technology, 73, 15-32.

[9] Lee, Jen-Chun, Chien-Ping Chang, and Wei-Kuei Chen. "Detection of copy–move image forgery using histogram of orientated gradients." Information Sciences vol.32,no.1 , pp.250-262, (2015).

[10] MahaleVivek, PravinYannawar, and Ashok T. Gaikwad. "Image inconsistency detection using histogram of orientated gradient (HOG)." In Intelligent Systems and Information Management (ICISIM), 2017 1st International Conference on, pp. 22-25. IEEE, 2017.

[11] M. H. Alkawaz, G. Sulong, T. saba, A Rehman, " Detection of Copy – Move image Forgery based on discrete cosine transform," neural comput& application, Springer, 2016

[12] Mahale, V. H., Ali, M. M., Yannawar, P. L., &Gaikwad, A. T. (2017). Image Inconsistency Detection Using Local Binary Pattern (LBP). Procedia Computer Science, 115, 501-508.

[13] Dalal, Navneet, and Bill Triggs. "Histograms of oriented gradients for human detection." In Computer Vision and Pattern Recognition, 2005. CVPR 2005. IEEE Computer Society Conference on, vol. 1, pp. 886-893. IEEE, 2005.

[14] CoMoFoD database, available at: http://www.vcl.fer.hr/comofod.

[15] Ashok T. Gaikwad ,Palmprint Identification System Based On Histogram Of Oriented Gradient (Hog) ,Global Journal Of Engineering Science And Researches, 5(7) pp: 482-490.,): July 2018, DOI: 10.5281/zenodo.1323534

Table 1: show the analysis of image forgery detection Based on HOG Method

Type	*Class name*	*Images in class*		*TP*	*FP*	*FN*	*TN*	*TPR*	*FPR*	*Identification Rate %*
		Original	*Forge*							
Sample1	***BC***	*3*	*3*	*2*	*1*	*0*	*3*	*1*	*0.25*	***83.3333333***
	CA	*3*	*3*	*3*	*0*	*1*	*2*	*0.7*	*0*	***83.3333333***
	CR	*3*	*3*	*3*	*0*	*0*	*3*	*1*	*0*	***100***
	IB	*3*	*3*	*1*	*2*	*0*	*3*	*1*	*0.4*	*66.6666667*
	JC	*3*	*3*	*3*	*0*	*0*	*3*	*1*	*0*	***100***
	NA	*3*	*3*	*2*	*1*	*3*	*0*	*0.4*	*1*	*33.3333333*
Sample2	***BC***	*3*	*3*	*3*	*0*	*1*	*2*	*0.75*	*0*	***83.3333333***
	CA	*3*	*3*	*1*	*2*	*0*	*3*	*1*	*0.4*	*66.6666667*
	CR	*3*	*3*	*2*	*1*	*2*	*1*	*0.5*	*0.5*	*50*
	IB	*3*	*3*	*3*	*0*	*0*	*3*	*1*	*0*	***100***
	JC	*3*	*3*	*1*	*2*	*0*	*3*	*1*	*0.4*	*66.6666667*
	NA	*3*	*3*	*3*	*0*	*0*	*3*	*1*	*0*	***100***
Sample3	***BC***	*3*	*3*	*3*	*0*	*0*	*3*	*1*	*0*	***100***
	CA	*3*	*3*	*2*	*1*	*0*	*3*	*1*	*0.25*	***83.3333333***
	CR	*3*	*3*	*2*	*1*	*3*	*0*	*0.4*	*1*	*33.3333333*
	IB	*3*	*3*	*1*	*2*	*1*	*2*	*0.5*	*0.5*	*50*
	JC	*3*	*3*	*3*	*0*	*0*	*3*	*1*	*0*	***100***
	NA	*3*	*3*	*1*	*2*	*0*	*3*	*1*	*0.4*	*66.6666667*

 DOI : 10.18231/2454-9150.2018.0687