International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 3, March 2016

Copy- Move Forgery Detection Using Passive Technique

[1]U. Neha, [2] K. Priyadharshini, [3]M.Priyanka, [4]K.Kiruthika
Kamaraj College of Engineering and Technology, Virdhunagar
[1]nehauttam100@gmail.com, [2]priyakarthikeyan1994@gmail.com, [3] priyankamurgan21@gmail.com,
[4]kiruthi.engg@gmail.com

***Abstract*— An extensive growth in digital technology has resulted in tampering of image. Image plays an important role in today's digital world. Powerful image editing tools has made it difficult to determine whether the image is authentic or forged. The main objective of this paper is to detect the forgery in which a part of the image is copied and pasted on to same image without the information of the original image. First, the forged image is segmented. With the help of SIFT features, key points are extracted. The matching process of these key points detects the copy move region.**

***Index Terms*—Copy- move forgery detection, image forensics, segmentation, SIFT features, tampering detection.**

I. INTRODUCTION

In today's digital world, use of images in our day to day live has increased tremendously. Digital images are one of the major means of communication. Every day millions and millions of images are uploaded on social networking sites. With the availability of powerful image editing software it becomes very important to verify the content of digital images before relying on them. With the advancement and easy availability of image editing tools like Photoshop, it becomes very easy to manipulate or tamper the digital images and create forgeries without leaving any visual clues, and such manipulations may change the whole semantics of the image.

Image forgery detection system is needed in many fields for protecting copyright and preventing forgery or alteration of images. Cyber Crimes in India are registered under two different acts, the IT Act and the Indian Penal Code (IPC)

Table I Number of cyber crime registered in India during the years 2011 to 2015

Year	No of Cyber crime registered
2011	13,301
2012	22,060
2013	71,780
2014	1,42,189(approx)
2015	3,00,000(approx

Fig.1. Example of Copy Move Attack on Image (truck in
this image is masked by some other region of same image)

The tampered image may totally convey different information than that of the original image. Therefore, digital images have lost their trust and it has become necessary to check the originality of content of the images when they are used in some critical situation like criminal investigation. Digital images found their applications in various fields like media, journalism, scientific publications, copyright and sometimes they are used as evidence in courts. Hence it becomes very important to verify that whether the image is real or fake. So, the Digital Image Forensics emerged as research field that aims to detect the forgery in digital images.

The passive image forensic method is used to detect one of the important tampering technique Copy-Move forgery that involves copying a part of an image and pasting on another part of the same image. Copy-Move forgery is done to hide some details or to duplicate objects within an image. Since the forgery is performed within a single image, therefore, the tampered region has almost similar properties as that of the original image which makes it very difficult to identify by the human eye.

Hence the copy move forgery detection method should be robust enough to identify the forged part. This paper involves 3 major stages. In first stage, input image is preprocessed and then segmented. Each segment is called as patches. In second stage, the features of the patches are extracted by key-point extraction. In third stage, key-point in a patch is matched with rest of the patches in the same image. This process is repeated until suspicious pairs are found. If no such pairs are found ,the image is 100 percent genuine.

The rest of the paper is organized as follows. Section II consists of the literature survey on existing system. Section III discuss about the proposed work. Section IV focus on results and observation. Section V discuss about the performance analysis followed by conclusion in section VI.

II. LITERATURE SURVEY

In this chapter, via surveying various other papers the need for the proposed method can be understood. This section deals with the overview of CMFD scheme, segmentation, feature extraction and keypoint matching.

A. CMFD Scheme

CMFD determines if an image has some regions containing identical contents and also locates those tampered regions. Using this scheme image can be determined into a set of local patches, like blocks or key points. Then the problem of CMFD is to compare these patches [1]. The block-based method is used to create a balance between performance and complexity.

The very first passive method for detection of copy move forgery is presented by Fridrich et al [3] that uses Discrete Cosine Transform (DCT) for the detection of copy move forgery. In [2] Popescu and Farid apply PCA on overlapping image blocks to yield a reduced dimension representation. This method suffers from the drawback that,

1. It cannot detect small duplicate regions

2. It needs a large amount of time to detect an image [1].

To overcome the limitations of block based methods the researchers use keypoint based methods: SIFT and SURF for detection of copy move forgery. Keypoint-based methods are faster and more favorable than the block-based ones, because the number of the image keypoints is smaller than that of the divided blocks.

To deal with this problem Amerini et al. proposed a method based on clustering the matched keypoints [6], using Scale Invariant Feature Transform (SIFT). In this method the SIFT features are extracted from the image which are then matched with each other to locate the forged duplicate regions in an image.

B. Image Segmentation

In order to separate the copying source region from the pasting target region, the image should be segmented into small patches, each of which is semantically independent to the others. Liu et al. proposed a forgery detection method using JPEG features and local noises discrepancies [9], where segmentation is proved to be useful to splicing detection. It is observed that the segmentation method does not greatly influence the CMFD's efficiency. Among them the methods in quick SIFT and SLIC are more favorable owing to their comparatively lower complexity In order that two CMF regions do not exist in the same patch,

C. Feature Extraction

Feature extracted in this paper is keypoint extraction and description. There are various kinds of keypoint detection and description methods.[11]

Huang et al. [12] proposed a method based on Scale Invariant Feature Transform (SIFT) algorithm for copy-move forgery detection. SIFT descriptors of an image are invariant to rotation, illumination and scaling. SIFT descriptors of the image are first extracted. Descriptors are then matched in order to detect similar patches in the image. Although the methods of keypoint detection and description are not rather important, note that the number of the keypoints should be larger than 2000 for good performance.

D. Key Point Matching

G2NN (Generalized 2 Nearest Neighbor) is used to match keypoints of the source region with that of target region. This method deals with the geometrical transformation. G2NN search for multiple copy paste detection. This method is robust to all transformation attacks.

III. PROPOSED METHOD

The proposed method has four steps as shown in fig 2 below.

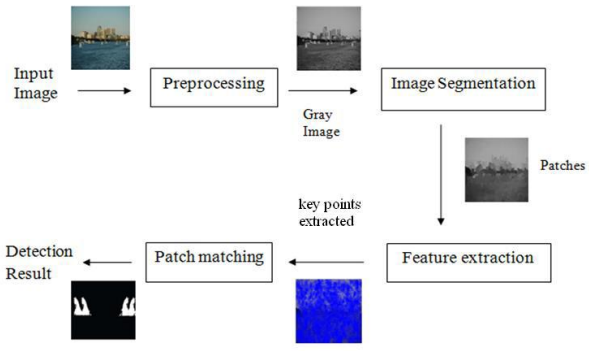


Fig 2. Overall system architecture of proposed system

A. Preprocessing

In preprocessing, input image is converted to gray scale image. rgb2gray() converts the true color image RGB to the grayscale intensity image. The rgb2gray function converts RGB images to grayscale by eliminating the hue and saturation information while retaining the luminance.

B. Image Segmentation

In order to separate the copying source image from the pasting target region, the image should be segmented into small patches, each of which is semantically independent to the others. The goal of segmentation is to simplify the image and make it easier for analysis. Each segments is called as patches. Each image is empirically segmented into no less than 200 patches and thus a copy move forgery region may be in two or more patches. So there are more than one chance to find the tampering operation. In this paper quickseg is used for segmentation. vl_quickseg is a wrapper function from vl_feat tool kit which takes care of the transformation of the image to LAB and performs segmentation and makes the job easier.

This function has four parameters whose values are ratio as 0.7 ,kernelsize as 1 and maxdist as 15 and the input image. Here ratio is the tradeoff between color importance and spatial importance (larger values give more importance to color), kernelsize is the size of the kernel used to estimate the density, and maxdist is the maximum distance between points in the feature space that may be linked if the density is increased

C. Feature Extraction

Feature extraction is done to collect relevant information from the input image to do the desired task instead of doing it with initial large data..

SIFT (Scale Invariant Feature Transform) is an algorithm to detect and describe the local features in images and SIFT features are robust to scaling, rotation and affine transformations that are well- suited for the detection of copy- move forgeries. The number of key points should be larger than 2000 for better performance. The SIFT detector is controlled mainly by two parameters: the peak threshold and the (non) edge threshold.

This approach uses vl_sift from vl_feat tool kit. The parameter to this function is single precision segmented image.

D. Key Point Matching

Matching among SIFT features is adopted to detect if an image has been tampered with and, subsequently, localize such forgery. This process is performed by comparing each patch with the rest. Key point matching is iterated until similar features are found between patches. If more number of matching pairs occurs between any two image patches. Then they are considered to be suspicious pairs. Else the image is genuine. This process is iterated until suspicious pairs are found.G2NN (Generalized 2 Nearest Neighbor) is used to match keypoints of the source region with that of target region. This method is robust to all transformation attacks.

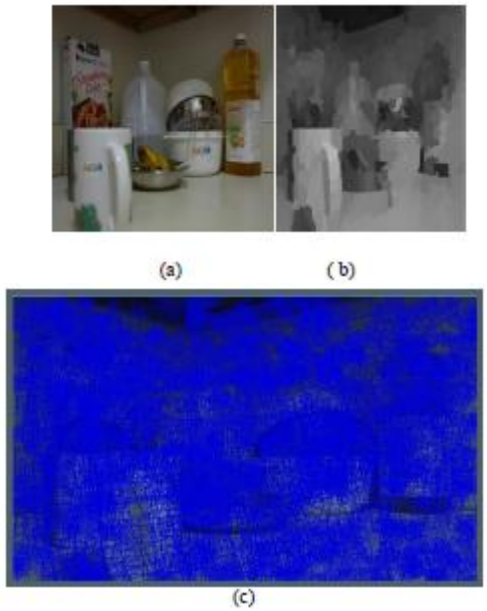
The keypoints extracted by SIFT are matched based on their feature vectors. It is used for detecting the match between two key points. For checking the key-points match, the ratio of Euclidian distance of the closest neighbor to that of second closest one is calculated and is compared with threshold (T). The keypoint is said to be matched only if the ratio is less than T.

IV. EXPERIMENTAL RESULTS

Experimental results of the technique proposed in this paper can be understood clearly in the Fig.3. MICC-F220 dataset is used for experimentation of this paper. It contains of 220 image of which 110 are tampered images and 110 are genuine images. 220 images are tested and error rates are found.

A. TEST CASE 1: TAMPERED IMAGE

For the first test a tampered image is taken Fig.3.(a). This image is peprocessed and then segmented as shown in Fig3.(b).into several patches. Then SIFT features are extracted as shown in Fig.3.(c).Features match points the region of forgery.

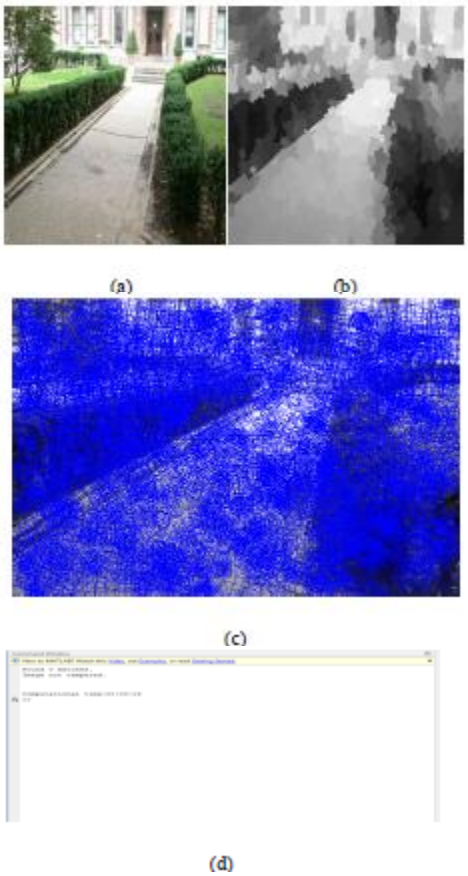


(d)

(e)

Fig.3.Experimental result for test case 1 (a) Input image (b) Segmented image (c) Feature extracted image (d) Suspicious pair (e) Detected result B. TEST CASE 2: ORIGINAL IMAGE

In test case 2 a genuine image is tested Fig.4.(a). Same procedure as of done for test case 1 is repeated. While no keypoints matched for this image showing its originality.



(a) (b)

(c)

(d)

Fig.4.Experimental result for test case 2 (a) Input image (b) Segmented image (c) Feature extracted image (d) Detected result Similar 218 other images were tested and studied for this paper. The detected result Fig.4.(d). shows that no points match in the image and the image is not tampered.

V. PERFORMANCE ANALYSIS

A manual observation of this approach shows the performance measure of this technique. It shows the error rate in detection. Following table II shows the false negative ratio (FN) in which it calculates ratio of the missing detected to the forged images and false positive ratio (FP) in which it calculated ratio of the false alarm to the original images. These results confirm the efficiency of this algorithm in detecting forged image However there is a need to improve the better accuracy in detecting the original image for which a threshold of 4 keypoint detection is set.

Table II Performance analysis with 220 images

Image type	**No of images in dataset**	**Correct detection**	**Wrong detection**	**Error rate**
Tampered	110	110	0	O
Original	110	72	28	0.3454

Error measures are found using following formula,
FN = |{Forged images detected as original}|
|{Forged images}|
FP = |{Original images detected as forged}|
|{Original images}|

VI. CONCLUSION

This paper mainly focuses on detecting copy-move forgery using keypoint extracted. This paper propose to segment the image to simplify the complex operations and matching is performed between these patches using the extracted keypoints. This paper also shows not only matching between patches but also detection result along with compilation time. In future work refinement process can be included to increase the accuracy.

REFERENCES

[1] Jian Li, Xiaolong Li, Bin Yang, and Xingming Sun, " Segmentation-Based Image Copy-Move Forgery Detection Scheme," in IEEE Trans on information forensics and security, vol. 10, no. 3, march 2015.

[2] Popescu A, Farid H. Exposing digital forgeries by detecting duplicated image regions. Technical Report

TR2004-515. Department of Computer Science, Dartmouth College; 2004.

[3] Fridrich, A. Jessica, B. David Soukal, and A. Jan Lukáš. "Detection of copy-move forgery in digital images." in Proceedings of Digital Forensic Research Workshop. 2003.

[4] Saiqa Khan, ArunKulkarni, " obust Method for Detection of Copy-Move Forgery in Digital Images," International Conference on Signal and Image Processing, 2010.

[5] S. Bayram,H. Sencar, and N.Memon, "An efficient and robust method for detecting copy-move forgery," in Proc. IEEE Int. Conf. Acoustics,Speech, and Signal Processing, pp. 1053–1056, Apr. 2009.

[6] I. Amerini, L. Ballan, . Caldelli, A. D. Bimbo, and G. Serra, "A SIFT based forensic method for copy-move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[7] Xu Bo, Wang Junwen, Liu Guangjie and Dai Yuewei, "Image Copy-move Forgery Detection Based on SU F," International Conference on Multimedia Information Networking and Security,2010 .

[8] H. Farid, "Exposing digital forgeries in scientific images," in Proc. 8th Workshop Multimedia Secur. (MM&Sec), New York, NY, USA, 2006,pp. 29–36.

[9] B. Liu, C.-M. Pun, and X.-C. Yuan, "Digital image forgery detection using JPEG features and local noise discrepancies," Sci. World J., vol. 2014, pp. 1–12, Mar. 2014, Art. ID 230425.

[10] Ashraf A. Aly1, Safaai Bin Deris2, Nazar Zaki3," Research Review For Digital Image Segmentation Techniques," in International Journal of Computer Science & Information Technology (IJCSIT) Vol 3, No 5, Oct 2011

[11] Maja Rudinac, Boris Lenseigne, Pieter Jonker, "Keypoint extraction and selection for object recognition," in MVA2009 IAPR Conference on Machine Vision Applications, May 20-22, 2009, Yokohama, JAPAN

[12] Huang, Hailing, Weiqiang Guo, and Yu Zhang. "Detection of copy-move forgery in digital images using SIFT algorithm." Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on. Vol. 2. IEEE, 2008.

[13] H. Bay, T. Tuytelaars, L. van Gool, "SURF: Speeded Up Robust Features," Computer Vision and image understanding , Vol. 110,No. 3, pp. 346–359, 2008

[14] A Vedaldi and B. Fulkerson. (2008). VLFeat: An Open and Portable Library of Computer Vision Algorithms[online]. Available: http://www.vlfeat.org