COPY MOVE FORGERY DETECTION USING 2 STAGE MATCHING PROCESS

[1] Srilakshmi R*, [2] Elizabeth Rose Lalson*

Dept Of Computer Science and Engineering

ER&DCI-Institute of Technology,

C-DAC Campus,Trivandrum,Kerala.

[1]lakshmi.r0606@gmail.com

[2] elizarosylalson@gmail.com

***Abstract*— Digital images are easy to manage and modify due to availability of powerful image processing and editing software. Nowadays, it is possible to add or remove important features from an image without leaving any obvious traces of tampering. As digital cameras and video cameras are emerged, the need for authenticating digital images, validating their content also increases. Detection of malicious manipulation with digital images is the content of this project. In particular, the paper focus on detection of image forgery – the copy-move taken place in which a part of the image is copied and pasted in the same image with some malicious intention. Problem of detecting the copy-move forgery and describe an efficient and reliable detection method is also explained using matching process. The matching process consists of two stages. In the first stage, the suspicious pairs of patches are taken into considerations, and estimation is done using affine transform matrix. In the second stage, an Expectation-Maximization-based algorithm is designed to refine the estimated matrix and to confirm the existence of copy-move forger.**

Keywords — Scale Invariant, Feature Transform, Expectation Maximization algorithm.

1. INTRODUCTION

With the rapid diffusion of inexpensive and easy to use devices that enable the acquisition of visual data, almost everybody has today the possibility of recording, storing, and sharing a large amount of digital images. The availability of photo editing software tools in the market makes extremely simple to alter the content of the images, or to create new ones, so that the possibility of tampering and counterfeiting visual content is no more restricted to experts.

An image with copy-move forgery (CMF) contains at least a couple of regions whose contents are identical. CMF is performed by an attacker or a forger aiming either to cover the truth or to modify the visual effect of the image. Normal people might neglect this malicious operation when the forger deliberately hides the tampering trace. So this made the urgent need of an effective CMF detection method to automatically point out the duplicate regions in the image. And CMFD is becoming one of the most important and popular digital forensic techniques currently [3].

Copy move forgery is more or less alike to image splicing. In this type of image forgery technique, part of the image is copied and pasted at some other place in the same image. There are many types of copy move forgery as follows: 1) just Copy-move 2) Copy-move with reflection; 3) Copy-move with different scaling; and 4) Copy-move with rotation.

2. SCENARIO OF THE CMFD SYSTEM DESIGN

The initial process is to add the test image in which the forgery is to be found out. If forgery is detected, the output is obtained. The forgery procedure is carried based on two stages of matching process. At two stages different algorithms are implemented.

Given an original image, there exist two processing alternatives. CMFD methods are either keypoint-based method or block-based methods. Keypoint-based methods calculate their features on regions with high entropy, without

any image subdivision. Similar features within an image are afterwards matched. Both, keypoint- and block-based methods include further filtering for removing spurious matches [5]. An optional post processing step of the detected regions may also be performed, in order to group matches that jointly follow a transformation pattern.

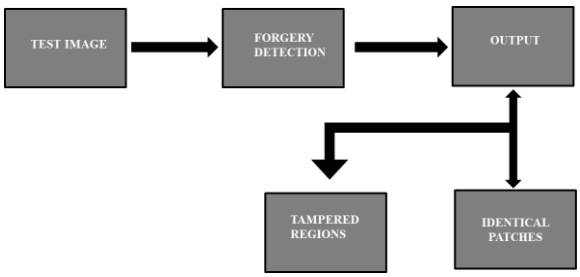

Fig 1 Block Diagram for Forgery detection scenario

3. EXISTING IMAGE FORGERY DETECTION TECHNIQUES

A large number of techniques have been proposed for detecting copy move forgery. Copy Move Forgery Detection method can either block based and keypoint based approach. Most of the time in block based method needs gray scale images so the RGB image is first converted into a gray-scale image. For feature extraction, this gray scale image is divided into non overlapping/overlapping block of same size. From each block, a unique representation as a feature vector is computed. And then detect the copy move forgery by looking for the similar blocks [18].

Fridrich et. al [2] first analyzed the exhaustive search and then suggested a block matching method to espy copy move forgery. This method was based on Discrete Cosine transformation (DCT). Lexicographic Sorting is done in this and the neighboring blocks are taken as the forged area. Thus these considered neighbor region are compared in the matching step .This technique in some complicated manipulation techniques like blurring or random noise addition it is not easy task to detect the forgery.

A method based on Discrete Wavelet Transform (DWT) and Kernel Principal Component Analysis (KPCA) is proposed by Bashar et al. [4]. In this method input image is splited into small overlapping blocks. Each block of input image is transformed by DWT or KPCA. DWT is applied on the image to minimize the size and obtained the low approximation coefficients. KPCA is used for feature collection and lexicographic sorting is used to cluster the alike feature blocks. This method is robust to manipulations such as translation-flip and translation-rotation of duplicate region

4. IMPORTANCE OF IMAGE SEGMENTATION AND TWO STAGE MATCHING PROCESS

Image segmentation is the process of partitioning a digital image into multiple sets of pixels, also known as super-pixels, refer figure 2. Image segmentation simplifies the representation of an image into something that is more meaningful and easier to analyze [18]. Image segmentation is typically used to locate objects and boundaries, lines, curves, etc. in images. Thus its the process of assigning a label to every pixel in an image such that pixels with the same label share certain characteristics.

Fig 2 Segmentation

In the first stage of matching process found that the suspicious pairs of patches as well as the transform matrix between them. Some of the detected patches may be just false alarm containing not any CMF regions. So introduce a second stage of matching process where the estimation of the transform matrix is refined via an EM-based algorithm and the false alarm patches might also be eliminated in this stage.

The second stage of matching process where the estimation of the transform matrix is refined via an EM-based algorithm and the false alarm patches might also be eliminated in this stage. Here searching new pixels for more accurate estimation. Then adaptive over segmentation can be carried out here. Adaptive over segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. Discrete wavelet transform is employed to analyze the frequency distribution of the host image. Compute the

adaptive block size and employ SLIC segmentation method to obtain the image blocks.

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 independent to the others. Segmentation can be carried out using Simple Linear Iterative Clustering (SLIC) method. SLIC adapts k means clustering but it is somewhat different from k means. Method used in this project generate superpixels which is faster than existing methods, more memory efficient, exhibits state-of-the-art boundary adherence, and improves the performance of segmentation algorithms.

5. IMPLEMENTATION AND RESULTS

A. Login

The login page is the first page through which the user gets access into the tool or application. The user can click login option and get into the next page. Once the user credentials are entered and verified, image can be added.

In this page, the user can click the browse option and add any files (forgered image) to the application. The image will be shown in the picture box. After clicking next, the respected histogram for the added image will be drawn.

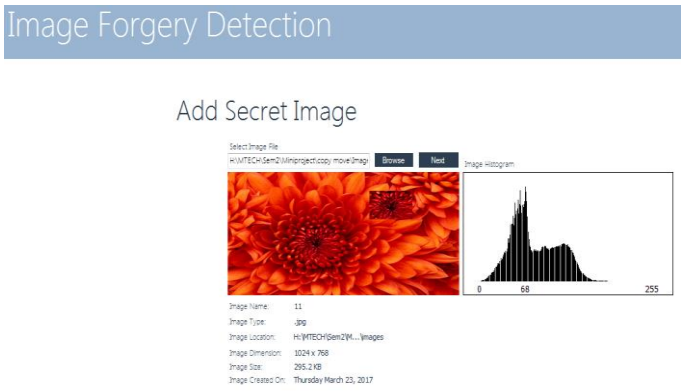

Fig 3 Image to be detected

B. Image Foreground Background Separation

The input image is further made into edge detection for separating the foreground and background. The purpose of edge detection is mainly to calculate the color component content in the input image. Pressing the edge detection button will produce the gray scale versions of the image with different strong and weak edges.

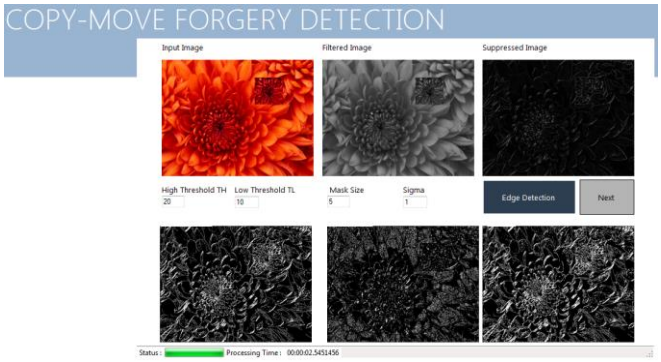

Fig 4 Edge Detection

C. Filtration

Copy move forgery detection requires the matching key points. Key point extraction is done as the 1st stage of process. In Key-Point based methods, input or test image is firstly divided into corner or isolated points to provide local features description of the image. The Key-Point algorithm for detecting of copy-move forgery starts by extracting high entropy regions i.e. Key-points. Feature descriptors are extracted from these features. These feature descriptor are compared with each other to detect the matched Key-Points and hence forgery detected. The Key-Point descriptors is SIFT (Scale Invariant Feature Transform) [13].

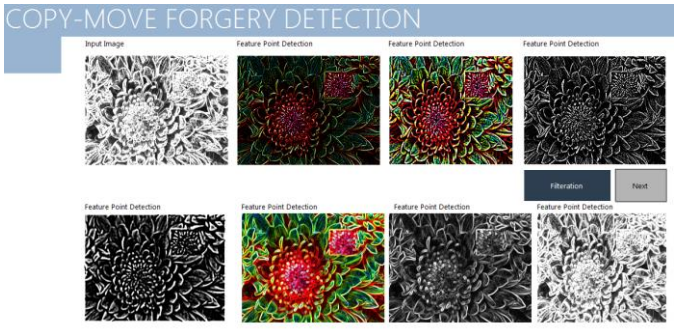

Fig 5 Filtration for key point extraction

D. SEGMENTATION, TRANSFORM ESTIMATION, GAUSSIAN TRANSFORM AND OVER SEGMENTATION

Proposed system exploits all the pixels in the matched patches to find out a more accurate estimation H. The pixels belonging to CMF regions, since the really matched pixels in the copying source region and pasting target region should be close to each other. Some correspondences are not accurate enough because they may be at the smooth image regions. One is the CMF region from the background is the same problem as classifying these two kinds of pixels.

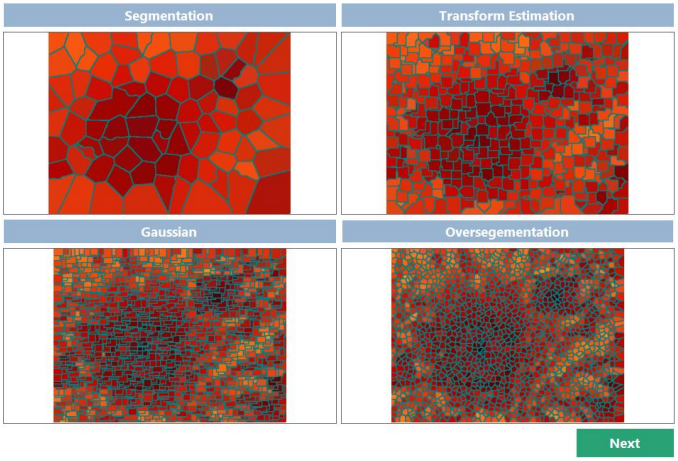

Fig 6 Over segmentation

E. Detection and Confirmation Phase

The entire process is repeated for all blocks. Identifies whether the image is forged or not by analyzing the pixel size variation. The similar regions are marked using black color lines. The detection is shown in figure 6 and the image used is shown in figure 7.

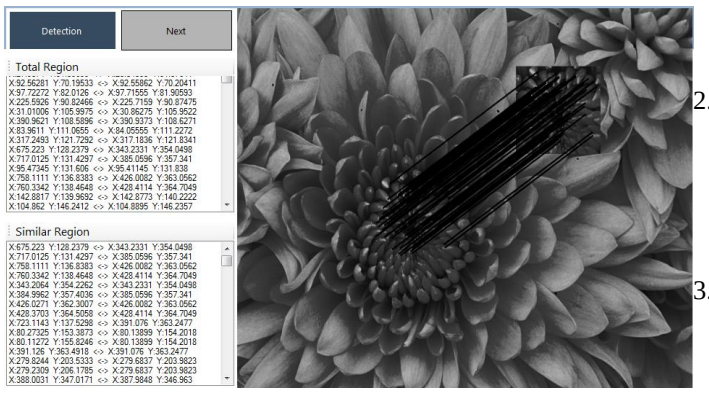

Fig 6 Forgery detected

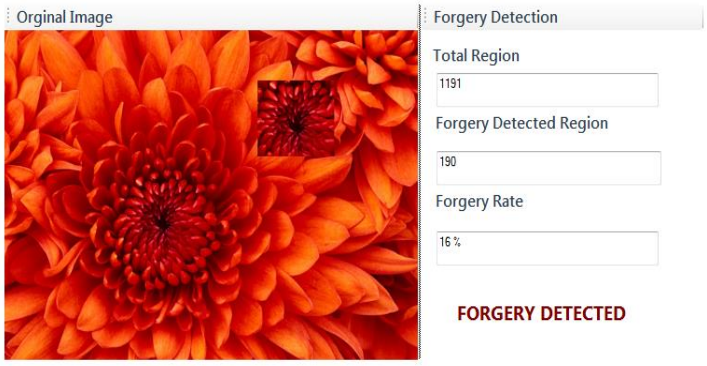

Fig 7: Foregery detection confirmation

6. CONCLUSION

The paper presented a CMFD scheme based on image segmentation. Although the CMF regions are detected mainly by comparing the keypoints extracted in the image, the implementation can be seen as a combination of both existing schemes because in the two stages of matching process both key points and pixel features are employed. For practical use, the most important aspect is the ability to distinguish tampered and original images. The power of an algorithm to correctly annotate the tampered region is also significant. In CMF detections, performance at two levels are also analyzed, at image level it focuses whether the fact that an image has been tampered or not and at pixel level evaluates how accurately can tampered regions be identified. The proposed scheme mainly contains two steps, namely the image segmentation and the transform estimation refinement.

REFERENCES

1. **Bayram, I. Avcibas, B. Sankur,** and **N. Memon**, "Image manipulation detection," J. Electron. Imaging, vol. 15, no. 4, p. 41102, 2006.
2. **Fridrich, A. Jessica, B. David Soukal, and A. Jan** Lukáš. 2003. ***"Detection of copy-move forgery in digital images".*** in Proceedings of Digital Forensic Research Workshop. 2003.
3. **Irene Amerini, Lamberto Ballan** and **Alberto Del Bimbo,** A SIFT-Based Forensic Method for Copy Move Attack Detection and Transformation Recovery.

4. **M. Bashar, K. Noda, N. Ohnishi and K. Mori** . 2010. **"**Exploring duplicated regions in natural images**"**.IEEE Trans Image Process, (2010), pp. 1–40.
5. **M. Ghorbani, M. Firouzmand,** and **A. Faraahi,** "DWT-DCT (QCD) based copy-move image forgery detection," in Proc. 18th Int. Conf. Syst., Signals Image Process. (IWSSIP), Jun. 2011, pp. 1–4.
6. **Pablo Arbel´aez**, Member, IEEE, **Michael Maire**, Member, IEEE, **Charless Fowlkes**, Member, IEEE, and **Jitendra Malik**, Fellow, IEEE, Contour Detection and Hierarchical Image Segmentation.
7. **Rameeza M Ashraf and Veena K Viswam,** a Fast Copy-Move Forgery Detection Scheme Using Patch - Based Descriptors.
8. **Vincent Christlein**, Student Member, IEEE**, Christian Riess**, Associate Member, IEEE, **Johannes Jordan**, Student Member, IEEE, **Corinna Riess**, and **Elli Angelopoulou**, Member, IEEE An Evaluation of Popular Copy-Move Forgery Detection Approaches.
9. **D. G. Lowe**, "Distinctive image features from scale-invariant keypoints," Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, Nov. 2004.
10. **H. Bay, A. Ess, T. Tuytelaars,** and **L. Van Gool,** "SURF: Speeded up robust features," Comput. Vis. Image Understand., vol. 110, no. 3, pp. 346–359, Jun. 2008.
11. https://en.wikipedia.org/wiki/Scale-invariant_feature_transform.
12. https://en.wikipedia.org/wiki/Image_segmentation
13. https://en.wikipedia.org/wiki/Image_segmentation#Edge_detection
14. **I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo,** and **G. Serra,** "SIFT-based forensic method for copy–move attack detection and transformation recovery," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.
15. **M. A. Fischler** and **R. C. Bolles**, "Random sample consensus: A paradigm for model fitting with applications to image analysis and automated cartography," Commun. ACM, vol. 24, no. 6, pp. 381–395, Jun. 1981
16. **P. Kakar and N. Sudha**, "Exposing postprocessed copy–paste forgeries, through transform-invariant features," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1018–1028, Jun. 2012.
17. **Q. Liu, G. Cooper, N. Linge, H. Takruri,** and **R. Sowden**, "DEHEMS: Creating a digital environment for large-scale energy management at homes," IEEE Trans. Consum. Electron, vol. 59, no. 1, pp. 62–69, Feb. 2013.
18. **R. Hartley** and **A. Zisserman**, Multiple View Geometry in Computer vision, 2nd ed. New York, NY, USA: Cambridge Univ. Press, 2004.
19. Segmentation-Based Image Copy-Move Forgery Detection Scheme **Jian Li, Xiaolong Li, Bin Yang, and Xingming Sun**, Senior Member, IEEE.
20. **Salam A.Thajeel, Ghazali Bin Sulong .**2013. "State of the art of copy-move forgery Detection Techniques: a review" .IJCSI Issues, Vol.10, Issue 6, No 2.