© 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Copy-Paste Forgery Detection in Digital Image Forensic

Anushree U. Tembe[1], Supriya S. Thombre[2]

Department of Computer Science & Engineering, YCCE, Nagpur, Maharashtra, India

ABSTRACT

The digital image forensic has increased nowadays new trends and creative ways to forged images. The software's are available that are used to manipulate the image so that the image looks like as original. In this paper the point-based approach used, in which relevant keypoints are extracted using Scale Invariant Feature Transforms. Interested points are extracted from the image, and extracted points are modelled as a set of connected triangles using Delaunay Triangulation Copy-paste image forgery where one portion of an image is replaced with the same image. Finally trying to show the efficiency and accuracy of this technique for detecting copy-paste forgery with translation, scaling, rotation, stretching.

Keywords: Image Forensic, Tamper Detection, Copy-Paste Forgery

I. INTRODUCTION

Digital image plays a very important role in different fields of technologies. Many image processing software available for altering or modify the image. With the use image manipulating software easily hide some meaningful or useful information to make forged images. The main aim of image forensics to address image integrity and authenticity. Image retouching, tampering, morphing, copy-move has been done to make forged images and lost the integrity of the image. These digitally forged images are difficult to recognize the image is original or not. Therefore, authenticity and integrity verification of digital image has been done for gain researcher attention in image processing fields.

The various types of tools widely used for manipulating or alter digital images such as Photoshop and Freehand etc. Therefore, verifying this developing technique in digital images became important especially when images are used for any law of the court, financial documents, and medical use, sector of transportation etc [2-4]. The digital image forgery detection techniques are proposed to deal with different tampering technique and determine the image trustworthiness and authenticity [5]. In recent times, many authors worked and analyzed the issues of determining image forgeries and presumption the tempered images and cannot detect any visual effect and anomalies, the essential information of tempering images compare with original images.

A. Applications of Digital Image Forensic

- Digital forensics is used widely for private investigation and criminal law.
- Forensic analysis the images on online social networks.
- Used to detect Forged or tampered image.
- Forgery detection system is needed in many fields for preventing Forgery and protecting copyright or alteration of images.

B. Classifications of Approaches

Digital image Forgery detection techniques are divided into active evidence approach and passive /blind approach.

1. **Active Approaches**: An active evidence detection method which consists of adding information at preprocessing stage such as digital signature, digital watermarking etc.
2. **Passive Approach***:* Passive/blind evidence method detects the duplicated objects in forged images without the need of real image watermarked or signature. The passive evidence is used to detect the location and the amount of forgery in the image.

There are two methods of passive approach. Image source identification -- It identify the device used for the data acquisition of the digital image. It used to detect digital camera image or computer generated image. In this method, the exact location of image forgery cannot be determined. Tampering detection -- It detects the intentionally manipulated image for malicious purposes. Tampering is denoted as image manipulation when it aims at modifying the content of the visual message.

The rest of the paper is organized as follows. In Section 2, literature survey is described. The proposed approach is provided in Section 3, and in section 4 experimental result are provided. The conclusion and future scope are drawn in section 5 and section 6.

II. LITERATURE SURVEY

In the last decade, passive evidence techniques copy-move forgery has been proposed. Fridrich [1] first presented a method to detect copy-move forgery of overlapping blocks using discrete cosine transform (DCT). Popescu [2] proposed a method used principal component analysis (PCA) for the represent image segments i.e. overlapping square blocks of discrete cosine transformation. Luo [4] presented a method for copy-move forgery localization and detection method based on an image is divided into small overlapping blocks, then compare the similarity between each block and finally trying to identify possible tampered regions using intensity based feature characteristics. The algorithm requires less computational time and is more robust against various types of attacks. A different approach was presented by Kang [6] introduced a method, singular value decomposition (SVD) for copy-move forgery detection of features representation. In this method used to correlate copy and paste areas and search for equal regions. Bayram [9] presented Fourier-Mellin transform (FMT) a method to detect copy-move forgery.FMT is applied to each block and then the values of FMT projected to one dimension to make the feature vector. Mahdian [6] introduced a method for copy-paste forgery detection based on blur moment invariants to find the tampered regions. Li [23] presented a method for forgery detection to extract the features of the circular blocks using the method of rotation invariant uniform local binary patterns Ardizzone [27] introduced copy-move forgery detection by matching triangles of Key-points, Detection methods use block-matching approaches or point-based approaches to find similar areas. In this method, it proposed the new triangulation method is used to detect the fraud. Ferreira [31] presented method multi-scale behaviour knowledge space (BKS) algorithm is to detect the fraud region based on probability condition.

III. PROPOSED SYSTEM

Following Fig.1. Shows the idea of proposed System. The idea behind our approach is simple: the objects are a represented as a set of connected triangles. In this proposed system first extract points of interest from an image, using SIFT detector. A Delaunay triangulation is built onto the extracted points. The image is subdivided into triangles, which contents pixels with very similar features. In this paper, we present methods that use this model to represent the objects: the method analyses the properties of the vertices that form the triangles, which are the interesting point of the image.

Here presenting some steps of proposed system for forgery detection is given below

An input image is applied there for forgery detection, the image can be any size N*M etc.

a. Preprocessing is apply over that, it improves the data of the image that remove noise distortions and enhance the image features, preprocessing is applied to enhance the certain feature of the image.

b. Feature Extraction, we extract some feature of the image using keypoint based approach. The scale invariant feature transform algorithm is used to extract an important feature from the image.

c. Delaunay Triangulation

In this stage, feature points are selected through Delaunay triangulation. Triangles built onto the extracted points. The image is therefore subdivided into triangles, which include pixels having similar features. Interested points are extracted from the image, and objects are modeled as a set of connected triangles built onto these points. The triangles are then matched according to the mean vector descriptors.

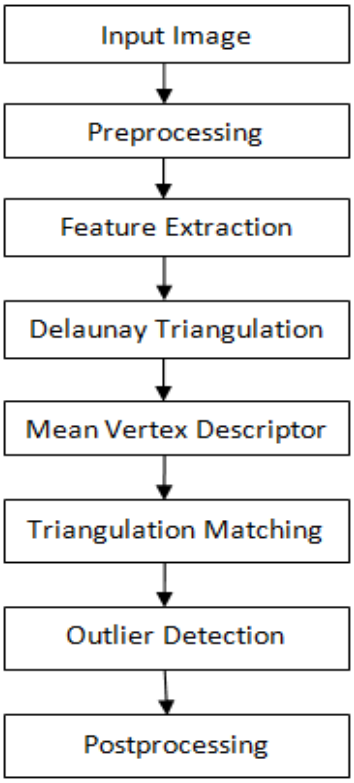

Figure 1. Proposed System

d. Triangles Matching by Mean Vertex Descriptors

For each triangle, find the Mean Vertex Descriptor as the average value of the feature vectors extracted onto the geometric vertices of the triangles.

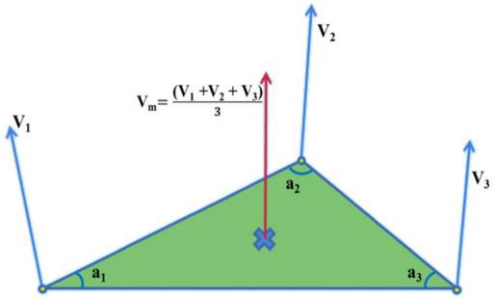

Fig. 2. The Delaunay Triangle of interest points. Each Triangle is represented by Inner Angles are (α1, α2, α3), Vector Descriptor are (V1, V2, V3) and Vector mean (Vm).

For each triangle, the Mean Vertex Descriptor Vmi is obtained as:

$$Vmi = (V1i + V2i + V3i)/3$$

Where Vj =1...3, i=1…N is the feature vector extracted onto the geometric vertices of the triangles and N is the number of the Delaunay Triangles inside of the image. The SIFT detector is used to extract the feature point of interest. If interested points are extracted by the scale invariant feature transform algorithm. To find duplicate regions, sort the triangles according to the L1 norm of their MVDs and the MVD of each triangle is compared to the next ones in the list, within a fixed window of size ws.

Also, in this case, a fixed window approach is preferable to an adaptive window one.

Two triangles match if the L1 distance of their corresponding MVD is lower than a threshold. If j and k (k>j) are the indexes of two triangles to be compared and Vmj, Vmk are the corresponding MVDs:

$$|Vmj - Vmk| \leq T\,Hv\,(k - j) < ws$$

Where THv is a threshold, ws is the fixed window size.

An RANSAC filter is used for outlier detection, to filter out false matches.

e. Post-processing: In this stage is used to reduce the probability of false matches for forgery detection

IV. EXPERIMENTAL RESULTS

Figure 2. Input Image

Figure 3. after apply pre-processing stage

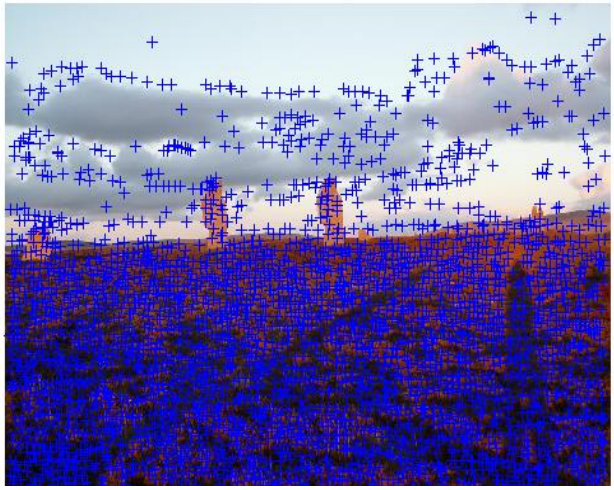

Figure 4. After apply SIFT feature detector

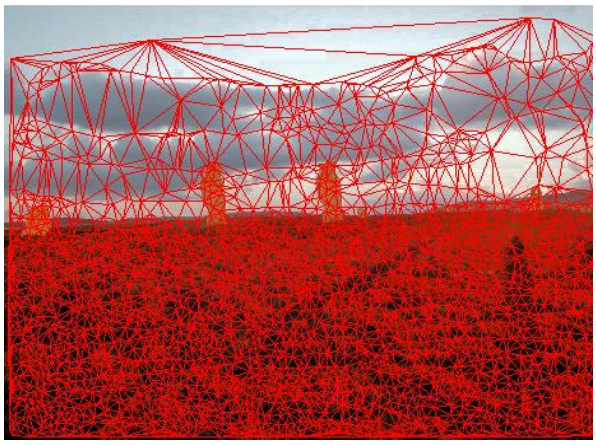

Figure 5. After Applying Delaunay Triangulation

After applying the triangulation matching using mean vertex descriptor 36 triangles are matched and after removing the outliers the total 18 are found.

Figure 6. Result after Forgery Detection

V. CONCLUSION

In the proposed method, SIFT keypoints based method used to analyze the structure of the objects in the scene represented as a mesh of triangles. This work is used as well for copy-move detection and recognition, as they are able to find the present copy-moved areas and to expose parts of them. It detects tampered areas of the images, also in the case of geometric transformations, but they are able to recover only parts of the pixels of the region, that are in most cases enough to detect the shape of the copied objects. On the other hand, our methods are two orders of magnitude faster than block based ones. In comparison with point-based ones, our methods have more or less the same performances, in terms of link precision, but have a lower number of false positives at the image level. This can be explained as we imposed tighter constraints with respect to the point based algorithm. In fact, we search for a structure that matches rather than single points.

Our methods perform better in the case of simple scenes, as the number of keypoints, and of triangles, are lower. In the case of complicated scenes the high number of triangles is detected, finally, the result shows worse performances. The keypoint based approaches, in proposed method, cannot be used if no interest points are detected. The proposed methods can be used in the future to find tampered copies also in the case of some other type of geometric transformations. In the post-processing stage, the techniques are used to recover some missing matches, e.g. filling the holes between triangles, and to increase the recall of the methods.

VI. FUTURE SCOPE

In future work, more tests will be performed on pictures with greater quantity of testing samples, with different scale invariant factor such as additive noise; scaling, stretching, blurring etc. forged part can be included or trying to detect the forgery where the multiple tampering is done. A comparison of different performance evaluation factors in image forgery detection can also be investigated in future work.

VII. REFERENCES

[1] J. Fridrich, D. Soukal and J. Lukas, "Detection of Copy-Move Forgery in Digital Images, *Digital Forensic Research Workshop, Cleveland*, pp. 19–23, 2003

[2] C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions", Tech. Rep. TR2004-515, Dartmouth College, 2004

[3] A. Popescu and H. Farid, "Exposing Digital Forgeries in Color Filter Array Interpolated Images," *in IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3948-3959, Oct. 2005

[4] W. Luo, J. Huang and G. Qiu, "Robust detection of region-duplication forgery in digital images", *in International Conference on Pattern Recognition*, vol. 4, (2006), 746–749

[5] G. Li, Q. Wu, D. Tu, and S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD," *in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing China*, pp. 1750-1753, July 2-5, 2007

[6] B. Mahdian and S. Saic, "Detection of copy-move forgery using a method based on blur moment invariants", *Forensic Sci. Int*., vol. 171, (2007) pp. 180–189

[7] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics", in Proceedings of *International Conference on Com-puter Science and Software Engineering*, (2008), pp. 926–930

[8] Z. Ting and W. Rang-Ding, "Copy move Forgery Detection Based on Svd in Digital Image," *in Proceedings of Image And Signal Processing, Cisp'09. 2nd International Congress On*, pp. 1-5, 2009

[9] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast And Robust Forensics for Image Region duplication Forgery," *in Proceedings of Acta Automatica Sinica*, Vol. 35, pp. 1488-1495, 2009

[10] S. Bayram, H. Taha Sencar and N. Memon, "An Efficient and Robust Method for Detecting Copy-Move Forgery," *in IEEE International Conference on Acoustics, Speech and Signal Processing*, Taipei, pp. 1053-1056, 2009

[11] S. Ryu, M. Lee and H. Lee, "Detection of Copy-Rotate-Move Forgery Using Zernike Moments," *in Proceedings of Information Hiding Springer Berlin Heidelber*g, pp. 1053-1056, 2009

[12] S. Khan and A. Kulkarni, "Robust Method For Detection Of Copy-Move Forgery In Digital Images," *in Proceedings of Signal and Image Processing (ICSIP), 2010 International Conference on*, Chennai, pp. 69-73, 2010

[13] L. Fitzpatrick and M. Dent, "Region Duplication Detection Using Image Feature Matching," *in IEEE Transactions On Information Forensics And Security*, vol. 5, no. 4, 2010

[14] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image Copy-Move Forgery Detection Based on Surf," *in Proceedings of Multimedia Information Networking and Security, International Conference On*, pp.889-892, 2010

[15] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, "An SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery," *in Proceedings of IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, Sept. 2011

[16] M. Sridevi, C. Mala, And S. Sandeep,"Copy–Move Image Forgery Detection In A Parallel Environment," *in Proceedings of Image And Signal Processing, Cisp'09. 2nd International Congress On*, 2012

[17] V *Christlein*, *C Riess*, *J Jordan*, *C Riess*, *E Angelopoulou*, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *in IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841-1854, Dec. 2012

[18] P. Kakar and N. Sudha, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features," *in Proceedings of Information Forensics And Security, IEEE Transactions On*, Vol. 7, Pp. 1018-1028, 2012

[19] *H. Shah, P. Shinde and J. Kukreja*, "*Retouching Detection and Steganalysis*", *IJEIR, Vol. 2, pp. 487-490, 2013*

[20] L. Zhong and W. Xu, "A Robust Image Copy-Move Forgery Detection Based On Mixed Moments", *in Proceedings of IEEE International Conference on Software Engineering and Service Sciences (ICSESS*), May 2013

[21] S. Thajeel and G. Sulong,"A Survey Of copy-Move Forgery Detection Techniques", *Journal of Theoretical and Applied Information Technology*, Vol.70, 10th December 2014

[22] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," *in IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, March 2015.

[23] C. Hsu, J. Lee, and W. Chen, "An efficient detection algorithm for copy-move forgery," *in Proceedings of Asia Joint Conference on Information Security* (AsiaJCIS), pp. 33–36, May 2015

[24] N. Joglekar, and P. Chatur, "A Compressive Survey on Active and Passive Methods for Image Forgery Detection," in *IEEE Transactions on Image Processing*, vol. 4, issue 1,2015

[25] H. Kaur and K. Kaur, "Image Forgery Detection using Steerable Pyramid Transform and Lab Color Space", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, August 2015

[26] E. Ardizzone, A. Bruno, and G. Mazzola,"Copy–move Forgery Detection By Matching Triangles Of Key-points," IEEE Transactions On Information Forensics And Security, Vol. 10, No. 10, Oct. 2015

[27] Chen-Ming Hsu, Chungli, Taiwan, Jen-Chun Lee and Wei-Kuei Chen, "An Efficient Detection Algorithm for Copy-Move Forgery" *in Proceedings of* 10th Asia Joint Conference on Information Security, pp 33-36, May 2015

[28] N. Nirmalkar and S. Kamble, "Illumination Color Classification Based Image Forgery Detection: A Review" *International Journal of Computer Science and Applications, 8*(1), 2015

[29] K. Asghar, Z. Habib & M. Hussain , "Copy-move and Splicing Image Forgery Detection and Localization Techniques: A Review," *in Proc.*Australian Journal of Forensic Sciences, Vol. 0(0), pp. 1-27, 2016

[30] A. Ferreira, S.C. Felipussi, C. Alfaro, P. Fonseca, And A. Rocha," Behavior Knowledge Space-based Fusion For Copy-move Forgery Detection," IEEE Transactions On Image Processing Vol. 25, No. 10, Oct. 2016