RESEARCH ARTICLE OPEN ACCESS

Advanced Digital Image Forgery Detection by Using SIFT

Priyanka G. Gomase, Nisha R. Wankhade
Department of Information Technology, Yeshwantrao Chavan College of Engineering an Autonomous Institution, Nagpur, India.
Email: priyankagomase@gmail.com
Email: nisha.wankhade@gmail.com

ABSTRACT
Due to the availability of powerful image processing software's, it is easy to manipulate or modify digital images. So that the image is look like as an original image. Therefore to judge the authenticity of given image is very difficult. Nowadays, it is possible to add or remove important features from an image without leaving any obvious traces of tampering. Digital photographs are used as evidence in law issues or to be circulated in mass media, so it is necessary to check the authenticity of the image. This paper, describes a digital image forgery detection method based on SIFT (Scale invariant feature transform). Copy-Move forgery is a specific type of image manipulation technique, in which part of an image itself is copied and pasted on different location within the same image. In this approach an improved algorithm based on scale invariant feature transform (SIFT) is used to detect such copy-move forgery. First apply SIFT to extract the keypoints and feature descriptor, and then feature matching based clustering is performed. After this estimate a geometric transformation for rotating and scaling between image regions.

***Keywords* -** Copy-move forgery, image forgery, image feature matching, scale invariant feature transform, tampering.

I. Introduction

In today's world it is easy to manipulate the digital image by adding or removing some elements from the image which results in a high number of image forgeries. With the increasing applications of digital imaging, different types of software are introduced for image processing.The availability of powerful digital image processing programs, such as Photoshop, makes it relatively easy to create digital forgeries from one or multiple images. Such software can do an alteration in digital image by changing blocks of an image with no showing the effect of the modification in the forged image. These modifications cannot be noticed by human eyes. Therefore verification of originality of images has become a challenging task. An image can be manipulated with a wide variety of manipulation techniques such as scaling, rotation, blurring, resampling, filtering, cropping, etc. The variety of applications such as military, forensic, media, scientific, glamour, etc. are uses digital images therefore the verification of originality of images is required. Image tampering is a digital art which needs understanding of image properties and good visual creativity. Detecting forgery in digital images is a rising research field with important implications for ensuring the credibility of digital images.

Copy-Move forgery is a very popular forgery in digital image forensics, in which a part of the image is copied and pasted into another part of the same image. This forgery is usually performed with the intention that to make an object "disappear" from the image by covering it with a segment copied from another part of the same image. The copied parts come from the same image therefore its noise component, and most other important properties will be compatible with the rest of the image and thus will not be detectable. As a result, it has become relatively easy to manipulate digital images and create forgeries that are difficult to distinguish from authentic photographs.

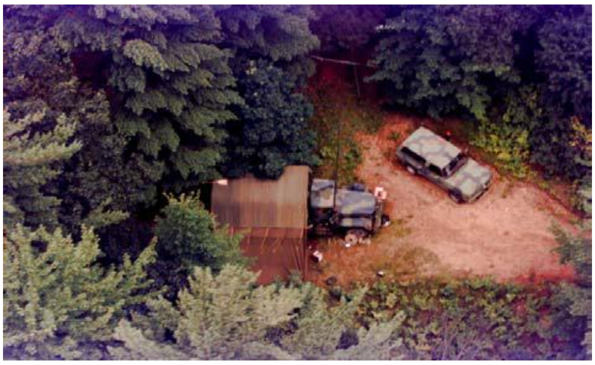

Fig. 1 forged image “jeep” (above) and its original version (below).

Above figure 1 shows the Copy-Move forgery. In Figure, you can see a less forgery in which a truck was covered with a portion of the leaf left of the truck.

II. Literature Review

There were several techniques proposed to detect image forgery in the literature of digital image forensics and all are giving their efforts for detecting such forgeries. The ways introduces to categorize the image tampering based on different points of view Firstly, the given image is divided into overlapping rectangular blocks except in where overlapping circular block are created. Secondly, to reduce the search area and to make the search unit as robust as possible to post processing like compression, Gaussian noise, scaling and rotation, some transformation technique is used like DCT, PCA, DWT, SVD, LLE etc. Thirdly feature vectors, after transformation are sorted lexicographically or using k-d tree. The neighboring vectors are compared against the similarity parameters to hint the duplication of region [1]. Since the key characteristics of Copy-Move forgery is that, copied part and the pasted part are in the same image, one method to detect this forgery is exhaustive search, but it is computationally complex, in which the image blocks are reduced in dimension by using Principal Component Analysis (PCA). But the detection algorithm was not more effective to detect forgery because, blocks are directly extracted from original image and that resulting in a large number of blocks [2]. The other technique which is DCT based copy-move forgery detection in single image [3], in which the image blocks are represented by quantized DCT coefficients, and a lexicographic sorting is performed to detect the duplicated image blocks. The author presents a literature based on sorted neighbourhood approach based on DWT [4] and SVD (Singular Value Decomposition).In this method the computation of SVD takes lot of time and it is computationally complex. Copy-move forgery detection method based on SURF [5], which detects duplication region with different size and it also shows that the proposed method can detect copy-move forgery with minimum false match for images with high resolution. To increase the speed of operation process many researchers use blocking approaches [6]. Among the techniques devised by the ‘Image Forensic’ community, those relying on scale invariant feature transform (SIFT) features are the most effective ones. The method is based on SIFT features allows both to understand which are the image points involved in the counterfeit attack and, to recover the parameters of the geometric transformation [7]. Generally, to adapt the image patch to the new context a geometric transformation is needed. To detect such modifications, a novel methodology based on Scale Invariant Features Transform (SIFT) is proposed [8], such a method allows both to understand if a copy-move attack has occurred and, furthermore, to recover the geometric transformation used to perform cloning.

The proposed methodology is based on the image SIFT features. We first detect keypoints in an image and compute the features for it. The next step is the image is divided into non-overlapping blocks. For each block, estimate a geometric transformation for rotating and scaling between image regions.

III. Proposed Methodology

The proposed methodology is based on the SIFT algorithm to extract robust features which can allows it to find if a part of an image was copy-moved and furthermore which geometrical transformation was applied.

1.1 Extracting keypoint and feature descriptor

The scale invariant feature transform is used to detect and describes local features in image. First detect SIFT key points in an image and compute the SIFT features for such key points. At each key point, a 128 dimensional feature vector is generated from the histograms of local gradients in its neighbourhood. It includes different steps are as follows:

1.1.1 Scale-space extrema detection: The first stage of computation searches over all scales and image locations, which is used to find the local extremas in scale-space. It searches over the scales and image locations. After searching locate the local extremas. A cascade filtering approach is used to get scale-spaced images for octave [9].

1.1.2 Keypoint localization: Keypoints are selected based on measures of their stability. Once a keypoint candidate has been found by comparing a pixel to its neighbors, the next step is to perform a detailed fit to the nearby data for location, scale, and ratio of principal curvatures. This information allows points to be rejected that have low contrast (and are therefore sensitive to noise) or are poorly localized along an edge [9].

1.1.3 Orientation assignment: At each keypoint location one or more orientations are assigned based on local image gradient directions. All future operations are performed on image data that has been transformed relative to the assigned orientation [9].

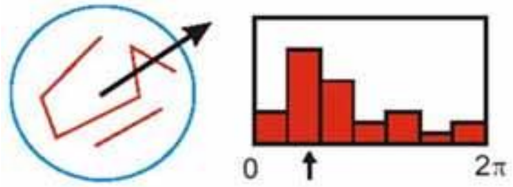

Fig. 2 orientation selection

1.1.4 Keypoint descriptor: The local image gradients are measured at selected scale in the region around each keypoint. These are transformed into a representation that allows for significant levels of local shape distortion and change in illumination [9].

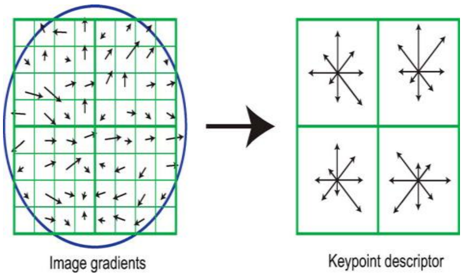

Fig. 3 image gradients and keypoint descriptor

1.2 Feature Matching based Clustering

To identify possible tampered areas, feature matching based approach is used. Clustering is performed on coordinates of the matched points. It creates a hierarchy of clusters which may be represented by a tree structure. The algorithm starts by assigning each keypoint to a cluster; then it computes all the cosine distances among clusters, finds the closest pair of clusters, and finally merges them into a single cluster. Such computation is iteratively repeated until a final merging situation is achieved. The way this final merging can be accomplished is basically conditioned both by the linkage method adopted and by the threshold used to stop cluster grouping.

1.3 Keypoint Matching

Which mainly concern with the matching of extracted feature keypoints from SIFT algorithm. In key point matching first reads the keypoint from given input image then, Compare the keypoints of images and if the keypoints matches then draw a line which indicating the matched keypoints, then append the two images and draw a line which indicate the matches.

1.4 Geometric transformation estimation

Translation, rotation and scaling transformation between an original area and its copied area can be determined using the set of extracted matched points. Let the matched point coordinates be, for the two areas, xi = (x, y, 1) T and xi" = (x", y", 1)T respectively, their geometric relationships can be defined by an affine homography which can be represent by a 3 × 3 matrix as

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = H \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$$

This matrix can be computed by at least three matched points. In particular, we determine H by using Maximum Likelihood estimation of the homography.

1.5 Detection Results

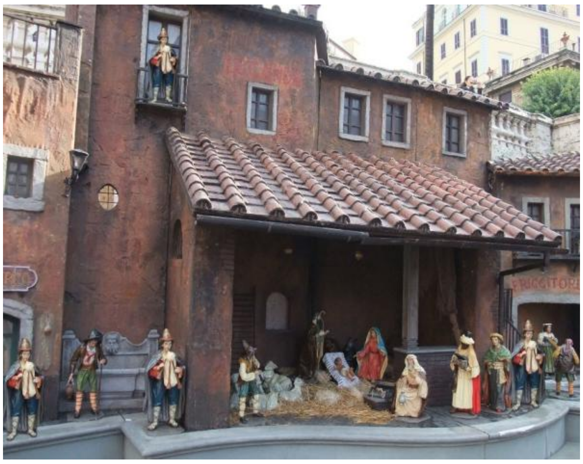

Fig. 4 test image

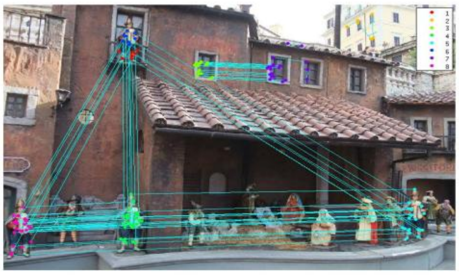

Fig.5 detection result

Fig. 6 library

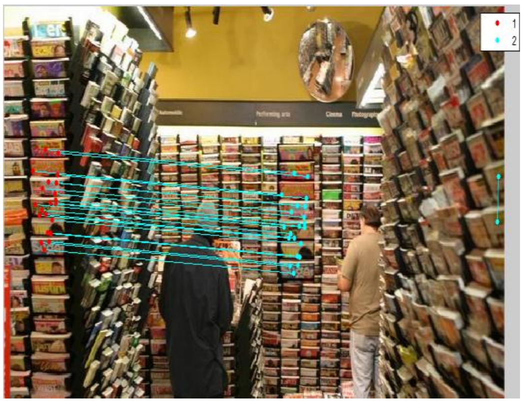

Fig. 7 detection result

Fig. 8 twin tower

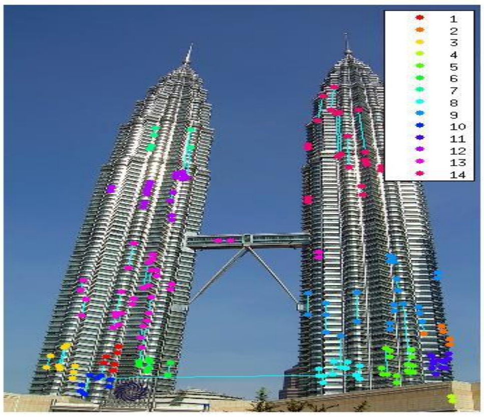

Fig.9 detection result

The natural duplication image input is given to the system then it gives the correct output that the image is not tampered.

IV. Conclusion

This paper introduces a new forgery detection technique which is able to detect a copy-move forgery in which a part of an image is copied and pasted into the another part of the same image by using SIFT based technique which detects keypoints and feature descriptor after that apply matching and clustering over all the key points and matching points for getting output with geometrical estimation.

V. Acknowledgements

I would like to thanks Head of the Department of Information Technology Yeshwantaro Chavan College of Engg., Nagpur and our HOD. Prof. R. C. Dharmik and I also extend my thanks to Dr. K. K. Bhoyar Professor Dept. of Information Technology YCCE Nagpur, for their valuable suggestions in making the final version of this manuscript.

References

[1] S. Kumar, P. K. Das, Shally, S. Mukherjee, “Copy-Move Forgery Detection in Digital Images: Progress and Challenges”, International Journal on Computer Science and Engineering (IJCSE) ISSN: 0975-3397 Vol. 3 No. 2 Feb 2011.

[2] A.C.Popescu and H.Farid, *“Exposing digital forgeries by detecting duplicated image regions”,* Dartmouth College, Hanover, New Hampshire, USA: TR2004-515, 2004.

[3] J. Fridrich, D. Soukal, and J. Lukas, “Detection of copymove forgery in digital images”,

Proceedings of the Digital Forensic Research Workshop. Cleveland OH, USA, 2003.

[4] G.Li, Q.Wu, D.Tu, and Shaojie Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD*", IEEE International Conference on Multimedia & Expo, 2007.*

[5] B.L.Shivakumar and Lt. Dr. S.Santhosh Baboo "Detection of Region Duplication Forgery in Digital Images Using SURF*", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.*

[6] Sarah A. Summers, Sarah C. Wahl, *"Multimedia SecurityandForensics.Authentication.of.Digital.images",*http://cs.uccs.edu/~cs525/studentproj/proj52006/sasummer/doc/cs525projsummer.sasummer/doc/cs525projsummersWahl.doc.

[7] I. Amerini, L. Ballan, R. Caldelli, A. D. Bimbo, and G. Serra, "Geometric tampering estimation by means of a SIFT based forensic analysis", *in Proc. IEEE ICASSP 2010.*

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

[9] S. Kudke, A.D. Gawande, "Copy-move attack forgery detection by using SIFT", *International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-5, April 2013.*