Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

An Efficient Approach for Detection of Digital Photo Forgery using Copy-Cover Techniques

Navpreet Kaur Gill
Assistant Professor
Deptt. Of CSE, Khalsa College
Mahilpur, India

Abstract—**With the high availability of image-editing softwares, authenticity of images is a major concern. This has led to the various forgery detection methods to check if a particular image is doctored or original. Copy-Move is a most difficult forgery to detect as the part which is pasted is taken from the same image. In this paper, a hybrid approach by combining the features of DCT (Discrete Cosine Transform) and SURF (Speeded Up Robust Features) has been proposed. This technique will show significant results against attacks performed by geometric transformations like rotation, scaling etc and is also robust to noise, blur and compression. Experimental results will prove that the proposed hybrid technique is better than Keypoint based methods in terms of reliability and block based methods.**

Keywords:- Copy-Move forgery, Digital forensics, DCT, SURF.

I. INTRODUCTION

With the swift development sophisticated image editing softwares, authenticity of images is a great challenge these days. To authenticate the images, there are two type of techniques: Active and Passive Techniques. Active Techniques are based on the fact that there must be prior information embedded in the image like digital watermarking and digital signature methods for forgery detection. On the contrary, there is no need of any prior information in case of passive techniques. These techniques are of five types such as Pixel based, Format based, Camera based, Physics based and Geometry based.

Among existing forgery techniques, Copy-Move is one of predominately used technique in which some part of a image is copied and pasted on some other part in the same image. In Cloning, part of the original image is copied and pasted to another location in the same image to conceal some responsive or significant information. As both the source and target part belongs to the image itself, properties like color, texture, noise, etc. remains the same. This correlation makes difficult to detect copy-move forgery with the human eyes because of local similarity of color and texture [1] .

Keypoint based and block based techniques can be used for detection of this kind of forgery. Block based techniques include DCT, PCA, DyWt, FMT and Zernike moments. Computational cost of block based methods will keep on increasing with the increasing image size.

Keypoint based methods are best alternative in this case because number of keypoints are less than the number of blocks and leads to lower computational cost. SURF (speed-up robust features) and SIFT (Scale Invariant Feature Transform) are two keypoint based methods for copy-move forgery detection. But keypoint based methods failed to work in flat regions. Hence a hybrid approach combining the features of both keypoint based and block based methods is a best choice. DCT is the block based technique which is combined with SURF for effective forgery detection in this paper.

DCT is chosen over the other block based image forgery detection techniques because of its reliability when combined with SURF. On the other hand, SURF is chosen over SIFT because of its speed and a hybrid approach combining features of these two is proposed.

II. GENERALIZED SCHEMA FOR FORGERY DETECTION

Copy-cover Forgery identification in pictures is two step method. The principle target of blind forgery detection technique stays to categorize a given picture as real or altered. We will depict a widely used schema of image forgery identification procedure, that comprises of the following steps:

1. Image Preprocessing: Image preprocessing is the initial pace. Some preprocessing is performed on the picture under deliberation like image filtering, image enrichment, trimming, change in DCT coefficients, RGB to grayscale transformation before handling the image to feature extraction procedures.

2. Feature Extraction: Selection of features for every class separates the image-set from different classes however in the meantime stays constant intended for a specific class chosen. The attractive element of the chosen set of features is to have a tiny measurement so that computational complexity can be diminished and have an extensive distinction with other classes.

3.Selection of Classifier: Depending upon the feature-set that is extracted in above step, suitable classifier is either chosen or composed. The large training sets will yield the improved performance of classifier.

4.Classification:-The only motive behind classification is to determine if the image is original or not. Neural systems ,LDA and SVM are classifiers used for this purpose.

5.Postprocessing:-Some forgeries will possibly require post processing that include manipulations like localization.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

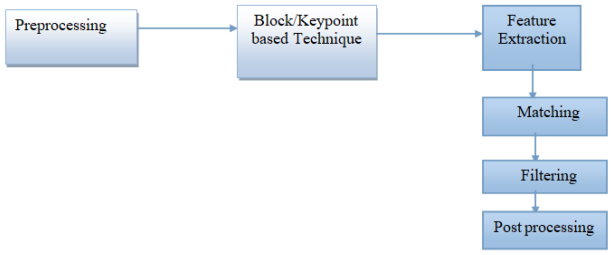

Fig. 1: Generalized Schema for Forgery Detection

III. RELATED WORK

Z. Ting et al. [66] described a for copy-move forgery detection by utilizing SVD. Firstly singular value SV features are extracted and further matching is performed k-d tree. This method has low computational complexity and is robust to post image processing.

Luo et al. [67] describes the technique of copy-move forgery detection based on intensities. Image is divided into overlapping blocks which are divided into two equal parts and four directions. Compute block characteristic vector for every block and further they are sorted using lexicographical sorted. Use shift vector method to find which part of image is duplicated. This algorithm works well with post-processing operations and has lower computational complexity. This method works well when the block size is smaller than forged regions but cannot work with the flat regions.

Lin et al. [68] proposed a new technique in which image is divided into fixed size blocks and further divide each block into four sub-blocks. Calculate intensity for every sub-block and obtain the features. As the feature vectors obtained are integer values, sort them using radix sort for determining the similar feature vectors. Further calculate the shift vectors so that false matches can be reduced. The blocks having highest value of shift vector are termed as forged blocks. This method shows robustness against JPEG compression and additive noise but is not applicable for rotation.

S. Ryu et al. [69] conducted a study on copy-move forgery detection by using Zernike moments. This methods works well for all type of geometric transformations like JPEG Compression, Gaussian noise, blurring and rotation upto 30 degree.

Z. Wang et al. [70] proposed a method by using Hu moments for forgery detection. Dimension will be reduced in this method by using Gaussian pyramid and the image is divided into overlapping blocks. Apply Hu moments to each block and calculate eigen values. Sort these vectors using lexicographical sorting and false detections can be reduced by selecting an area threshold. Mathematical morphological techniques are used for matching purpose.This method works well even when the post processing is performed on the image.

B. Mahdian et al. [71] utilizes blur moment invariants to represent forged image. Firstly tilt the image with blocks of particular size and represent them with blur invariants. Then apply the PCT (Principal Component Transformation) to reduce the dimensions of each feature vector. K-d tree is used for matching purpose. Further verify the similar blocks found b finding neighborhood of similar blocks. This method works well in case of duplicated regions with changed contrast and blurring. Disadvantage of this algorithm is that it has high computational complexity.

B. Ustubioglu et al. [72] presented the method which decreases the false negative rate. Firstly image is divided into the non-overlapping blocks. After that obtain the LBP values for every block and apply the DCT on every block. This method decreases the computational cost and gives the more accurate results than the existing DCT method.

J. Zheng et al. [73] presented a new method based on ORB (Oriented FAST and Rotated BRIEF) on the basis of visual descriptor BRIEF (Binary Robust Independent Elementary Features) and FAST (Features from Accelerated Segment Test) key-point detector. This method is the alternative for other keypoint based techniques like SIFT and SURF for the detection of duplicated regions. The advantage of this method is that its matching time is less than the other keypoint based techniques. Less storage space is required by this method and it can also handle all type of geometric transformations like scaling and rotation etc.

C. Haipeng et al. [74] proposed a method based on scale space and ORB (Oriented FAST and rotated BRIEF). Detection of forgery in high resolution images is very time-consuming with this method. But the main advantage of this method is that it lowers the false matches and can handle the different geometric transformations.

D. Lin et al. [75] proposed a technique which combines the features of Discrete cosine transform (DCT) with Speeded up Robust Features (SURF).This method will tells the exact position of the forgery and works well with the JPEG format. It can also detect forgery at multiple positions. This method does not work well in case of flat regions

G. Zhang et al. [76] proposed a technique which combines the features of Fourier Mellin Transform (FMT) with Speeded up Robust Features (SURF). Block based technique is used to determine the forgery in case of flat regions while keypoint based technique is used for forgery detection in non-flat regions.

IV. PROPOSED APPROACH

In the proposed approach, an image is firstly divided 8*8 blocks using block based technique named Discrete Cosine Transform (DCT). After that SURF is used to compute the keypoints from the whole image. After that we will divide the image regions into flat and Non-flat areas based on ratio between the keypoints and pixels. If there is more than two flat regions in the image, then DCT is used to detect forged areas in flat region. Post Processing is based on morphological operations like Region properties, area open technique and boundary filling etc. to locate the forged regions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

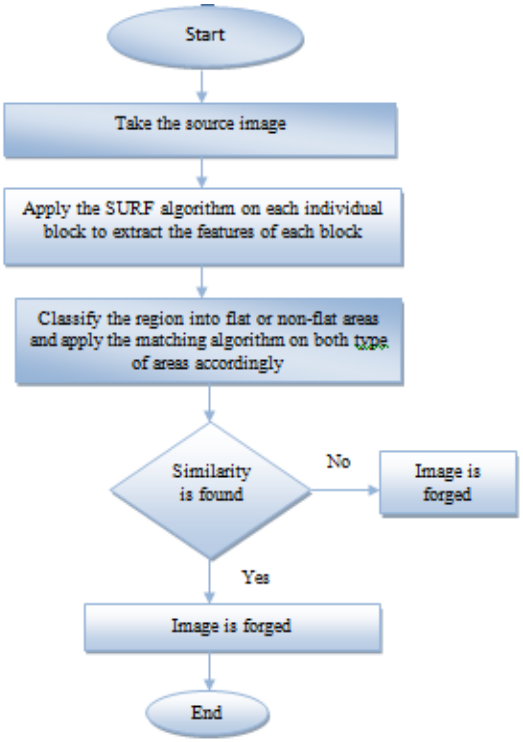

Fig. 2: Flowchart of Proposed Method

4.1 Preprocessing

Preprocessing has been performed for the enhancement of image and for conversion into binary form to increase the accuracy of results. Noise is also removed from the image to get the accurate results. Operations are also performed on the blurred images to get the proper content of the image.

4.2 Extract the Keypoints and classify the regions

Keypoints are extracted from the image with the help of SURF algorithm from the whole image. Keypoint extraction technique will fail in case of flat regions. Hence there is a need of division of areas into flat and non-flat region. Find the ratio between Keypoints and pixels for this purpose.

$$K = \frac{\text{Number of Keypoints,N}}{\text{Naumber of Pixels,Np}}$$

If the ratio is less than the threshold value, then that region is flat region and if the value is greater than threshold value, then the region is called Non-flat region.

4.3 Detection in Non-Flat Region

Detection of forgery in the non-flat region is done with the help of a know algorithm Speeded Up Robust (SURF) which is discussed below in the pseudo-code.

Pseudo code for tampering detection in Non-Flat Regions

Begin
Step 1. Firstly reduce the dimensions of the input image using DCT.
Step 2. Extract the keypoints with the help of Hessian Matrix Approximation.
Step 3. Match the features using g2NN strategy.
Step 4. Based on matching features, forgery decision is taken.
End

4.4 Detection in Flat Region

Detection process in the flat region is performed with the help of block based method named as DCT. Detection is performed in the four different steps which are discussed below in the pseudo code.

Pseudo code for tampering detection in Flat Regions

Begin
Step 1. Firstly count the number of flat regions. If there are more than two flat regions, then perform the below steps else move to the post-processing step directly.
Step 2. Divide the flat region into 8*8 non-overlapping blocks.
Step 3. Discrete Cosine Transform (DCT) is chosen as block based method because of its less computational complexity.
Step 4. Feature Vector Matrix is sorted with the help of lexicographical sorting and blocks are matched for forgery detection.
End

4.5 Post-processing

Post-processing to locate the duplicated regions is necessary due to the sparse nature of the keypoints. In this technique, Post-processing has been performed on the basis of morphological operations like area open technique, Filling, Boundary and region properties. After that all the forged regions which are extracted by keypoint as well as block based technique are combined.

V. RESULTS AND DISCUSSION

The following metrics are used to analyze the performance of the algorithm :

1. Precision: Probability that a detected forgery is truly a forgery, computed as:

$$P = \frac{Tp}{Tp+Fp}$$

2. Recall: Probability that a forged image is detected, computed as:

$$R = \frac{Tp}{Tp+Fn}$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

This is also called True Positive Rate.

3. This combines both Precision and Recall in a single value. It is computed as:

$$F = 2 * \frac{P*R}{(P+R)}$$

Sr.No.	Precision	Recall	F-measure	Accuracy
1.	0.985	2.56	0.032	97.43
2.	0.983	1.94	0.034	98.13
3.	0.984	2.56	0.033	97.61
4.	0.983	2.51	0.034	97.83
5.	0.981	1.89	0.029	98.12

Table 4.1 Results of Proposed Work

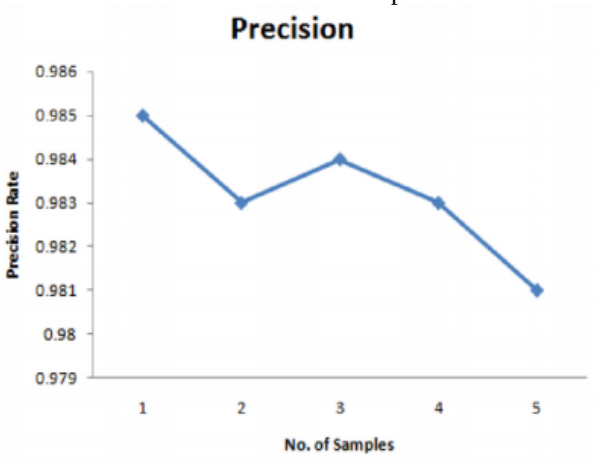

Fig 3: Precision of Proposed Method

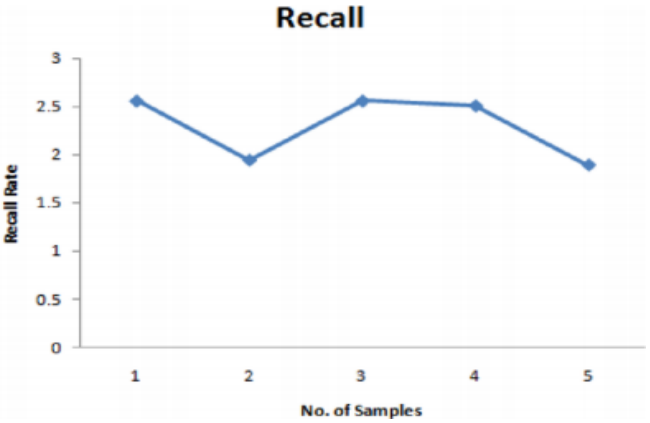

Fig 4: Recall of Proposed Method

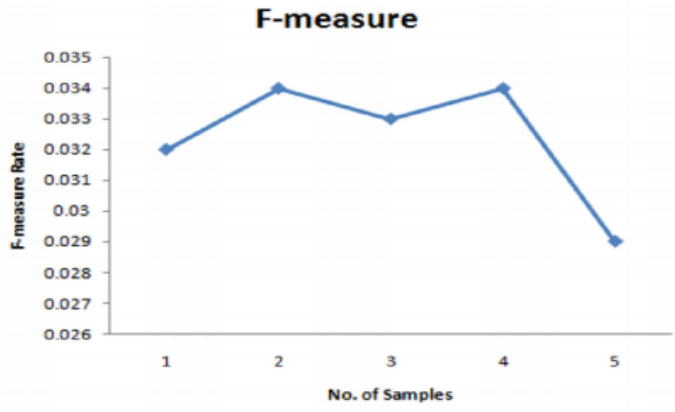

Fig 5: F-Measure of Proposed Method

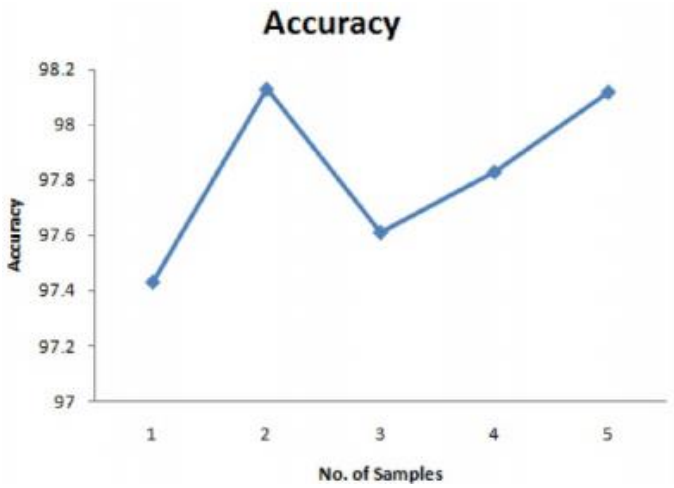

Fig 6: Accuracy of Proposed Method

VI. CONCLUSION

Copy-Move Forgery detection techniques still suffer from large number of issues and till now there is no unified algorithm which can detect every type of forgery. As a result of it, a hybrid approach has been implemented to resolve some of the issues. The implemented method shows robustness against geometric transformations and the proposed method shows robustness against geometric transformations and the proposed technique shows improvement in results in terms of Precision, Accuracy and FPR as compared to existing techniques.

The prime drawback of the existing methods is Automation that is the answers can be interpreted with the intervention of human only. Second drawback is that if we talk about copy-move forgery, then the use of these methods is computationally expensive .Thirdly as these techniques are applied to images only, we can extend the research on audios and videos. Fourthly at present there is no technique which can identify between the malicious forgery and just the retouching like artistic manipulation. The most challenging tasks is to develop a unified algorithm having capacity to detect any type of forgery.

REFERENCES

[1] M. K. Johnson and H. Farid, "Exposing Digital Forgeries by Detecting Duplicated Image Regions", *ACM Multimedia and Security Workshop*, New York, NY, 2005.

[2] Zhang Ting, Wang Rang-ding, "Copy-Move Forgery Detection based on SVD in Digital Image", Eighth conference on Image and Signal Processing ,Oct. 2009.

[3] W. Luo, J. Huang, G. Qiu," A Novel Method for Block Size Forensics Based on Morphological Operations", International Workshop on Digital Watermarking , pp 229-239, 2016.

[4] Z. C. Lin, R. R. Wang,"Detecting doctored images using camera response normality and consistency", IEEE Computer Society Conference on Computer Vision and Pattern Recognition,pp 1087–1092,2010

[5] S. Ryu, M. Lee, H. Lee, "Detection of copy-rotate-move forgery using zernike moments," in Proc. International Workshop Information Hiding, Springer , pp. 51–65, 2010.

[6] Z.Wang," A passive image authentication scheme for detecting region-duplication forgery with rotation",Journal of Network and Computer Applications, Vol. 34 , Sep.2011, pp. 1557-1565.

[7] B.Mahdian , S. Saic," Detection of copy–move forgery using a method based on blur moment invariants", Forensic Science International, an international journal dedicated to the applications

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

of medicine and science in the administration of justice, Vol.171 ,pp. 181-189,2007.

[8] B.Ustubioglu, G.Ulutas, M.Ulutas, V.Nabiyev and A.Ustubioglu, "LBP-DCT Based Copy Move Forgery Detection Algorithm," Springer International Publishing Switzerland, pp. 127-136, 2016.

[9] J. Zheng and L. Chang, "Detection of Region-duplication Forgery in Image Based on KeyPoints Binary Descriptors", Journal of Information & Computational Science, vol. 11, pp. 3959-3966, 2014.

[10] Z.Ye, S.Xuanjing and C.Haipeng, "Copy-Move Forgery Detection Based on Scaled ORB", Proceedings of Multimedia Tools and Applications, vol. 75, pp. 1-13, 2015.

[11] D. Lin and W.Tszan, "An Integrated Technique for Splicing and Copy-move Forgery Image Detection", 4th International Conference on Image and Signal Processing (CISP), pp. 1086 – 1090, 2011.

[12] G.Zhang and W. Hang, "SURF based Detection of Copy-Move Forgery in Flat Region", International Journal of Advancements in Computing Technology (IJACT), vol. 4, 2012.