

# Copy Move Image Forgery Detection Using SURF Feature Point Extraction

Jaseela S

M.Tech student

Department of Computer Science and Engineering  
Mohandas College of Engineering  
Anad, Trivandrum

Mrs.Nishadha S. G.

Asst.Professor

Department of Computer Science and Engineering  
Mohandas College of Engineering  
Anad, Trivandrum

**Abstract**— The talk about image forgery is very common in the digital image forensic area. But with advanced image editing tools exposure of tampered part from the original image is hard. Human cannot visually identify the fabricated region from the Image. So, it is imperative to advance a technique which can detect the forged image from the original one. Copy-move/paste image forgery is a frequent category of image forgery, in which the precise part of image is copied and pasted in the same image to hide some important or useful information.

**Keywords**— Image Forgery, Segmentation, key-points

## I. INTRODUCTION

Impressive and readily accessible photo editing tools such as Photoshop and Freehand made manipulating and tampering of digital images are successful. Because of this, there is a swift increase of the image forgery in virtual and social media. This trend leads to severe vulnerabilities and loss of credibility in the digital images. As things go the social security detection of image forgery is essential. In this sense, image tampering detection is the central attraction of digital image forensics. An example for image forgery is shown in Fig.1.

Copy-move image forgery is an important area of image forgery; in this a precise apart is copied and pasted on the region of same image to hide some crucial information. During the these types of forgeries, digital image pre-processing techniques such as scaling, rotation, blurring, noise and compression, are applied to make satisfying forgeries. An example for this type of forgery can be seen in Fig.2.

Because of the ease of use copy move image forgery is very common. Recently, many authors studied the main problem of detecting these forgeries, considering the nature of region-duplication; there are at least two similar regions in a forged image. According to the existing methods, there are two copy-move image forgery detection methods block-based algorithms [1],[2], and feature keypoint extraction[3],[4],[5],[6] based algorithms.

In block-based methods, the image is divided into overlapping/non-overlapping blocks and feature vector is

computed for each blocks. Similar feature points are selected and matched to find forged regions.

In key-point based methods, keypoints are selected and according to feature vector similar key points are selected . The image is not divided into blocks, the feature vectors are matched to find forged regions.



Fig..1. Digital image forgery in news paper



**Fig. 2 :** Example of copy move image forgery

Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi [7] proposed a copy move image forgery detection technique as a combination of basic block based approach and key point based approach. This method mainly introduces two new techniques, adaptive over segmentation and feature-point matching algorithms. The adaptive over segmentation is similar to block-based detection methods, in which to divide the host image into non-overlapping and irregular blocks adaptively to the host image texture. Then, similar to the keypoint-based technique in feature-point matching, the feature points are extracted from each image block as block features.

As this is a new approach to the area of copy move image forgery, it had met many of the existing forgery problems. So I took this as my base paper.

## II. BASEPAPER

The existing block-based algorithms have three main drawbacks:

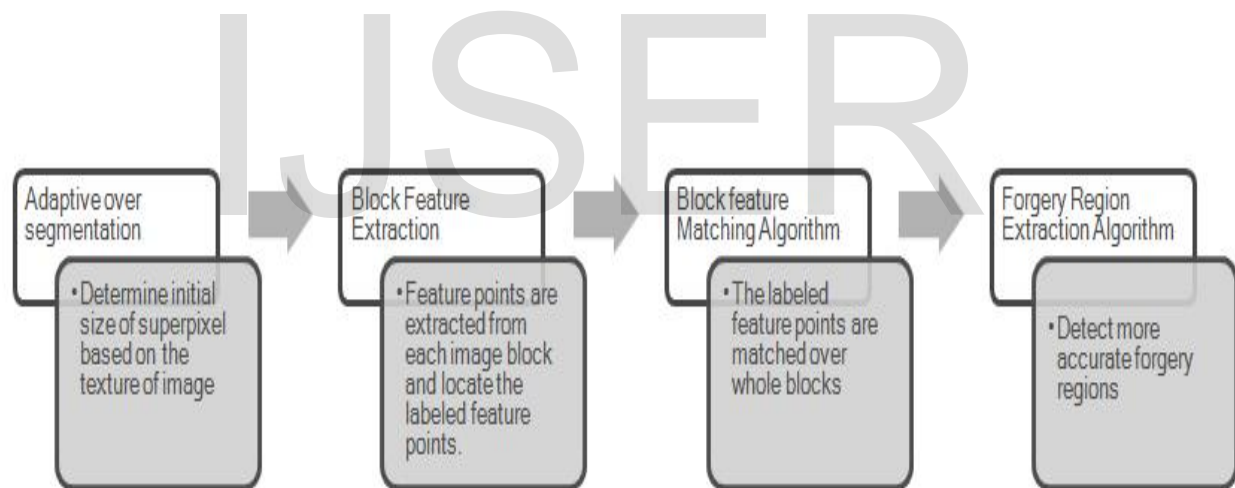
- 1) The host image is divided into over-lapping regular blocks, which would be computationally overpriced as the image size increases
- 2) These algorithms cannot route momentous geometrical transformations in the forgery regions.
- 3) Since their blocking method is regular in shape, their recall rate is low.

The existing keypoint-based found solution for the first two problems; but the recall results of the existing keypoint-based forgery methods were very poor.

Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi [7] proposed technique accepts the advantages of the two categories of image forgery techniques.

They propose four steps are introduced. They are

- A. Adaptive Over Segmentation
- B. Block Feature Extraction
- C. Block Feature Matching
- D. Forgery Region Extraction Algorithm



**Fig 3.** Frame work of proposed forgery detection method.

## II. (A) ADAPTIVE OVER SEGMENTATION

This technique is similar to traditional block-based forgery detection methods which divide the host image into blocks. This method determines the initial size of the superpixels adaptively based on the texture of the host image. The texture

is calculated using the discrete wavelet transform. The superpixel size is given to the SLIC (Simple Linear Iterative Clustering) algorithm, which segment the image to irregular

non overlapping image blocks. SLIC uses the K-means clustering algorithm for generating the superpixels

#### II.(B) BLOCK FEATURE EXTRACTION

For each image blocks the feature points extracted using SIFT (Scale Invariant Feature Transform), feature points extracted from this is invariant to various distortions, such as image scaling, rotation, and JPEG compression.

#### II.(C) BLOCK FEATURE MATCHING

From the located block features we have to find the matched block features. For this first the number of matched feature points is calculated, and the correlation coefficient map is generated; then, the corresponding block matching threshold is calculated adaptively; with the result, the matched block pairs are located; and finally, the matched key-feature points in the matched block pairs are extracted and labeled to locate the position of the suspected forgery region



IMAGE		SIFT	SURF
	Key-points extracted	5977	1473
	Speed	60.88S	32.899S
	Forgery detection	SUCCESS	SUCCESS
	Key-points extracted	2180	639
	Speed	26.489s	21.622s
	Forgery detection	SUCCESS	SUCCESS
	Key-points extracted	12893	3471
	Speed	182.861s	132.89s
	Forgery detection	SUCCESS	SUCCESS
	Key-points extracted	2637	802
	Speed	23.476 s	20.054
	Forgery detection	SUCCESS	SUCCESS

Table1. Examples of forgery detection



### III. (D) FORGERY REGION EXTRACTION ALGORITHM

To improve the precision and recall results, we measure the local color features of the superpixels, which are neighbors to the suspected regions; if their color feature is similar to that of the suspected regions, and then we merge the neighbor superpixels into the corresponding suspected regions, which generate the merged regions. Finally, a close morphological operation is applied to the merged regions to generate the detected copy-move forgery regions.

### IV. PROPOSED MODIFICATIONS

Although the Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi [7] proposed technique can solve almost all problem related

to existing copy move image forgery techniques, some modification in their techniques give better results.

For the feature extraction the SIFT is used by Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi [7]. In SIFT image content is transformed into local feature coordinates that are invariant to translation, rotation and imaging parameters. Since the extracted number of keypoints is maximum, the computational cost and memory cost is very large. The algorithm cannot use without the permission of the mentors.

The alternative method for the feature extraction is SURF (Speeded Up Robust Features), which is based on the Hessian matrix. The key point extracted is minimum compared to SIFT, so the time needs to execute and memory is comparatively less than SIFT. These advantages are the adoption of SURF for the feature extraction.





IMAGE		SIFT	SURF
	Key-points extracted	5977	1473
	Speed	60.88S	32.899S
	Forgery detection	SUCCESS	SUCCESS
	Key-points extracted	2180	639
	Speed	26.489s	21.622s
	Forgery detection	SUCCESS	SUCCESS
	Key-points extracted	12893	3471
	Speed	182.861s	132.89s
	Forgery detection	SUCCESS	SUCCESS
	Key-points extracted	2637	802
	Speed	23.476 s	20.054
	Forgery detection	SUCCESS	SUCCESS

Table 2. Comparison of SIFT and SURF based algorithms.

#### IV. EXPERIMENTAL RESULTS

Series of experiments are conducted to evaluate the effectiveness of the proposed image forgery detection scheme using adaptive over-segmentation and feature point matching. For this here used the dataset [8] is formed based on 10 high resolution uncompressed PNG true color images, and the average size of the images is 1500\*1500.

First we can check the experimental results of by Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi [7] proposed method. The examples of forgery detection are shown in Table1. Using the proposed method all the forged images had shown positive results.

The experimental results show that SURF based forgery detection algorithms are much faster than SIFT based forgery detection algorithm. The experimental results are shown in Table 2.

#### VI. CONCLUSION

The proposed method works faster than the all existing forgery detection techniques. The morphological operations give the better results for the detection of transformation in the forged part. The future work focuses to splicing and forgery in video.

#### References

- [1] Jessica Fridrich, David Soukal, and Jan Lukáš, "Detection of Copy-Move Forgery in Digital Images", in *Proc. Digit. Forensic Res. Workshop*, Cleveland, OH, Aug. 2003.
- [2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004
- [3] Saiqa Khan, Arun Kulkarni, "Robust Method for Detection of Copy-Move Forgery in Digital Images" International Conference on Signal and Image Processing, 2010.
- [4] L. Fitzpatrick and M. Dent, "Region Duplication Detection Using Image Feature Matching," *Ieee Transactions On Information Forensics And Security*, Vol. 5, No. 4, 2010.
- [5] Jian Li , Xiaolong Li , Bin Yang and Xingming Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," *IEEE Transactions on Information Forensics and Security* , Volume:10 , dec 2014.
- [6] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe 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, September 2011
- [7] Chi-Man Pun, Xiao-Chen Yuan, and Xiu-Li Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching," *Ieee Transactions On Information Forensics And Security*, Vol. 10, No. 8, August 2015.
- [8] J. Bilmes, "A gentle tutorial of the EM algorithm and its application to parameter estimation for Gaussian mixture and hidden Markov models," *Int. Comput. Sci. Inst.*, Berkeley, CA, USA, Tech. Rep. TR-97-021, 1997.
- [9] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *Ieee Transactions on Information Forensics and Security*, vol. 7, pp. 1841-1854, Dec 2012