

# Copy-Move Tampering Detection Using SURF

Vaibhavi Panchal<sup>1</sup> Paresh Patel<sup>2</sup>

<sup>1</sup>P.G Student <sup>2</sup>Professor

<sup>1,2</sup>Department of Computer Engineering

<sup>1,2</sup>SVIT, Vasad-388306, India

**Abstract**— In the present world, images and videos are the main carrier of information. So that, they are usually provided as essential evidence in many different areas like ranging from mainstream media, journalism and scientific publication, criminal investigation and surveillance system, etc. However, this source of information can be easily tampered by using open source of powerful computer applications like Photoshop, Magisto Video Editor, Cyber Link Director Suite, Corel Video Studio Pro, etc. For making tampering more robust, various transformation like scaling, rotation, lighting changes, blurring etc. applied. Copy-move image forgery is frequently used to tamper the image. In copy-move forgery, a specific area is copied and then pasted into any region of the image. An efficient approach for detecting copy-move tampering is to use visual feature such as Speed Up Robust Features (SURF). This paper presents a tempering detection method based on SURF, which detects the key points and their corresponding features. From the key points, grouping is performed on the matched key points, which shows the copied and pasted regions.

**Key words:** Copy-move forgery, Feature detection, Feature matching, SURF

## I. INTRODUCTION

Digitalization of an image is the technology for creating, processing, and storing graphic memory and evidence. As it brings many advantages, it can be used as a misleading tool for hiding details and evidences. So that images are manipulated in such perfection that tampering cannot be detected visually.

Copy-move tampering is the most commonly used forgery, where a region within an image is copied and moved to another region in the same image in order to conceal an important object from the original image<sub>[1,2]</sub>. The copied block may be changed by any kind of pre-processing such as rotation, scaling, additive noise, etc. to suit the copied area with the whole image. Figure 1 shows, how copy-move tampering done on image.

Speed Up Robust Features (SURF) algorithm is used to find the image tempering. How SURF is used for feature detection, feature extraction and feature matching is described in next session.



Fig. 1: Copy-move Tampering

## II. SPEED UP ROBUST FEATURES (SURF)

SURF is developed by Herbert Bay, Tinne Tuytelaars and Luc Van Gool. SURF is invariant to common image transformations, rotation, scale change, illumination change and small change in viewpoint. The SURF algorithm extracts keypoints from images, and describes these keypoints using a vector. Keypoints are important points of an object that can be independently found in different views of the object. The purpose of SURF is to develop an algorithm that is faster and with the same performance than the other state-of-the-art algorithms like SIFT. SURF uses integral images which are used for convolution<sub>[3,4]</sub>.

SURF works in three steps: extraction, description and matching.

SURF extracts the features from an image using integral images and box filters. Box filters are used as an approximation of the exact filter masks. By using integral images together with box filters a major speed up is realized.

### A. Extracting Features Using SURF:

The detection is based on the Hessian matrix. Given a point  $x = (x, y)$  of an image  $I$  the Hessian matrix defined at scale  $\sigma$  is

$$H(x, \sigma) = \begin{bmatrix} L_{xx}(x, \sigma) & L_{xy}(x, \sigma) \\ L_{xy}(x, \sigma) & L_{yy}(x, \sigma) \end{bmatrix}$$

Where,  $L_{xx}(x, \sigma)$ ,  $L_{xy}(x, \sigma)$  and  $L_{yy}(x, \sigma)$  represent the convolution of the Gaussian second order derivative  $\frac{\partial g(\sigma)^2}{\partial x^2}$  with image  $L$  in point  $x$ .

The box filter can be calculated very fast using integral images. These integral images are built from the original image using,

$$I \sum(x) = \sum_{i=0}^{i < x} \sum_{j=0}^{j < y} I(i, j)$$

$x = (x, y)$  is a location in the integral image, than in the integral image  $I \sum(x)$  equals the sum of all pixels in the input image  $I$  of a rectangular region formed by that point  $x$  and the origin. With  $I \sum(x)$  calculated it only takes four additions to calculate the sum of the pixel values in any upright rectangular area independent of the size of this area<sub>[5]</sub>.

### B. Description of the Features Using SURF:

The first step consists of fixing a reproducible orientation based on information from a circular region around the interest point. And second construct a square region aligned to the selected orientation, and extract the SURF descriptor from it. In order to be invariant to rotation, it calculate the Haar-wavelet responses in  $x$  and  $y$  direction.

Haar-wavelet responses in  $x$  and  $y$  direction are calculated in a circular neighborhood of radius  $6s$  around the interest point,  $s$  is the scale that the interest point was detected at. The Haar-wavelet responses are represented as

vectors. Then, all responses within a sliding orientation window covering an angle of 60 degree are summed. Both horizontal and vertical responses in the window are summed yielding a new vector.

$$v = \left( \sum dx, \sum dy, \sum |dx|, \sum |dy| \right)$$

To get information about the polarity of intensity changes, sum of the absolute values of the responses  $|dx|$ ,  $|dy|$  is extracted [5].

### C. Features Matching Using SURF:

In order to speed up both the detector and the descriptor steps, integral image has been used. The main benefit of the integral image is, it requires only four array references to calculate the sum of intensities of any rectangular area in the image.[5].

## III. EXPERIMENTS

Figure2 is the original image, which is being tempered by copy-move forgery and so that Figure3 shows the Tampered Image. By using the SURF algorithm, Features are detected from the tampered image.



Fig. 2: Original Image



Fig. 3: Tampered Image

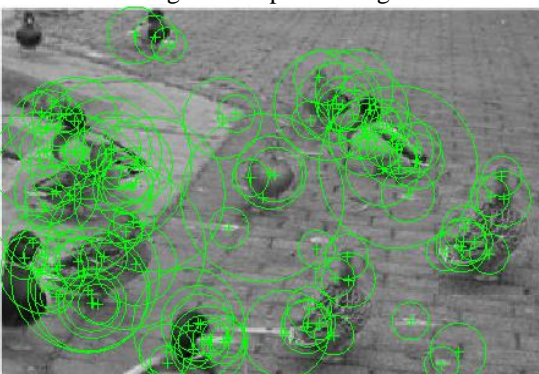


Fig. 4: Feature Detection

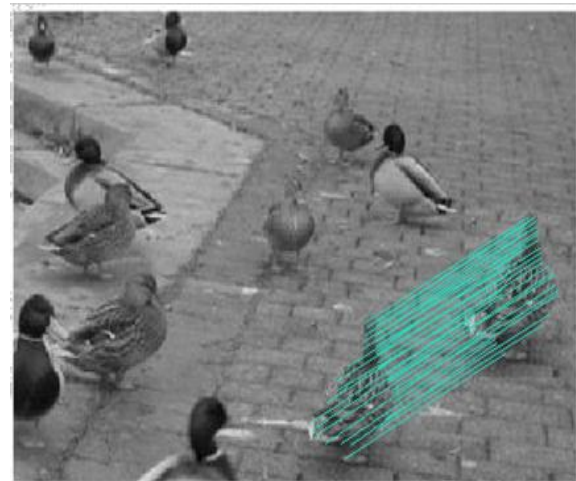


Fig. 5: Detection of copy-move tampering

After feature detection and extraction, features are being matched to check the tampered region in the image. If features are matched within the image, it gives results as shown in Figure 5.

## IV. CONCLUSION

This work is used to check whether the image is tampered or not. By using SURF algorithm, features are detected and extracted, which are used to find the duplicate region from the image. Experiment result indicates that this method can detect the copy-move tampering. For further research, we will apply the SURF algorithm on tampered videos, to find the duplicate region.

## REFERENCES

- [1] Mohasin n. Shaikh, prof. Yoginath r. Kalshetty, dnyaneshwar j. Ghanawajeer, "A SIFT for copy-move attack detection & Transformation recovery", international journal of advanced engineering research and studies, e-issn2249-8974, December 2013
- [2] Ghulam Muhammad, Muhammad Hussain, George Bebis, "Passive copy move image forgery detection using undecimated dyadicwavelet transform", Elsevier Ltd, April-2012
- [3] H. Kandil and A. Atwan, "A Comparative Study between SIFT- Particle and SURF-Particle Video Tracking Algorithms", International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 5, No. 3, September, 2012
- [4] Jin-Sup Shin, Jun-Ho Yoo and Dae-Seong Kang, "A Study on Moving Object Tracking Algorithm Using SURF Algorithm and Depth Information", Advances in Systems Theory, Signal Processing and Computational Science 2012
- [5] Professor Kaleem Siddiqi, "SURF: Speeded-Up Robust Features", McGill University, December 2008
- [6] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, Luca Del Tongo Giuseppe Serra, "Copy-move forgery detection and localization by means of robust clustering with JLinkage", ScienceDirect, April 2013
- [7] Sadhana P. Shisode and Prof. Mrs. K. P. Moholkar, "Real time object Identification, training and

matching via surf algorithm methods” International Journal of Advanced Research in Computer Science and Software Engineering, June-2014

- [8] Irene Amerini, Lamberto Ballan, Roberto Caldelli, Member, Alberto Del Bimbo and Giuseppe Serra, “A SIFT-based forensic method for copy-move attack detection and transformation recovery”, IEEE, Sep 2011

