APPLICATION OF SIFT ALGORITHM IN DIGITAL IMAGE TAMPERING DETECTION

Ms.Parul Pandey[*1] Dr.Aruni Singh[**2]

*[1]Computer Science & Engineering Dept., Kamla Nehru Institue of Technology, Sultanpur , UP

**[2s]Computer Science & Engineering Dept., Kamla Nehru Institute of Technology, Sultanpur, UP

Email: parulpandey209@gmail.com, Email: arunisingh@rocketmail.com

Abstract- In digital image processing, image tampering is advance concept for detecting forged images. Copy move forgery technique is used for tampering detection. The aim of this paper is to find copy move forgery in an image. In copy move forgery portion of an image is copied and pasted in the same image. To detect tampering in image we create algorithm which is on the basis of SIFT algorithm. It is used for feature extraction and feature detection in image.

Keywords- Tampering, Copy-move forgery, Scale invariant feature transform

I. INTRODUCTION

Digital image and video are the main source of the information. It has conveyed information fast due to their easy storage and acquisition. There are many software tools available for tampering. It has become very easy to modify the digital image by using some tools. Tampering is done by different methods: adding something new in the image hiding or deleting a part in the image and manipulate the image. Image tampering refers to manipulate the image. Basic requirement to test the originality of the image and video are authenticity. Fig 1 is showing image tampering [7]

A .Original image **B. Tampered image**

Fig 1 An example of Image Tampering

In this example in left portion of the image there are many people but in right portion of image some person are missing especially person who wear the police like outfit.

Image tampering is classified into two approaches: Active approach and passive approach which is shown in Fig 2. Active approach detects an image has tampered or not. It also detects the authenticity of image. On the other hand passive approach detects integrity of image content. This approach is divided into three parts-

1. Copy-move forgery
2. Image splicing
3. Image retouching

From above approaches copy move forgery has commonly used for detecting tampering.

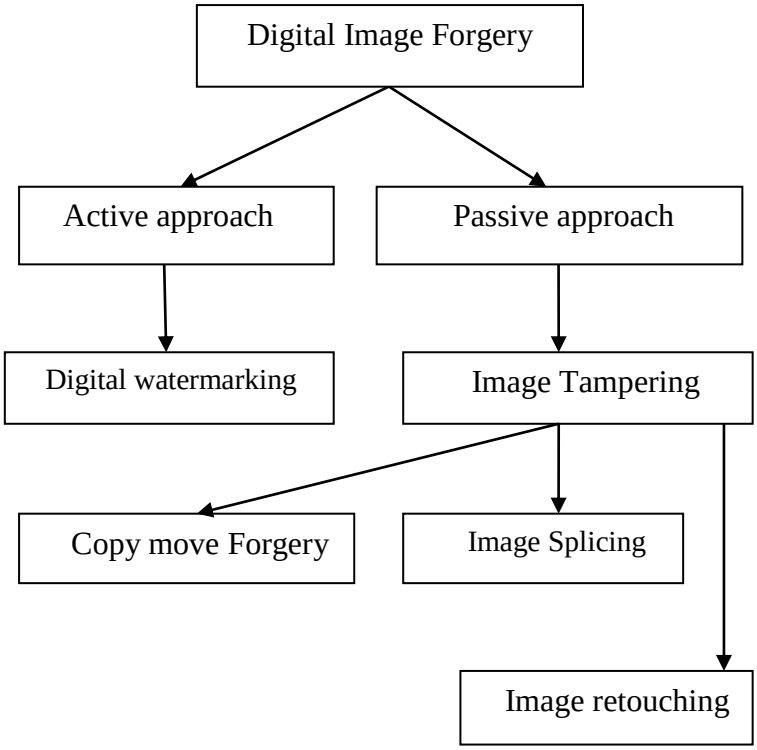

Fig 2 Methods of Image Tampering Detection

In copy move forgery we copied a part of image and pasted it into another area of same image. Fig 3 showing example of copy move forgery [3]

(a) Original Image (b) Copy move forgery

Fig 3 An example of copy move forgery

In this example we seen (a) is the original image but in part (b) more than one fountain has seen whether fountain placed on the right was copied and pasted over the left portion. To detect tampering there has been two technique and these techniques has based on two approaches. The approach is block based approach and second one is key-point based approach. The main purpose of this paper is to find tampering in images by using SIFT algorithm.

This paper is organized by discussing the tampering detection and their parts in section I. The key-point approach and also a brief introduction of their algorithm are discussed in section II. Section III describes the literature survey. Section IV describes the proposed method for detection of tampering and their experiment results are discussed in section V. Finally a conclusion of the topic based on the result obtained and suggestion for future work is discussed in section VI.

II. KEY-POINT BASED APPROACH

Key-point based method are used for recognize and selecting high entropy image regions. Key-point based technique has based on rotation, interest points, feature descriptor and detector. Copy move forgery are used block based approach as well as key-point based approaches.

To detect key-point two algorithms are available .First one is Scale Invarient Feature Transform (SIFT) and second is Speed up Robust Feature (SURF) algorithm.

2.1 Scale Invarient Feature Transform (SIFT)

It is used to find out features in an image. To detect feature point easily it uses approaches like clustering, the nearest neighbor, Euclidean distance etc. This algorithm finds the interest points which includes SIFT description and SIFT descriptor. SIFT feature has detected from gray level image. SIFT is categorized into four major parts-

1. Scale space representation of image.

2. Computation of key-points.

3. Orientation of key-points.

4. Key-point descriptor.

In first step it searches all scales and locations of image. It is implemented by difference of Guassian function.

In second step it computes key-point of the images .Key-point has detected on the basis of stability measures.

In third step each key-point location has one or more orientation which is based on gradient of image direction.

In last step around each key-point local image gradient region are computed at scale.

These are main steps of SIFT algorithm, after the completion of these steps at the end matching is performed. In key-point matching it identifies key-point and nearest neighbor between the similar images which is matched or not.

III. LITERATURE SURVEY

There are many techniques were used to detect forgery such as DCT based algorithm, PCA based algorithm, passive approach, active approach and watermarking techniques etc. These techniques were proposed before SIFT algorithm. Now discuss about some important literature on the basis of different algorithms.

Hany Farid et al [6] In this paper author discuss about techniques and method of image forgery detection. In this paper author give detail discussion about forgery detection.

Anil Dada Warbhe et al [2] In this paper author discuss about the key-point based technique. It detects and describes the feature of the image by using key-point based algorithms.

Irene Amerini, Lamberto Ballan, et al [3] In this paper author describe a method on the basis of SIFT algorithm. In this method geometric transformation is used for cloning. It performs key-point detection and matching. The result was obtained from this method very easily. It also detects forgery in images.

David G Lowe et al [5] In this paper author proposed a method for extracting the feature of the image. It was also discuss about approach of features which was used in object recognition. They were used nearest neighbor algorithm for matching.

Vincent Christlein et al [1] In this paper author analyzed the existing algorithms according to the feature set and also evaluated their performances. It was given results as: key-point based algorithm such as SIFT, SURF and block based algorithm such as DCT, DWT, PCA both gives better performance as well.

In all the above papers authors discuss about different algorithms like DCT, DWT, PCA etc to detect tampering detection in the images.

IV. PROPOSED METHOD

The proposed method is build on the Scale Invarient Feature Transform algorithm. This algorithm extracts the feature of images. In this method we input the original image, then we apply SIFT algorithm which includes scale space extrema, key-point detection, key-point descriptor and matching. After completion of SIFT algorithm we perform copy-move algorithm to detect tampering in image.

4.1 Proposed algorithm

The steps of proposed algorithm are:

Step1: First insert the original image.

Step 2: Next check whether image is gray scale or not.

Step 3: If image is found gray scale then find out scale space extrema using SIFT algorithm otherwise convert the image into gray scale image.

Step 4: Next detect key-point of images.

Step 5: After completion of key-point detection find key-point descriptor .

Step 6: Now perform matching of key-point using 2NN matching.

Step 7: If matching found then perform copy-move forgery detection algorithm.

Step 8: Now locate the tampered region it means tampering detection is done.

Step 9: Show resulting output image.

These steps clearly shows that copy move forgery detection using SIFT algorithm. In this proposed algorithm SIFT feature is detected and also tampering is detected.

4.2 Flow Chart of Proposed Algorithm

The flow chart of the proposed work is shown in fig 4. In this section follow above steps very carefully. In this section discuss about whole working of the SIFT algorithm for detecting tampered image.

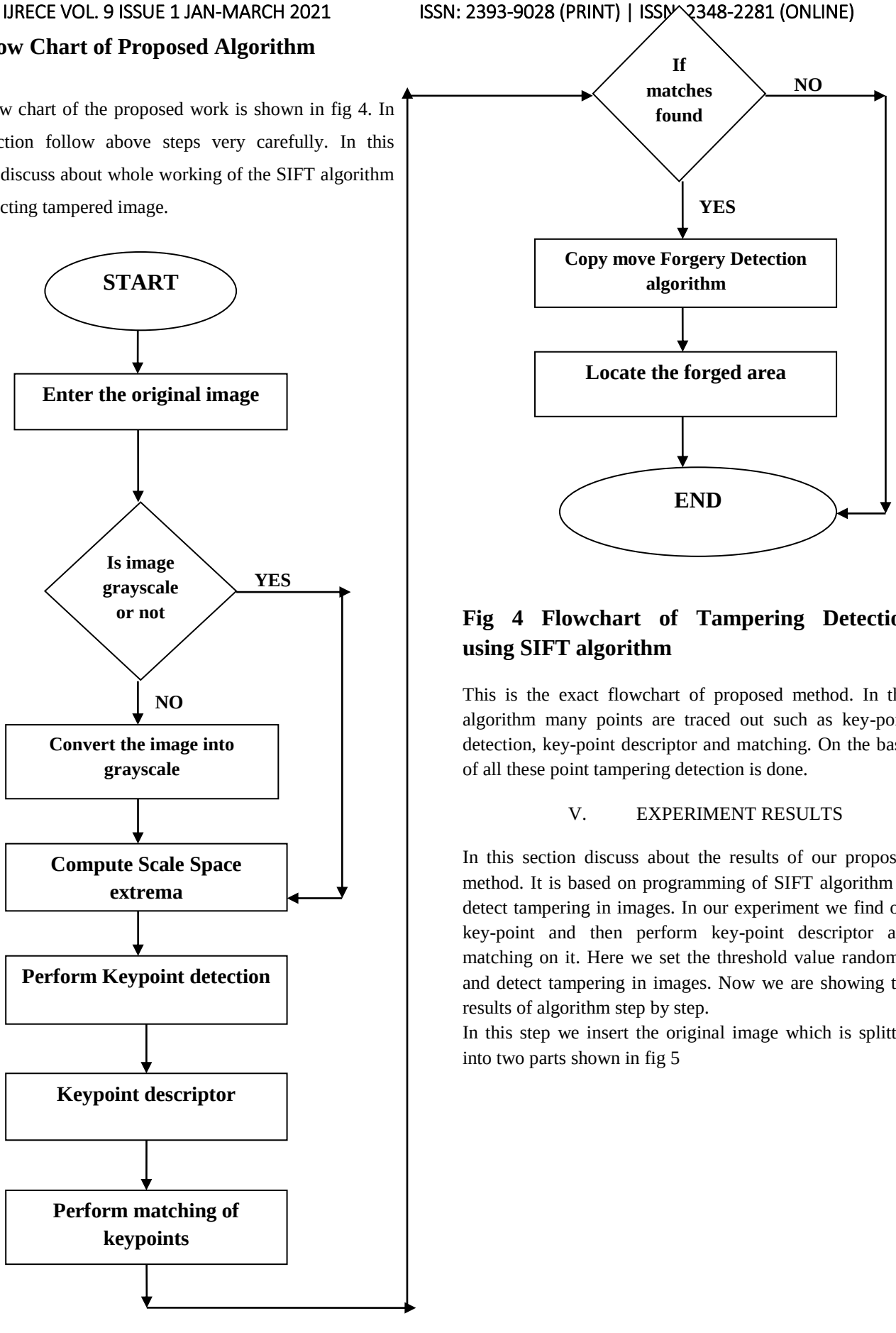

Fig 4 Flowchart of Tampering Detection using SIFT algorithm

This is the exact flowchart of proposed method. In this algorithm many points are traced out such as key-point detection, key-point descriptor and matching. On the basis of all these point tampering detection is done.

V. EXPERIMENT RESULTS

In this section discuss about the results of our proposed method. It is based on programming of SIFT algorithm to detect tampering in images. In our experiment we find out key-point and then perform key-point descriptor and matching on it. Here we set the threshold value randomly and detect tampering in images. Now we are showing the results of algorithm step by step.

In this step we insert the original image which is splitted into two parts shown in fig 5

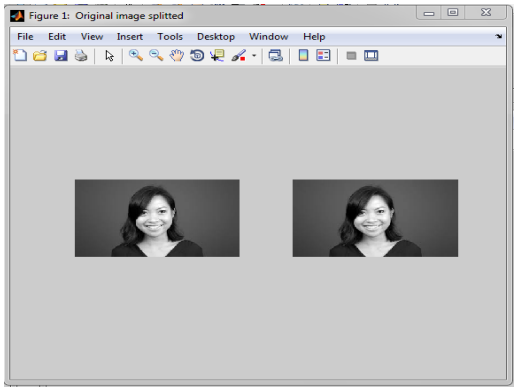

Fig 5 Insertion of original image

In next step we check image is grayscale or not. Here our image is in already grayscale so we move to next step otherwise we can convert original image to the grayscale by using this function I = rgb2gray(RGB)

newmap = rgb2gray(map) in matlab.

Then we detect scale space extrema in which we divide the image into three octaves. It obtains scales and location of images. It shows blurred image which is shown in Fig 6

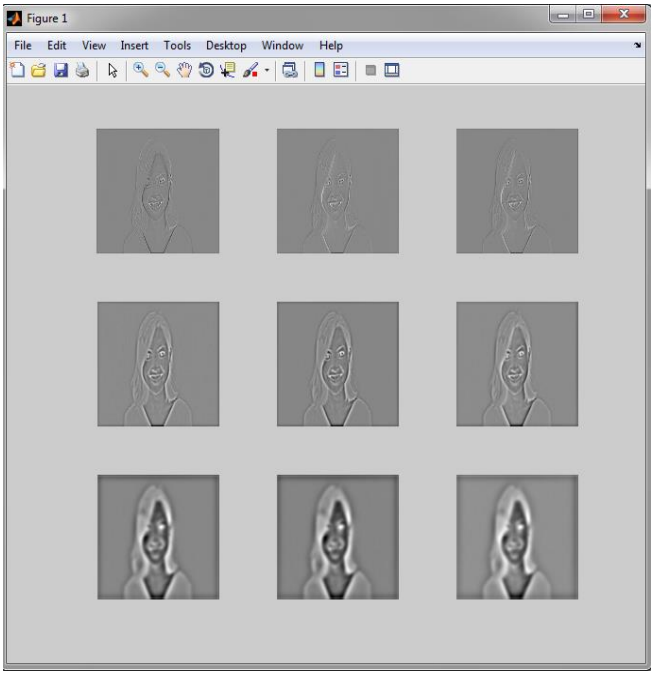

Fig 6 Result of scale space extrema

In next step calculate synthetic keypoint in the images. Keypoints are the maxima and minima in the DOG (difference of Gaussian) image. That is shown in Fig 7

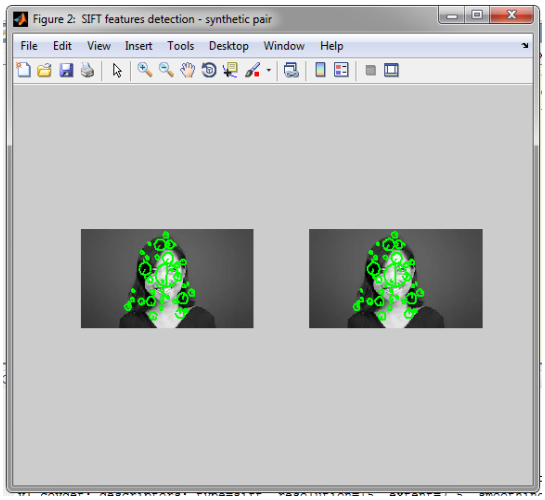

Fig 7 Showing keypoint detection

If we find out key-point of the image then we are perform feature descriptor that is image gradient. In this step we take any one key-point and form a gradient of image. SIFT computes this descriptor by taking a 16x16 block of pixels centered at a key point, dividing it into 4x4 cells, and computing an 8-bin histogram of gradient orientations within each cell[5]. This results in a 4*4*8=128-element vector, which is the descriptor. Result of descriptor is shown in fig 8.

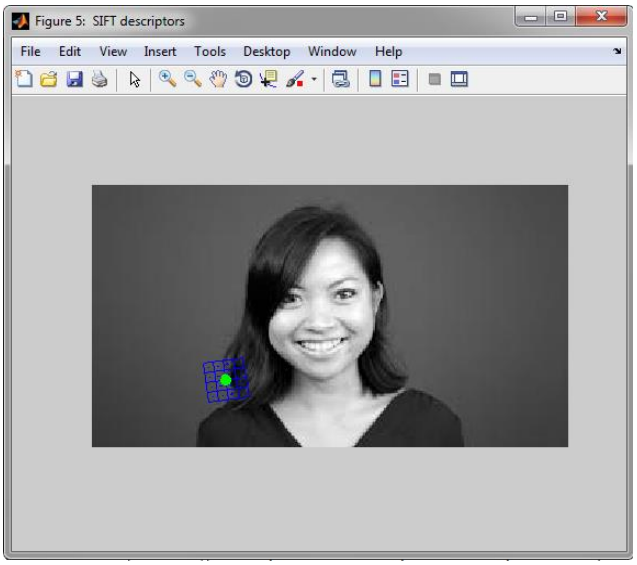

Fig 8 Result of Keypoint Descriptor

After completion of step SIFT descriptor now we move on to next step where we find matching**.** In this step we find keypoint matching by using 2NN matches method.

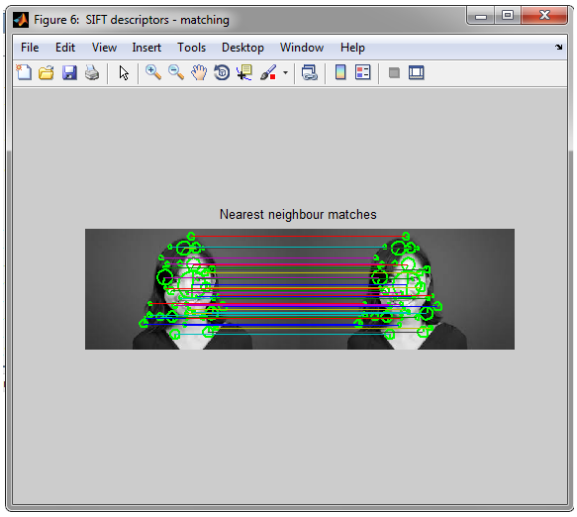

Fig 9 Result of matching

If matches are found then we apply copy move forgery algorithm to find out tampered image. In this step we copied a face of girl and pasted it into same image. Then we resize the image and next we show the copy move part of the image. These results are shown in Fig 10 and 11

Fig 10 Result of copy move forgery detection

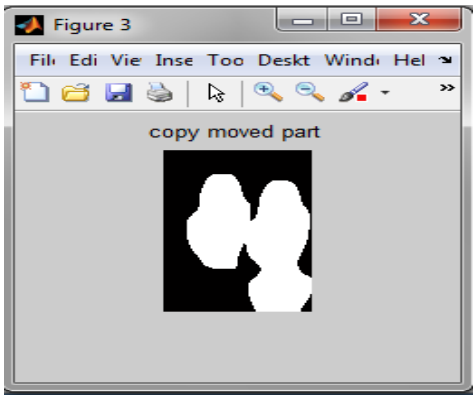

Fig 11 shows the copy moved part

These are results of experiment which clearly shows the tampering detection in image. It shows clearly the steps of SIFT algorithm. In first five figures it illustrate the SIFT algorithm and last two figures gives the result of forgery detection.

VI. CONCLUSION AND FUTURE SCOPE

Tampering detection in images has been done with the help of SIFT algorithm. SIFT algorithm gives results after performing key-point detection, key-point descriptor and matching. At the last two steps we obtained results of forgery detection. This algorithm is efficient for tamper detection. This paper has presented detection of tampering in image with the help of SIFT algorithm. Here only one type of key-point based algorithm is used for detection. Further we take another algorithm i.e. SURF algorithm for tampering detection.

VII. REFERENCES

[1] 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, no. 6, pp. 1841-1854, Dec. 2012.

[2] Anil Dada Warbhe, R.V. Dharaskar, V.M. Thakare, "A Survey on Keypoint Based Copy-paste Forgery Detection Techniques", *Procedia Computer Science*, Volume 78, Pages 61-67, 2016.

[3] Jie Zhao, Jichang Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD", *Forensic Science International*, Volume 233, Issues 1–3,Pages 158-166,2013.

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

[5] David G. Lowe, "Distinctive Image Features from Scale Invarient Keypoint", *International Journal of Computer Vision*, Volume 60, Issue 2, pp.91-110, November2004.

[6] H. Farid, "*Image forgery detection*," IEEE Signal Processing Magazine, vol. 26, no. 2, pp. 16-25, Mar 2009.

[7] R. Rajkumar and K. M. Singh, "Digital image forgery detection using SIFT feature," *2015 International Symposium on Advanced Computing and Communication (ISACC)*, Silchar,, pp. 186-191,2015.