Copy-Move Forgery Detection Using ORB and SIFT Detector

[1]Rajdeep Kaur,[2nd] Amandeep Kaur
[1]PG Student,[2]Assitant Professor
[1]Electronics& Communication Engineering,
[1] Giani Zail Singh College Campus of Engineering & Technology, Bathinda,India

***Abstract*—Copy-move attack is very frequently used to secrete or hide some information in the digital image for particular purpose and in this attack some part of the original image copied and pasted in the same image. Thus Copy-Move forgery is very important issue and active research area to check the confirmation of the image. In this paper, Copy-move forgery detection using Key-point based methods i.e. SIFT (Scale Invariant Feature Transform) and ORB (Oriented FAST and rotated BRIEF) are implemented. After feature extraction of the test images using SIFT and ORB, two algorithms SVM (Support Vector Machine) and EM (Expectation Maximization) are used to classify the forged and non-forged data. Experimental results are calculated in terms of accuracy, precision, recall and F_1. Experimental results show betterPerformance using ORB with SVM (Support Vector Machine) and ORB with EM (Expectation Maximization) methods in terms of Accuracy, Precision, Recall and F_1 than SIFT with EM method.**

***IndexTerms*—Copy-Move Forgery Detection, SIFT algorithm, ORB algorithm, SVM and EM algorithm.**

I. INTRODUCTION

Digital images play a very basic role in many applications and have become a leading source of information. In recent years, due to the increment in the image editing software applications and the easiness of using these, the probability of malicious changes on the images has also increased. The purpose of the editing of the digital images can be to hide or conceal some information from the original image, to enhance the quality of the image, to collect the more information from two or more images into one image.
Any image manipulation can become a forgery, there are three types of forgeries can be identified on the basis of the method adopted to do the forgery, such as using graphical software, contentbased [1]**.** Because today digital image can be manipulated in such perfection that forgery cannot be detected by naked eyes. So, the security concern of the digital images content has arisen a long time ago and different techniques have been developed to check the confirmation of the digital image[2]**.** Image forgery is also called image tampering. Image tampering is defined as changing or deleting some important features from an image without leaving any obvious trace. Digital image forgery can be divided into three main categories and listed below:

1) Copy-Move Forgery: In Copy-Move forgery, particular part of the original is copied and pasted into the target position in the same image [3]. Thus resultant image is called forged image.

2) Image Forgery Using Splicing: Image splicing is a method which uses cut and paste techniques form number of images to create a new fake images [2].

3) Image Retouching: Image retouching is less harmful techniques as compare to other forgery techniques. In image retouching enhancement of some feature of the image is done and the subject of the image remains same [4].

II. DIGITAL IMAGE FORGERY DETECTION

Digital image forgery detection techniques are mainly described briefly. These are mainly divided into two classes: active techniques and passive techniques.

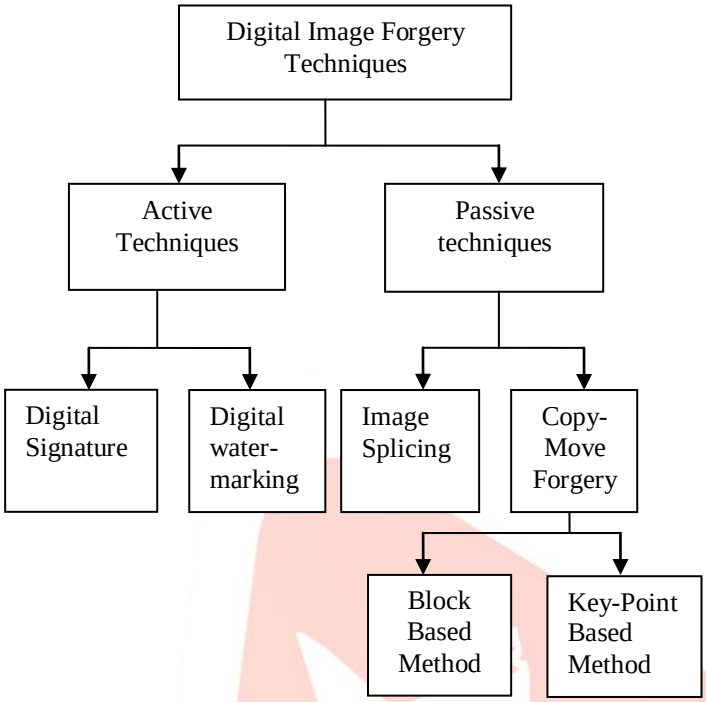

Figure 1:Types of digital images forgery detection techniques

A. ACTIVE TECHNIQUES: These active methods may be categorized into two classes: Digital watermark and Digital signature.

- **Digital Watermarking**: The digital watermarking is a two-way process. The source generates a watermark; encode it into an image to get the watermark image. The receiver side scans the watermarks image and extracts the watermark to test whether the image has been altered or not [8]. A digital watermark is a pattern of bits encoded into a digital image and scattered all around to avoid modification. Thus, the primarily process of digital watermarking is to add secret data and recovering the same partially for image confirmation.

- **Digital Signature:** In digital signature technique a unique feature of digital image is extracted while capturing the image [8]. During authentication same technique is applied to generate signature again. The authentication of image is identified through comparison.

B. PASSIVE TECHNIQUES: Passive methods are also known as digital image forensics and multimedia forensics. It is also known as blind techniques because there is no additional information about the image. Mainly passive techniques are image splicing and copy-move.

- **Image Splicing**: Image splicing is a method which deals with producing a forged image by copying and pasting a region from one or more images to another image [13]. In some cases, human eyes may be able to identify this type of forgery because a spliced image may have many irregularities in many features such as different lighting, color patterns, shadows etc.

- **Copy-Move Forgery:** Copy-Move Forgery is a most common technique for manipulating an image. A forger achieves a copy-move forgery by copying and pasting a part in the same image with the intent of hiding unwanted regions. Copy-Move forgery detection techniques are mainly classified as: Block based copy-move detection techniques and Key-point based copy-move detection techniques [11].

- **Block-Based Methods:** In block based methods, firstly the input image or test image is converted into gray-scale image. And gray scale image is converted into overlapping blocks for detecting the forged region. Block-based methods able to detect forgery; in flat regions and handle multiple cloning. Block based methods are robust against JPEG compression, noise addition and gives the exact location of tempered region. In literature block based methods are DCT, DWT, PCA, FMT and Zernike [10].

- **Key-Point Based Methods:** Key-points based methods; input image is firstly divided into corner or isolated points to provide local features description of the image. The key-point algorithm for detecting of copy-move forgery starts by extracting high entropy regions i.e. Key-points. These feature descriptors are extracted from these features. This feature descriptor is compared with each other to detect the matched key-points and forgery detected [3]. The well-known key-point descriptors are SIFT (Scale-Invariant Feature Transform) and SURF (Speeded-Up Robust features) and ORB (Oriented FAST and Rotation BRIEF).

III. METHODOLOGY

In this section, flow chart of the purposed scheme and brief discussion of various steps involved in implementation are given below:

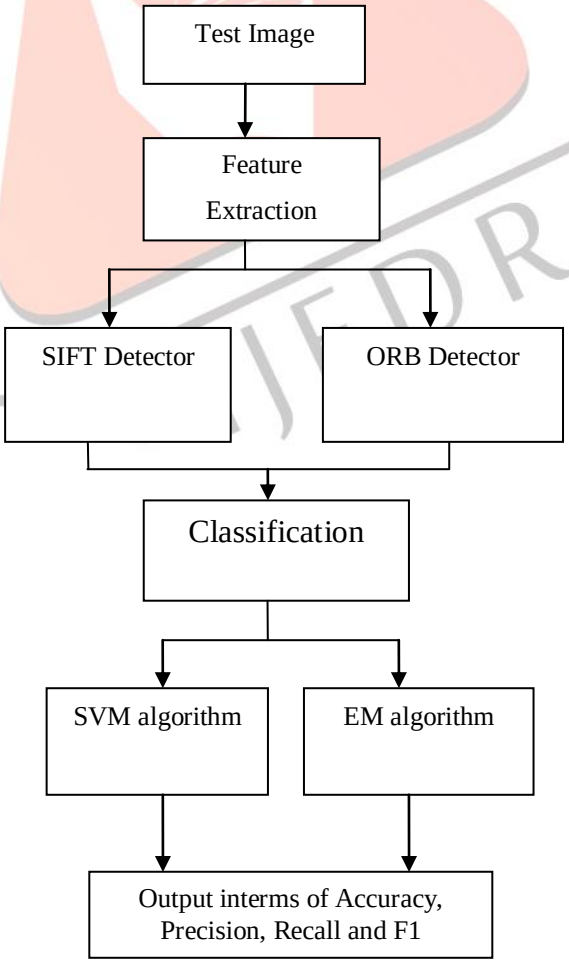

Figure 2:Flow Chart of Purposed Methodology

STEP 1: INPUT IMAGES OR TEST IMAGES- MICC-F600 dataset is used for input images. It consists 600 high resolution images containing realistic and challenging Copy-move attack.

STEP 2: FEATURE EXTRACTION-Feature extraction is the process of finding a new representation of the image in terms of features. Basic idea to extract discriminated features, that represent the data or image in a good manner. In purposed scheme, two feature detectors i.e. SIFT (Scale Invariant Feature Transform) and ORB (oriented FAST and rotated BRIEF method) is used.

STEP 3: SIFT ALGORITHM- SIFT (Scale Invariant Feature Transform) is a key-point based detector and descriptor [6] SIFT method involves various steps to extract key-points from the test images [12]. Steps are described below:

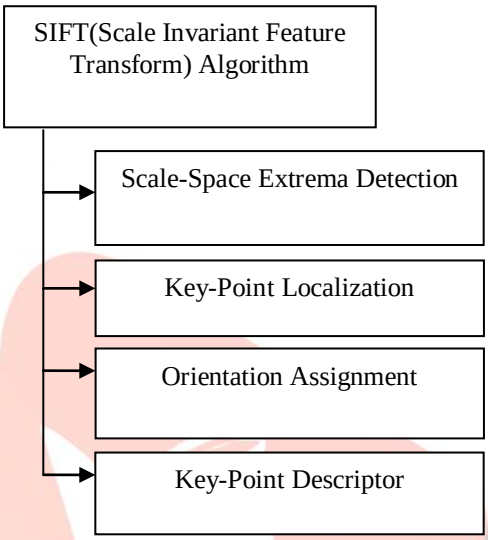

Figure 3: Step Involved in SIFT algorithm

STEP 3A: ORB DETECTOR- ORB is a feature descriptor that is oriented FAST and Rotated BRIEF. ORB consist FAST corner detector and BRIEF descriptor (Binary Robust Independent Elementary features) [9].

A. FAST is a Features from accelerated segment Test. It is a feature detector and involves some step to detect corner points in the test image; as given below:

a) Select a pixel P in the image which is to be identified as an interest point or not. Let its intensity be Ip.

b) Select appropriate threshold value t.

c) Consider a circle of pixels around the pixel under test.

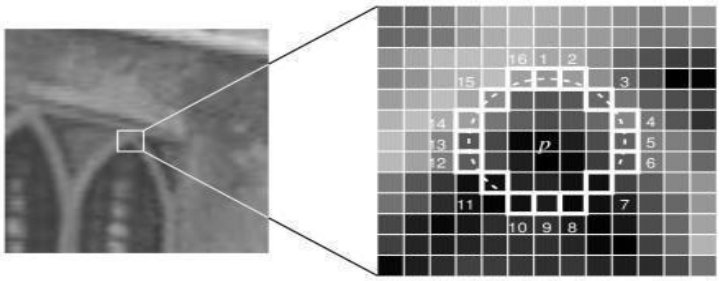

Figure 4:Example Of FAST Corner Detector

d) Now the pixel P is a corner if there exists a set of n contiguous pixels in the circle which are all brighter than Ip it Ip+ t or all darken than Ip-t. N was chosen to be 12.

e) A high-speed test was proposed to exclude a large number of non-corners. This test examines only the four pixels at 1, 9, 5 and 13 (first 1 and 9 are tested if so, then checks 5 and 13). If p is the case, then p cannot be a corner. The full segment test criterion can then be applied to the passed candidates by examining all pixels in the circle. This detector in itself exhibits high performance.

B. BRIEF: The brief descriptor is a bit string description of an image patch constructed from a set of binary intensity tests [7]. Consider smoothed image patch p, a binary test is defined by:

$$\tau(p;x,y) = \begin{cases} 1 : p(x) > p(y) \\ 0 : \ p(x) \leq p(y) 1) \end{cases}$$

Where p(x) is the intensity of a p at a point x. the feature is defined as vector of n binary tests.

Step 4 In proposed scheme, two different classifiers are used to classify the images whether it is copied or forged.

4A. First classifier is used SVM(support vector machine) with RBF kernal. SVM have linear classifier which is used to sepraable data and non-linear SVM[14]. In this original input space can be mapped to some higher dimensional feature space where the training set is separable. In this kernel function is used to maps the data to the higher dimensional space. Kernel function is used to replace dot product in higher dimensional feature space. The functions which are positive definite symmetric called as kernel. There is some kernel function i.e. polynomial kernel, radial basis function kernel, hyperbolic tangent kernel. In this test paper, SVM with RBF kernel is used for classification. RBF kernel is radial basis kernel. Kernel function is used with EM algorithm for classification of the training data.

4B. EM algorithm is used to classify the features obtained by ORB and SIFT, results are calculated in terms of Accuracy, Precision and Recall. EM algorithm is basically expectation-maximization. EM algorithm is used to find maximum likelihood parameters of a statistical model. These models involve latent variables in addition to unknown data observations. That is, either there are missing values among the data or the model can be formulated more simply by assuming the existence of additional unobserved data points. The statically model generates a set of observed data, a set of unobserved latent data or missing values, and a vector of unknown parameters is determined by the marginal likelihood of the observed data [5]. The EM algorithm seeks to find the mile of the marginal likelihood iteratively applying the following two steps: Expectation step (E-step): Calculate the expected value of the log likelihood function, with to the conditional distribution of given under the current estimate of the parameters. Maximization step (M-step): Find the parameters that maximize this quantity.

IV. RESULTS AND DISCUSSION

As discussed above, in this research paper classification of input images of dataset MICC-F600 is done by extracting feature of digital images using two different detectors i.e. SIFT and ORB. Thus results are shown in this section.

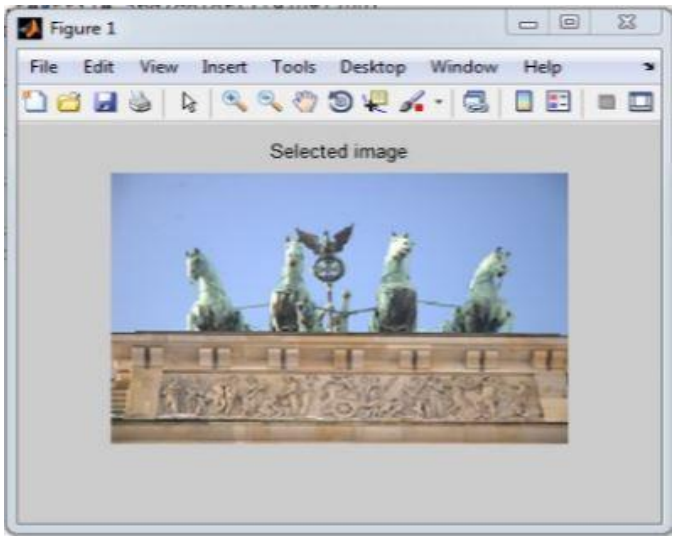

Figure 5: Input Image or Original Image

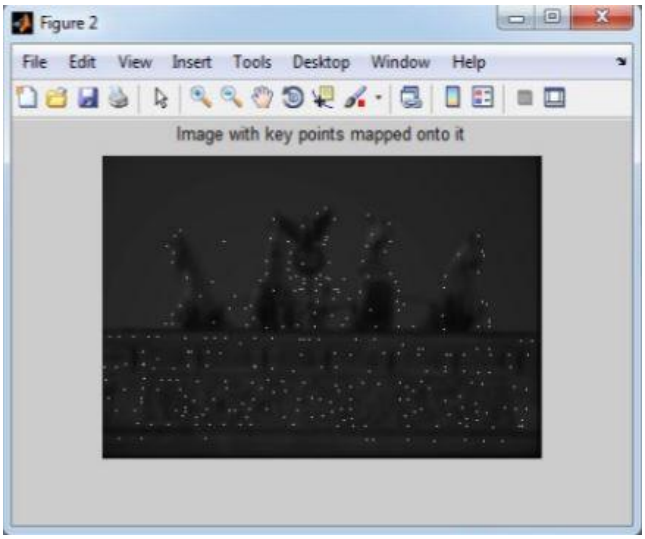

Figure 6: Key-Point Extraction or Feature Extraction of Input Image

Figure 7: Forged Image

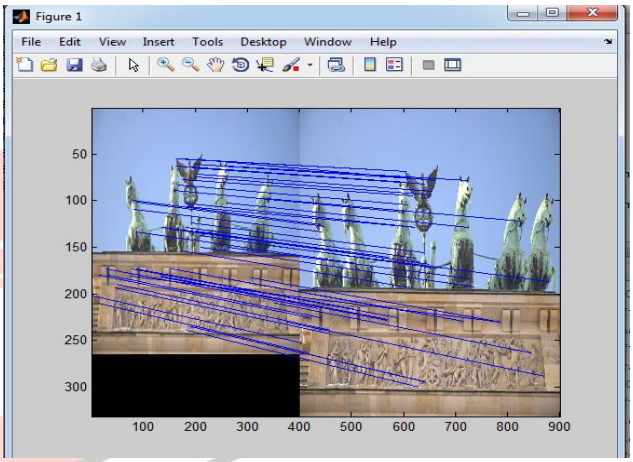

Figure 8: Copy-Move Forgery Detection using SIFT

Result of classification of the test images or dataset using SVM RBF kernel and EM algorithm in terms of Accuracy, Precision, Recall and F_1. Are given in the following table:

Table 1: Classification Result of feature extraction using SIFT+EM

F1	Recall	Precision	Accuracy	Input image	Method
81.04	81..1	81	90.5	Six hundred	SIFT+EM
79.84	79.93	79.75	89.14	Four eighty	SIFT+EM
71.32	71.51	71.14	80	Three hundred	SIFT+EM

ORB descriptor is used for feature extraction of the dataset MICC-F600. To demonstrate performance of ORB descriptor using python 2.7.5 platform is used. The results of feature extraction using ORB descriptor is represented below:

Figure 9: Input Image

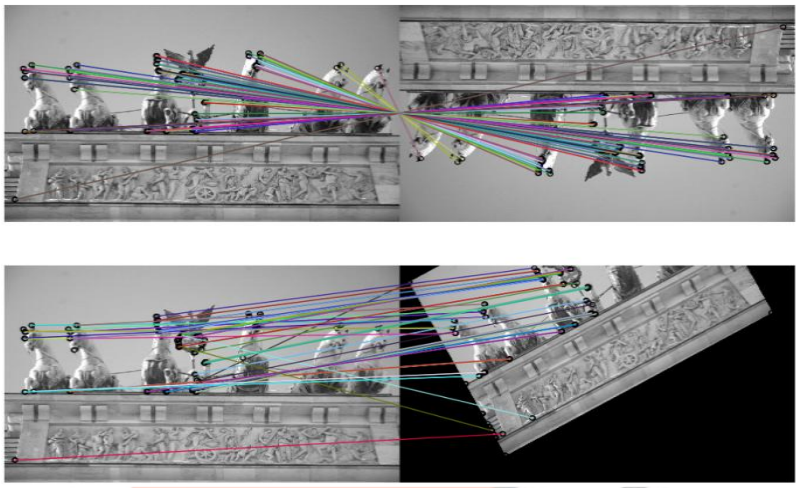

Figure 10: The original image is shown in the first column; the tampered images with rotated plane and oriented and scaled plane is shown in second column; and detection results using ORB descriptors are shown respectively.

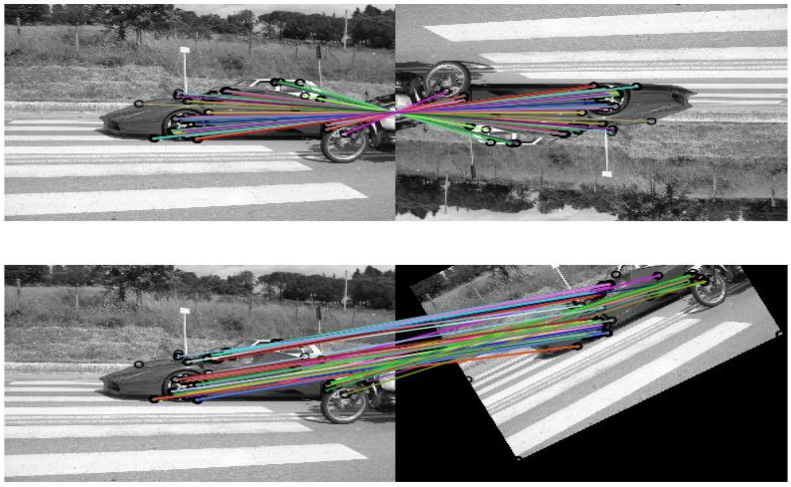

Figure 11: The second original image is shown in the first column; the tampered images with rotated plane and oriented and scaled plane is shown in second column; and detection results using ORB descriptors are shown respectively.

Table 2: Accuracy, Precision, Recall and F_1 for ORB descriptor with SVM and EM algorithm.

F_1	Recall	Precision	Accuracy	Input Images	Methods
85.39	87.285	83.58	90	Six hundred	ORB+SVM
85.65	85.22	84.085	92	Four eighty	ORB+SVM
88.26	90.11	86.5	93	Three hundred	ORB+SVM
84.64	85.22	84.085	92	Six hundred	ORB+EM
82.825	83.93	81.75	87	Four eighty	ORB+EM
90.54	91.54	89.665	94.14	Three eighty	ORB+EM

V. COMPARISON BETWEEN SIFT+EM, ORB+SVM AND ORB+EM

The performance of an image-forgery classification system can be measured in terms of Accuracy, Precision, Recall and F_1. The quantitative comparison of individual parameters i.e. Accuracy, Precision, Recall and F_1 as given in Table 1 and Table 2 is represented in graphs. First graph represents Accuracy parameters evaluated from SIFT+EM, ORB+SVM and ORB+EM implementation. In this graph, X-axes show Accuracy parameter which is evaluated in percentage (%) and value of percentage is shown in Y-axes.

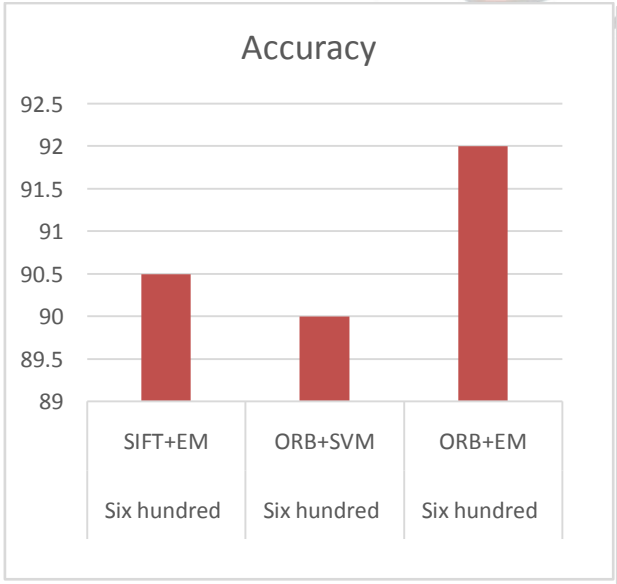

Figure 7 Graph represent Accuracy parameter with value evaluated from Implementation.

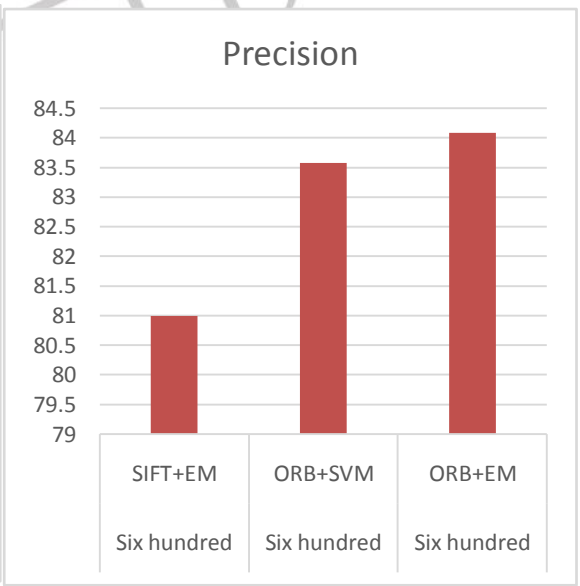

Figure 8: Graph represent Precision parameter with value evaluated from Implementation.

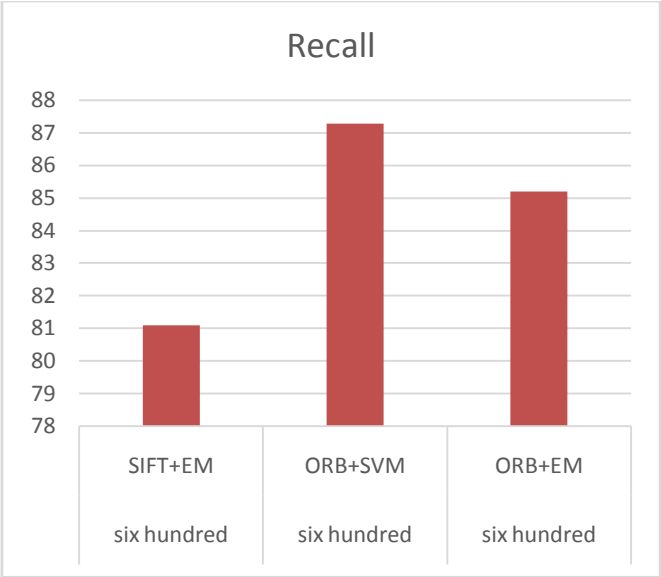

Figure 9: Graph represent Recall parameter with value evaluated from Implementation.

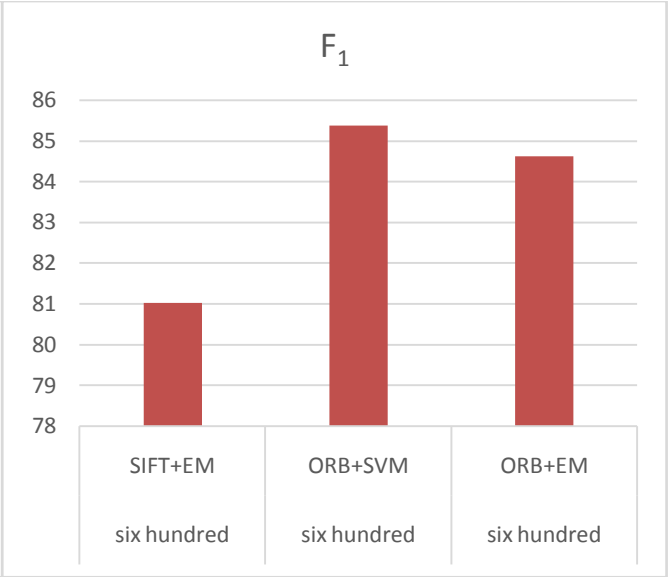

Figure 10: Graph represent F_1 parameter with value evaluated from Implementation.

FIGURE 7: Accuracy Parameter Evaluated For SIFT+EM Is 90.5%, ORB+SVM Is 90%, ORB+EM Is 92% And Graphical Representation Is Depicted In **Fig. 7**

FIGURE 8: Precision parameter evaluated for SIFT+EM is 81%, ORB+SVM is 83.5%, ORB+EM is 84% and graphical representation is depicted in **Fig. 8**

FIGURE 9: Recall parameter evaluated for SIFT+EM is 81.1%, ORB+SVM is 87.285%, ORB+EM is 85% and graphical representation is depicted in **Fig. 9**

FIGURE 10: F_1 parameter evaluated for SIFT+EM is 81.04%, ORB+SVM is 85.39%, ORB+EM is 84.64% and graphical representation is depicted in **Fig. 10**

FIGURE 11: Represents Comparison Graph of Parameters Accuracy, Precision, Recall andF_1.

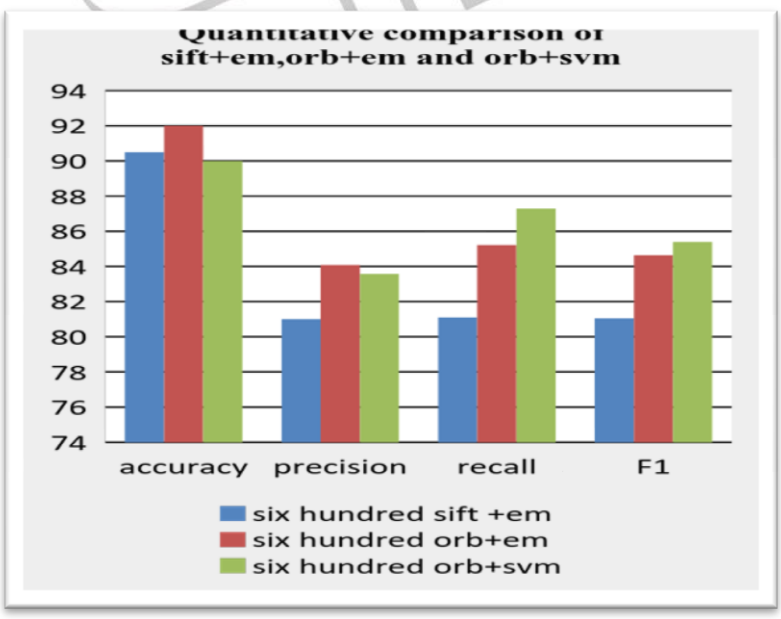

Figure 11 Comparison graphs of implemented techniques

VI.CONCLUSION

The paper presents a new method for Copy-Move Forgery Detection that utilizes ORB (Oriented FAST and Rotated BRIEF) with Expectation Maximization Algorithm and SVM RBF kernel Algorithm.SIFT (Scale Invariant Feature Transform) descriptor is used to extract key-point features from input image. But SIFT needs high computational time to extract or detect copied region. But ORB (oriented FAST and rotated BRIEF) is fast as compared to SIFT descriptor. So ORB is fast and consumes less time to extract features form input image.Experimental results show better performance in evaluated parameters i.e. Accuracy, Precision, Recall and F_1 in purposed methodology.

REFERENCES

[1] Rajdeep Kaur, Amandeep Kaur, "A Review of Copy-Move Forgery Detection", IRASCT, 2016, Vol.6, No.2, pp.249-253.

[2] ChitwanBhalla,SurbhiGupta,"A review on splicing Image Forgery Detection techniques",IRACST,2016,Vol.6,No.2,pg.262-269.

[3] Harpreet kaur, Jyoti Saxena and Sukhjinder Singh, "SimulativeComparison of Copy-Move Forgery Detection Methods for digital images", International Conference on Journal of Electronics, Electrical & Computational, 2015,Vol.4,pp 62-66.

[4] Toqeer Mohmood, "A survey on Block based Copy-Move Image Forgery detection Techniques", International Conference,2015,pp.1-6.

[5] Jian Li, Xialong Li, Nin Yang, Xingming, "Segmentation Based Image Copy-Move Forgery Detection Scheme," IEEE Transactions on Information Forensics and Security, 2015,Vol.10, No.1,pp.507-518.

[6] Emre Gurbuz, "Rotation Invariant Copy-Move forgery Detection Method", 9th International Conference on Electrical and Electronics Engineering,2015, pp.202-206.

[7] Mohan Ramakrishna, Shylaja SS, " Is ORB efficient Over Surf for Object Recognition?" , International Journal of Advanced Research in Science Engineering and Technology, 2014,Vol.3,No.8, pp.2783-2788.

[8] Prakash Kuppuswamy, Peer Mohammd Appa, Dr.Saeed Q.Y. Al-khalidi, " A new efficient digital Signature Scheme Algorithm based on Block clipher, IOSR journal of Computer Engineering,2012,pp.47-52.

[9] Ethan Rublee Willow Garage, Menlo Park, "ORB: An efficient alternative to SIFT or SURF," IEEE International Conference on Computer Vision, 2011, pp.2564-2571.

[10] Seung Jin Ryu, Min Jeong Lee, Heung-Kyuulee, "Detection of Copy-Rotate-Move Forgery Using Zernike moments", International Conference on Information, 2010, Vol.387, pp.55-65.

[11] Xu Bo, Wang Junwen, Liu Guangie and Dai Yuewei, "Image Copy-Move forgery Detection Based on SURF", International Conference on Multi-media Information Networking and Security, 2010, pp.889-892.

[12] David G. lowe, "Distinctive Image Features from Scale-Invariant Key-Points", International Journal of Computer Vision, 2009, Vol.60, No.2, pp.91-110.

[13] Hany Farid, "Image Forgery Detection", IEEE signal processing Magazine, 2009, pp.16-25.

[14] Yun, Q.Shi, Chunhua Chen, Ween Chen , "Image Splicing", 9th workshop on Multimedia & Security, 2007,pp. 51-62.