International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 08, August 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

# A HYBRID TECHNIQUE FOR COPY-MOVE FORGERY DETECTION IN DIGITAL IMAGES

**Navpreet Kaur Gill[1], Ruhi Garg[2], Amit Doegar[3]**

[1, 2, 3]*Department of Computer Science and Engineering, NITTTR,Chandigarh,(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 in terms of efficiency.*

***Keywords: Image Forensics, Copy-move forgery detection, DCT, SURF.***

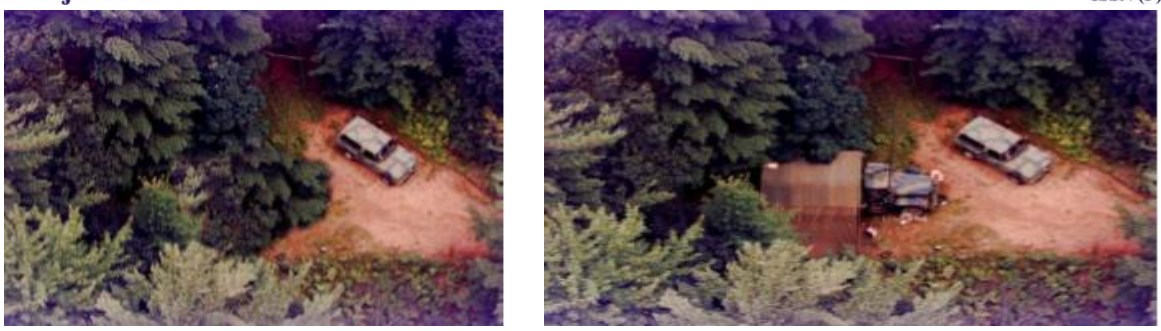
## I. INTRODUCTION

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 is depicted in Fig. 1(a) and (b). 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.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 08, August 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346



(a) (b)

**Fig. 1 (a) Untampered image (b) Tampered image [1]**

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. COPY-COVER FORGERY DETECTION METHODS

Copy-cover forgery became the most important issue in the image forgery. Copy-cover forgery is the most important issue in the image forgery. As depicted in Fig. 2 copy-cover forgery detection is primarily categorized into following classes:

[1.] Brute force methods

[2.] Block-based methods

[3.] Keypoint based methods

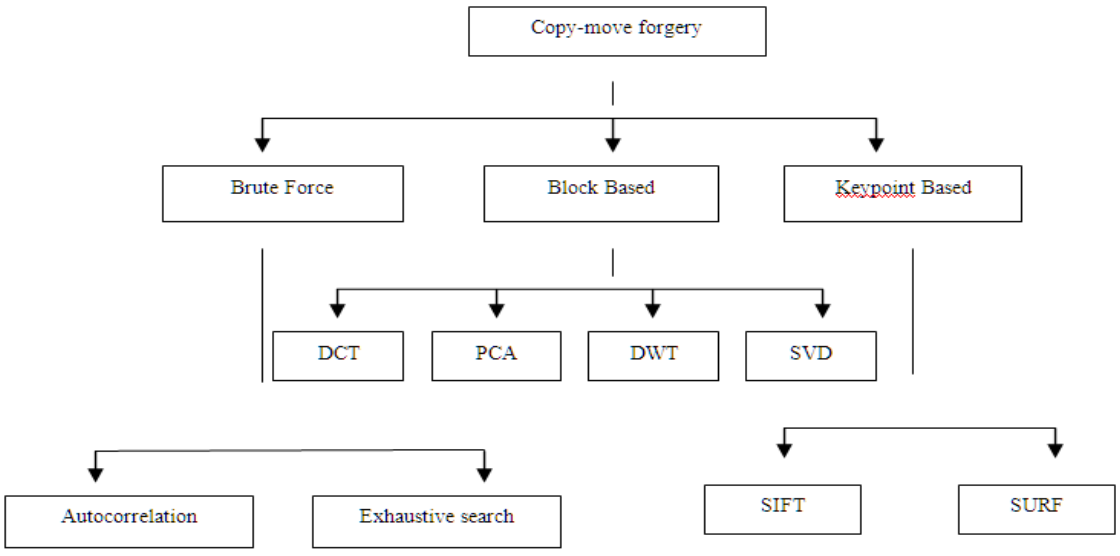



**Fig. 2 Categorization of Image Forgery Detection Techniques [6]**

### 2.1 Brute force Methods

Brute force method is based on exhaustive search and auto correlation technique. In exhaustive search, image is used to examine matching segment with circularly shifted versions. As it makes such large number of comparisons, its computational unpredictability is high. Autocorrelation determine location change.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

### 2.2 Block Based Techniques

Block based techniques came into existence because of different downsides of exhaustive search. These techniques work by dividing the image into small blocks and after that features are calculated and listed in a feature matrix. Comparison has been made to detect similar blocks. These techniques are robust against blurring, Noise addition and JPEG compression but cannot deal with geometric transformations. Block based approach use the algorithms such as Discrete Wavelet Transform (DWT), Principle Component Analysis [2] (PCA), Singular Value Decomposition (SVD) [3] and Discrete Cosine Transform[4] (DCT).

### 2.3 Key-Point Based Techniques

Keypoint based techniques overcome the shortcomings of block based techniques. These techniques show robustness in case of scale invariants and scan the whole image at once to extract the keypoints. After that sort the keypoints lexicographically to find the similar features. Key-point based approach use the algorithms such as SIFT and SURF [5].

## III. RELATED WORK

**A. C. Popescu et al. [6]** recommended a technique in which principal component analysis (PCA) has been performed on the overlapping square blocks.

**H. Lin et al. [7]** proposes a detection technique in which picture is separated into the squares of equivalent size, and after that element of each square is extracted and sorted. The difference of the positions of each pair neighboring elements is processed. The aggregated number of each of this distinction is computed, more gathered number means conceivable occurrence of copy area.

**L. Jing et al. [8]** proposes Scale Invariant Feature Transform (SIFT) calculation for recognizing neighborhood invariant components of image. When specified threshold value is compared with similar points and the value of similar points is greater, then image is manipulated.

**T. A. Kohale et al. [9]** propose a strategy which consolidates block based approach and feature based approach for falsification identification.

**R. A. Maind et al. [10]** propose an enhanced block based technique which compares both the methodologies viz PCA and DCT for distinguishing forgery.

As indicated by **V.S.Kulkarni et al. [11]** block based techniques give appropriate result for identification of forgery in any jpeg image but takes additional time than keypoint based strategies.

**Z. Ting et al.** [12] 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 shows robustness in case of post-image processing and has low computational complexity.

**W. Luo et al.** [13] proposed a 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.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

**S. Ryu et al.** [14] conducted a comprehensive study on copy-move forgery detection with the help of 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.** [15] utilizes Hu moments for forgery detection. Dimension will be reduced in this method by using Gaussian pyramid and divide the input image 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 on the image.

**B. Mahdian et al. [**16] utilizes blur moment invariants to represent forged image. Firstly tilt the image with blocks of particular size and represent them with blur invariants. Reduce the dimensions with the help of PCT (Principal Component Transformation). KD-tree is used for matching purpose. Further verify the similar blocks found by 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.** [17] presented the method which decreases the false negative rate. Firstly divide the image into 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.

**C. Haipeng et al.** [18] presented 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.** [19] proposed a technique that 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.

## IV. METHODOLOGY

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.

### 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-

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

flat region. Find the ratio between Keypoints and pixels for this purpose.

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

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 correlation based method.
Step 4. Based on matching features, forgery decision is taken.
End

**Fig. 3: Pseudo code for tampering detection in Non-Flat Regions**

### 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. 2.5 Post-processing

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

**Fig. 4: Pseudo code for tampering detection in Flat Regions**

### 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.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 08, August 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

## V. RESULTS AND DISCUSSION

### 5.1 Assessment Criteria

If we talk about practical applications, then there are two type of requirements in image forensics: One is to differentiate between forged and unforged region and other is to exactly locate the forged region. The proposed method fulfils both the requirements.

### 5.2 Performance Measures

The performance evaluation of a forgery detection algorithm can be done at two levels:-

- ✓ Image level, where the focus is on the ability to detect if there is a forgery.
- ✓ pixel level, where the accuracy of detecting the tampered regions

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:

$$P = \frac{Tp}{Tp+Fp} \qquad (4.1)$$

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

$$R = \frac{Tp}{Tp+Fn} \qquad (4.2)$$

This is also called True Positive Rate.

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

$$F = 2 * \frac{P*R}{(P+R)} \qquad (4.3)$$

### 5.3 Discussion of Results

The screenshots of proposed work has been shown stepwise. In figure 5 the working panel is shown in which icons for different purpose are shown stepwise. Figure 6 shows the results after the preprocessing. Figure 7 shows that the SURF algorithm is applied on every block and the features are extracted. Figure 8 shows the forgery detection results and Figure 9 shows the summarized results of the algorithm after the detection of the forgery


**Fig. 5 Working Panel**


**Fig. 6 Preprocessing**


**Fig. 7 Extraction of Features**


**Fig. 8 Detection of forgery**

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

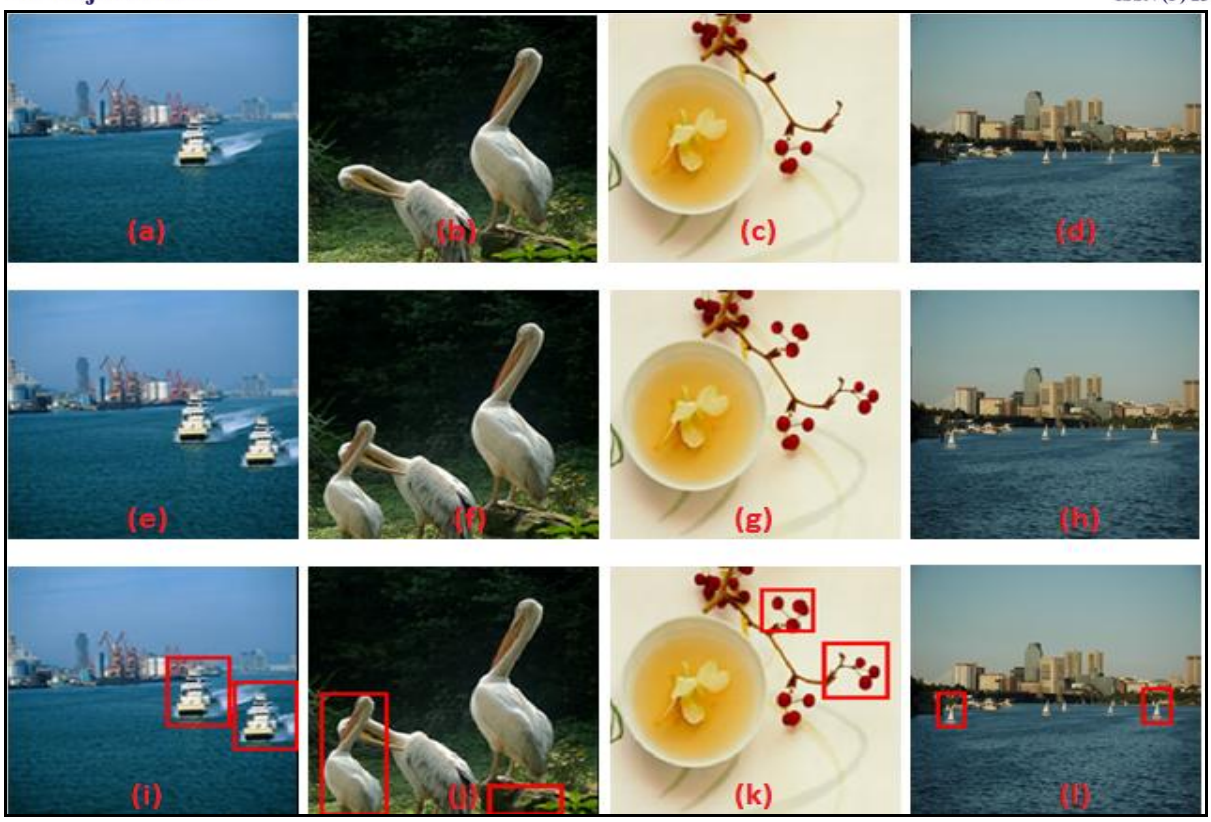



**Fig. 9 (a)(b)(c) and (d) are the original images, (e)(f)(g) and (h) are the forged images and (i)(j)(k) and (l) are the detected results**

### 5.4 Performance Results of Proposed Algorithm

| S 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 1 Performance Results of Proposed Algorithm**

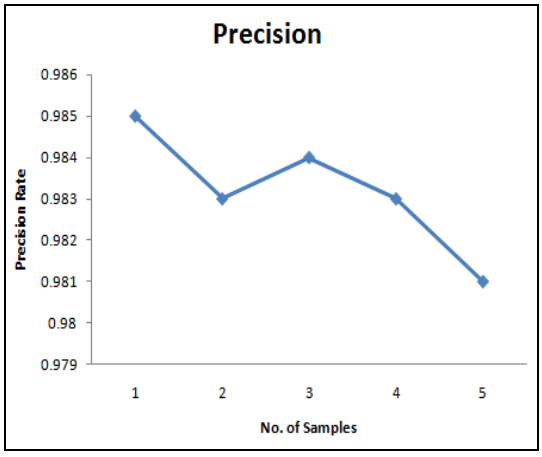



**Fig. 10 Precision of Proposed Algorithm**

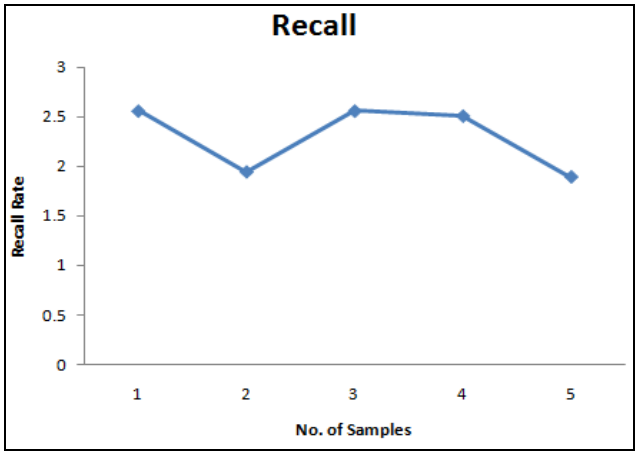



**Fig. 11: Recall of Proposed Algorithm**

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 08, August 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

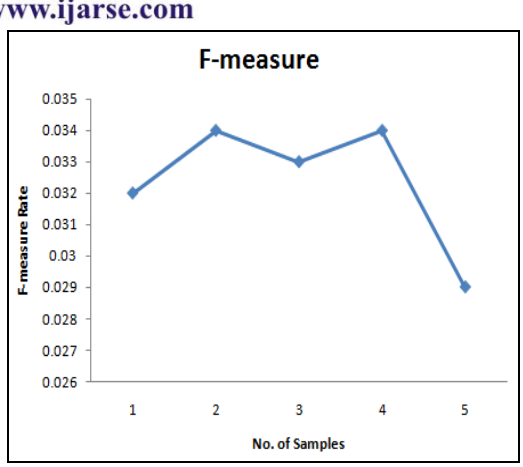



Fig. 12: F-Measure of Proposed Algorithm

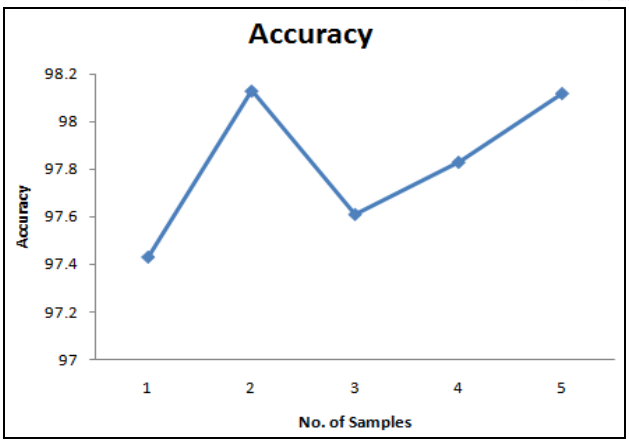


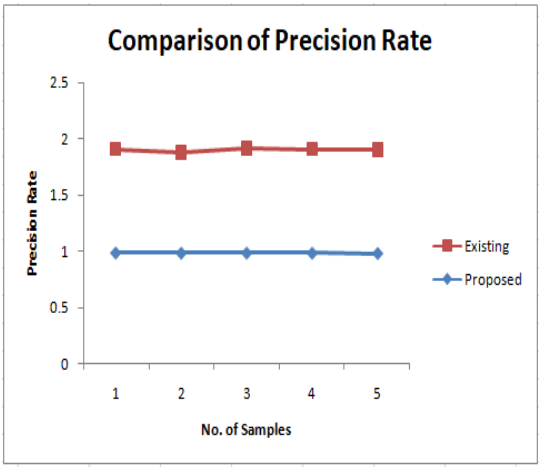

Fig. 13: Accuracy of Proposed Algorithm

### 5.5 Comparison with Existing Method

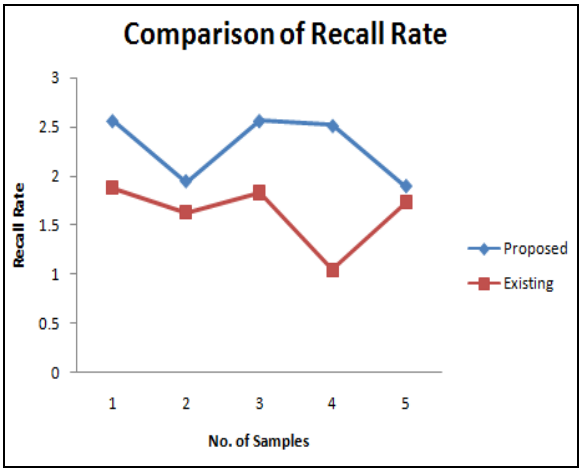
Results have been compared with the Existing technique on the basis of Precision, Recall, F-measure and Accuracy to validate the results. Different graphs have been plotted for different matrices which are shown below and the graphs will prove that our technique will outperform the existing techniques in all the four matrices but the algorithm outperforms in terms of accuracy and precision.

| S No. | Precision | | Recall | | F-measure | | Accuracy | |
|---|---|---|---|---|---|---|---|---|
| | Proposed | Existing | Proposed | Existing | Proposed | Existing | Proposed | Existing |
| 1 | 0.985 | 0.921 | 2.56 | 1.88 | 0.032 | 0.016 | 97.43 | 93.81 |
| 2 | 0.983 | 0.892 | 1.94 | 1.63 | 0.034 | 0.019 | 98.13 | 92.37 |
| 3 | 0.984 | 0.933 | 2.56 | 1.83 | 0.033 | 0.021 | 97.61 | 94.63 |
| 4 | 0.983 | 0.927 | 2.51 | 1.04 | 0.034 | 0.031 | 97.83 | 93.28 |
| 5 | 0.981 | 0.924 | 1.89 | 1.73 | 0.029 | 0.013 | 98.12 | 91.73 |

**Table 2 Table of comparison between proposed & existing work [20]**

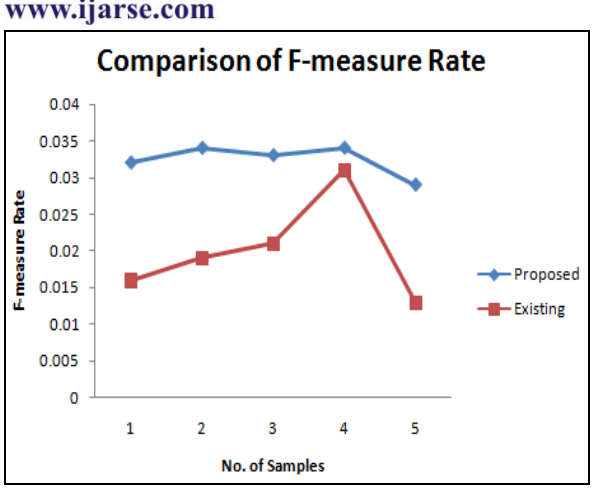


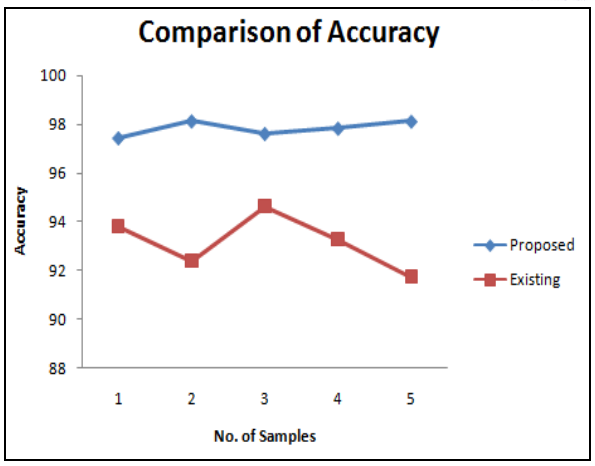

**(a)**




**(b)**

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346




**(c)** **(d)**

**Fig 13 (a) (b) (c) (d) Comparative results of Proposed and Existing Technique [20] in terms of Precision, Recall, F-measure and Accuracy**

## 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] S. Bayram, I. Avcibas , B. Sankur, N. Memon ,"Image manipulation detection," Journal of Electronic Imaging, vol. 15, no. 4, pp. 411002-411017, 2006.

[2] Y. Ke and R. Sukthankar, "PCA-sift: A more distinctive representation for local image descriptors," Computer Vision and Pattern Recognition CVPR, 2004.

[3] J. He, Z. Lin, L.Wang, and X. Tang, "Detecting doctored JPEG images via DCT coefficient analysis," European Conference on Computer Vision (ECCV), 2006.

[4] J.D. Eggerton, M..D. Srinath, "Statistical distribution of image DCT coefficients," Computer and Electrical Engineering, vol. 12, pp. 137-145, 1986.

[5] Bay H, Ess A, Tuytelaars T, and Van Gool L., "Speeded-up robust features(SURF)," Computer Vision Image Understand, vol. 110, no. 3, pp. 346-59,2008.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A.C.Popescu and H.Farid, "Exposing digital forgeries by detecting duplicated regions", Dept. of Computer Science, Dartmouth college Technical Representation,pp.2004-515,2004.

[7] H.Lin,C.Wang and Y.Kao, "An efficient method for copy-move forgery detection", International conference on applied computer and applied computational science,pp.250-253,2009.

[8] L.Jing and C.Shao,"Image copy-move forgery detection based on local invariant feature", Journal of multimedia,pp.90-97,2012.

[9] T.A.Kohale,S.D.Chede and P.R.Lakhe, "Forgery detection technique based on block and feature based method", International Journal of advanced research in computer and communication Engineering.,pp.7334-7335,2014.

[10] R.A.Maind,A.Khade and D.K.Chitre, "Image copy-move forgery detection using block representing method", International Journal of soft computing and Engineering(IJSCE),pp.49-53,2014.

[11] V.S.Kulkarni and Y.V.Chavan, "Comparison of methods for detection of copy-move forgery in digital images", InternationalJournal of Engineering science and Tech.,2014.

[12] Z.Ting, W. Rang-ding, "Copy-Move Forgery Detection based on SVD in Digital Image", Eighth conference on image and Signal Processing , 2009.

[13] 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.

[14] 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.

[15] 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.

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

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

[18] 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.

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

[20] 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.