# Detection of forgery region by using the adaptive over-segmentation and feature point extraction matching

**Betha Yugandhar (M.Tech Scholar) [1]**
**G.Rama Krishna (Assistant Professor) [2]**
Sana Engineering College, Kodad, Suryapet, District-508206, TELANGANA, INDIA
yugandharbetha@gamil.com[1] sanam8.ece@gmail.com[2]

**Abstract---** ***The invention of the internet has introduced the unimaginable growth and developments in the renowned research fields such as medicine, satellite imagery, image processing, security, biometrics, and genetics. The algorithms implemented in the 21$^{st}$ century has made the human life more comfortable and secure, but the security to the original documents belongs to the authenticated person is remained as concerned in the digital image processing domain. A new study is proposed in this research paper to detect the forgery detection in accurate manner using the adaptive over-segmentation and feature point matching. The integration of the block-based and key point-based forgery detection methods is the key idea in the proposed study and the detection of the suspected regions are detected by the adaptive non-overlapping and irregular blocks and this process is carried out using the adaptive over-segmentation algorithm. The extraction of the feature points is performed by performing the matching between the each block and its features. The feature points are gradually replaced by using the super pixels in the proposed Forgery Region Extraction algorithm and then merges the neighboring blocks that have similar local color features into the feature blocks to generate the merged regions; finally, it applies the morphological operation to the merged regions to generate the detected forgery regions. The proposed forgery detection algorithm achieves much better detection results even under various challenging conditions the earlier methods in all aspects.***

***Keywords:*** *Copy-move, Forgery detection, the adaptive over-segmentation, feature point matching, neighboring blocks, super pixels, feature points.*

## 1. INTRODUCTION

The digital image processing is the prominent research domain in the 21$^{st}$ century where its presence is clearly observed in various fields. The digital image processing is a important constituent of the electromagnetic spectrum and the security field remain as one of the major research areas on which lot of research needs to be done to secure the privacy and the confidential information with greater robustness. The forgery has become the major concerned area in the 21$^{st}$ and a lot of research is carried out in the literature but still achieving the desired results remained as unsolved issue. The digital images are considered as the primary source of the medium used for too meet the very purpose which includes the data transmission, the data compression, the data hiding and the various other applicative research areas. The forgery of the images has reach to the new level to pose serious issues in the 21$^{st}$ century and it creates the situation where the difference between the forged and non forged documents identification become the biggest drawback, which is addressed in efficient way using the proposed work.

Image forgery performance is easy nowadays. One of the most famous manipulations on digital image is copy-move forgery, in which we have to copy the particular region and paste it to another part of the same image. In literature we saw that so many forgery detection techniques are developed to copy–move forgery detection. Fridrich et al.proposed forgery detection technique in which input image is segmented into overlapped rectangular blocks to find tampered regions with the help of Discrete Cosine Transform (DCT) coefficient. Luo et al. for block feature we used RGB colour components as well as direction information in this technique. Li et al in this to get image feature we used two methods namely Discrete Wavelet Transform (DWT) and Singular Value Decomposition(SVD). Mahdian and Saic in this paper for feature extraction 24 blur-invariant moments are considered. Bayram et al. to get the feature, transform technique used is Fourier-Mellin Transform (FMT). Wang et al. to get the Block features , considerations of mean intensity with different radii are considered. Ryu et al. to get block features there is consideration of Zernike moments. RavoSolorio and Nandi to get block features there is consideration of Information Entropy. I. Amerini, L. Ballan to get block features there is consideration of Scale Invariant Feature Transform (SIFT). There are two existing methods for forgery detection, one is block based which work on input image to divide it into two regions as regular region , overlapping region and then it matches with the image pixels to get forged regions or their transform is taken for processing. Another is key point based forgery detection in which there is duplicate region detection.

These methods are common in use for forgery detection, but they are having following drawbacks: 1) There is very high computational complexity as there is division of image into overlapped regions. 2) To deal with the geometrical transformation of the forgery area is difficult. 3) There is a low recall rate due to host image division in regular blocks.

To address the shortcomings of the prevailing methods, we tend to propose a unique copy-move forgery detection scheme exploitation adjustive over-segmentation and have purpose matching during this paper. The adjustive Over-Segmentation algorithm is projected to adaptively divide the host image into non-overlapping and irregular blocks. Then the feature points are extracted from every block and matched with every other to seek out the tagged feature points which might approximately indicate the suspected forgery regions. And finally the tagged feature points are processed and also the morphological operation is applied to get the detected forgery regions.

## 2. Types of Digital Image Forgery

Fake images have become widespread in society today. Therefore, the tampering images are common in scandal, controversies. One can find forged images used to sensationalize news, spread political propaganda and rumors, introduce psychological. As the credibility of images suffers, it is necessary to devise techniques in order to verify their genuineness and trustworthiness of images.

The forgeries are classified into five major categories: image retouching, Image Splicing, Copy-Move (cloning), Morphing, Enhanced. The first type is image retouching, where the method is used for enhances an image or reduces certain feature of an image and enhances the image quality for capturing the reader's attention. In this method, the professional image editors change the background, fill some attractive colors, and work with hue saturation for toning and balancing. The second type is image splicing where the different elements from multiple images are juxtapose in a single image to convey an idea.

Copymove forgeries are usually detected by searching for matching regions in the image, although recent research has taken a more feature-based approach, concentrating on matching features (as in object detection) rather than blocks, in order to allow for various image transformations that can be used to create more convincing forgeries. The forth type is Morphing and in this type the image and video can be exposed into unique influence ,were the one object on image is turned into to another object in the other image. The morphing is used to transfer the one-person image from another person image by using seamless transition between two images.

Table 1: Types of Digital Image Forgery

| **Types** | **Detail** | **Appearance** |
|---|---|---|
| Image retouching, | An example of forgery where the original image and a forged image shows the difference [19]. |  |
| Image Splicing, | In these images some parts of image copy from base image like shark. The base image (helicopter rescue) first turns over horizontally and the shark image is pasted to make new forged image. The forged image is not splicing with the original helicopter rescue image [20]. |  |
| Copy Move (cloning), | The images shows the copy-move attack and in left side image three rockets and in The forged image contains four rockets [21]. |  |
| Morphing, | The left and right images are original the middle image is - morphing image [19]. |  |
| Enhanced | The original image is upper right side and after that enhanced image with color change, after perform blur on background, finally original image (lower right)Current. |  |

# 3. LITERATURE SURVEY

### 3.1 Detecting Duplicated Image

A technique that works by 1st applying principal element analysis to little mounted - size image blocks to yield a reduced dimension illustration was planned by Alin C Popescu et al. (2004). Whereas performing arts the on top of technique we are able to realize some duplicate pictures (noises). Then the duplicate regions are detected by lexicographically (the follow of aggregation dictionaries).Sorting the whole image blocks. This can be terribly wonderful and actual appropriate technique to yield a reduced dimension illustration. It’s sensitive to jpeg lossy compression and additionally it's additive to noise.

### 3.2 Fast Copy-Move Forgery Detection

A methodology to discover copy- move forgery by dividing the image into overlapping blocks of equal size, extracting feature for every block and representing it as a vector and typing all the extracted feature vectors victimization the base sort, was planned by Hwei-jen sculpture et.al (2009). Base type dramatically reduces the time complexness and also the adopted options enhance the aptitude of resisting of varied attacks like JPEG compression and mathematician noise. Each potency and high detection rates are incontestable.

### 3.3 Robust Copy-move Forgery

Sevinc Bayram et al.(2009) projected to use Fourier-Mellin Transform (FMT) options that square measure invariant to scaling and translation. A replacement detection scheme that creates use of investigation bloom filters is additionally introduced by them. It detects copy move forgery terribly accurately albeit the cast image is turned, scaled or extremely compressed. This detection scheme improves the potency. However the hardiness of the tactic is reduced.

### 3.4 Detection Digital Images Using SURF

B.L.Shivakumar et al. (2011)proposed a method to detect duplication regions. Because one of the common image forgery methods is copy move forgery (CMF). Identification of the CMF can be detected by the duplication regions using Speeded Up Robust Features (SURF) keypoints. These SURF keypoints are extracted from images. The duplication region can be detected with different sizes. The result shows that CMF with minimum false match for images with high resolution. A few small copied regions were not successfully detected.

### 3.5 A Sift-based Forensic Method

Irene Amerini et al. (2011) proposed a method to support image forgery detection based on SIFT algorithm. Thus, the algorithm is used to detect the regions which are duplicated and determine the geometric transformation applied to perform such tampering. But, the main drawbacks of this technique, it is unable to detect the image with uniform texture and salient keypoints.

### 3.6 Exposing Transform-invariant Features

Pravin Kakar et al. (2012) has proposed a method based on transforming-invariant features. These got y utilizing the features from MPEG-7 image signature devices.This method achieved good results, accuracy and extremely low false positives. Thus, these features are invariant to common image processing operations. This method cannot detect regions which have undergone affine transformations and/or multiply copied.

# 4. PROPOSED METHOD

The forgery detection has been gaining the attention from the years because of its sheer importance in the real time scenario. The adaptive over segmentation algorithm and the feature point matching scheme are used in the proposed study for the effective detection of the image forgery and its framework is accomplished as follows and its illustration is described in the Fig.1.

- The segmentation of the host image into non-overlapping and irregular blocks is the key process in the proposed study, which is carried out by using the adaptive over-segmentation method and the segmented blocks are called as image blocks (IB).
- The irregular block segmentation is followed by the Scale Invariant Feature Transform (SIFT)

technique, where it is applied to the each segmented block to extract the block features (BF) in a reliable way.

- The suspected forgery regions indication is the another important aspect of the proposed study, which is obtained by performing the matching between the block features with one another and the matched feature points are termed as the Labeled Feature Points (LFP) which is further used as reference for forgery region detection. Finally, we propose the Forgery Region Extraction method to detect the forgery region from the host image according to the extracted LFP. I.

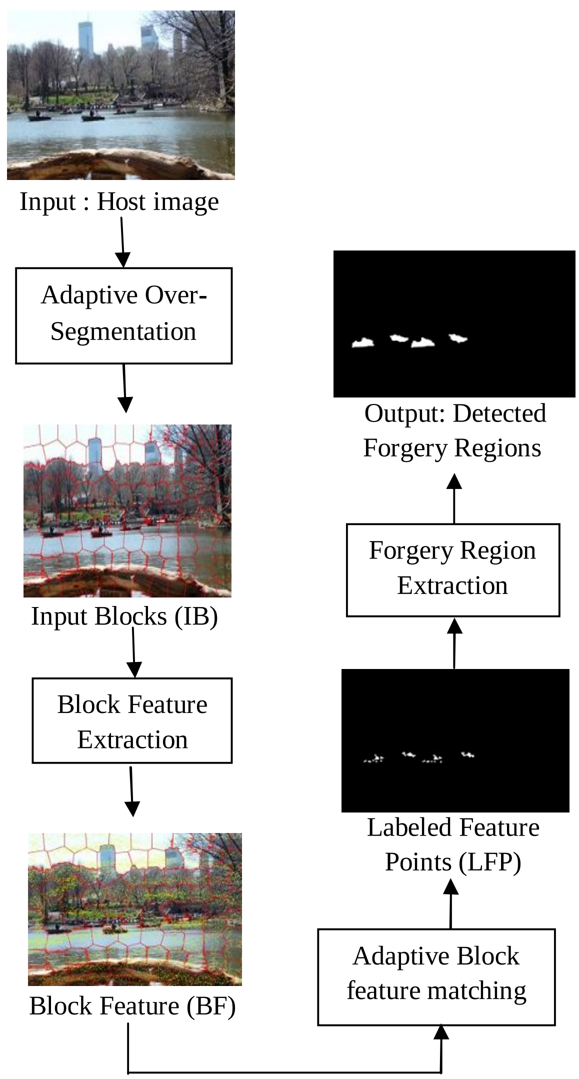



Fig.1: The proposed copy-move forgery detection scheme framework

### A. Adaptive over segmentation algorithm

The Adaptive Over-Segmentation algorithm, which is similar to when the size of the host images increases, the matching computation of the overlapping blocks will be much more expensive. To address these problems, we proposed the Adaptive Over-segmentation method, which can segment the host image into non-overlapping regions of irregular shape as image blocks afterward, the forgery regions can be detected by matching those non-overlapping and irregular regions. Segmentation method, the non-overlapping segmentation can decrease the computational expenses compared with the overlapping blocking; furthermore, in most cases, the irregular and meaningful regions can represent the forgery region better than the regular blocks. However, the initial size of the super pixels in SLIC is difficult to decide. In practical applications of copy-move forgery detection, the host images and the copy-move regions are of different sizes and have different content, and in our forgery detection method, different initial sizes of the super pixels can produce different forgery detection results; consequently, different host images should be blocked into super pixels of different initial sizes, which is highly related to the forgery detection results.

We have performed a large number of experiments to seek the relationship between the frequency distribution of the host images and the initial size of the superpixels to obtain good forgery detection results. We performed a four-level DWT, using the ‘Haar’ wavelet, on the host image; then, the low-frequency energy $E_{LF}$ and high-frequency energy $E_{HF}$ can be calculated using (1) and (2), respectively. With the low-frequency energy $E_{LF}$ and high-frequency energy $E_{HF}$ , we can calculate the percentage of the low-frequency distribution $P_{LF}$ using (3), according to which the initial size S of the superpixels can be defined as in (4)

$$E_{LF} = \sum |CA_4| \qquad (1)$$

$$E_{HF} = \sum_i \left( \sum |CD_i| + \sum |CH_i| + \sum |CV_i| \right), i = 1,2,\dots,4 \qquad (2)$$

$$P_{LF} = \frac{E_{LF}}{E_{LF} + E_{HF}} \,.\, 100\% \qquad (3)$$

$$S = \begin{cases} \sqrt{0.02 \times M \times N} & P_{LF} > 50\% \\ \sqrt{0.01 \times M \times N} & P_{LF} \leq 50\% \end{cases} \qquad (4)$$

where S means the initial size of the superpixels; M × N indicates the size of the host image; and $P_{LF}$ means the percentage of the low-frequency distribution

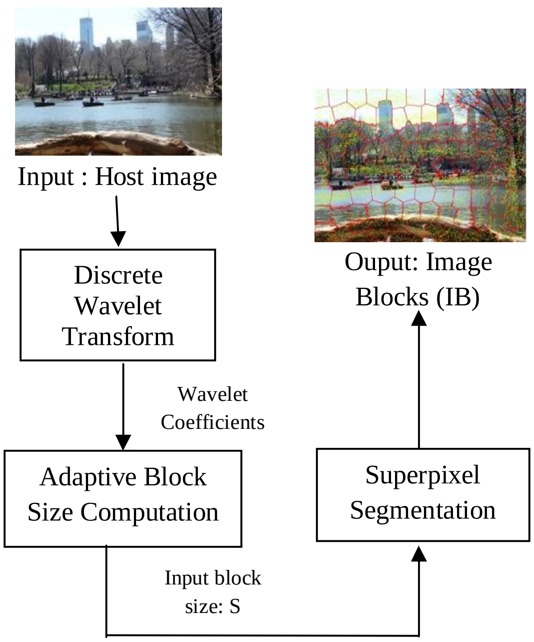



Fig.2: The adaptive over-segmentation flowchart

the proposed Adaptive Over-Segmentation method can divide the host image into blocks with adaptive initial sizes according to the given host images, with which each image can be determined to be an appropriate block initial size to enhance the forgery detection results.

### B. Block Feature Extraction Algorithm

After the host image is segmented into image blocks, block features are extracted from the image blocks (IB). The traditional block-based forgery detection methods extracted features of the same length as the block features or directly used the pixels of the image block as the block features. However, these features reflect mainly the content of the image blocks, leaving out the location information. Also, these features are not resistant to various image transformations. Therefore, in this project, the feature points are extracted from each image block as block features and the feature points should be robust to various distortions, such as image scaling, rotation, and JPEG compression. The feature point extraction methods, SIFT and SURF have been widely used. The feature points generated using these methods are robust against common image processing operations such as rotation, scale, blurring, and compression. Experiments have shown that the results obtained using SIFT are more constant and have better performance compared to other feature extraction methods. Hence, in this project SIFT is used for feature point extraction. Therefore, each block feature contains irregular block region information and the extracted SIFT feature points.

### C. Block Feature Matching Algorithm

In most of the existing block-based methods, the block matching process outputs a specific block pair only if there are many other matching pairs in the same mutual position, assuming that they have the same shift vector. When the shift vector exceeds a user-specified threshold, the matched blocks that contributed to that specific shift vector are identified as regions that might have been copied and moved. In our algorithm, because the block feature is composed of a set of feature points, we proposed a different method to locate the matched blocks.

**Algorithm: Block Feature Matching algorithm**

**Input:** Block Features (BF);
**Output:** Labeled Feature Points (LFP).
**STEP-1:** Load the Block Features BF ={BF1,BF2, ,BFN....., }where N means the number of image blocks; and calculate the correlation coefficients CC of the image blocks.
**STEP-2:** Calculate the block matching threshold BTR according to the distribution of correlation coefficients.
**STEP-3:** Locate the matched blocks MB according to the block matching threshold B TR .
**STEP-4:** Label the matched feature points in the matched blocks MB to indicate the suspected forgery regions.

### D. Forgery Region Extraction Algorithm

Once the labelled feature points (LFP) are extracted, there is a need to locate the forgery regions also. Since, this extracted LFP's are only the locations of the forgery regions. A Forgery Region Extraction algorithm is used to detect the forged regions more accurately. To obtain the suspected regions (SR), a method by replacing the LFP with the small super pixels is proposed. This is done by segmenting the host image very well as small superpixels. The local color features of the super-pixels that are neighbors of the suspected regions (SR) are also measured to improve the precision and recall rates.

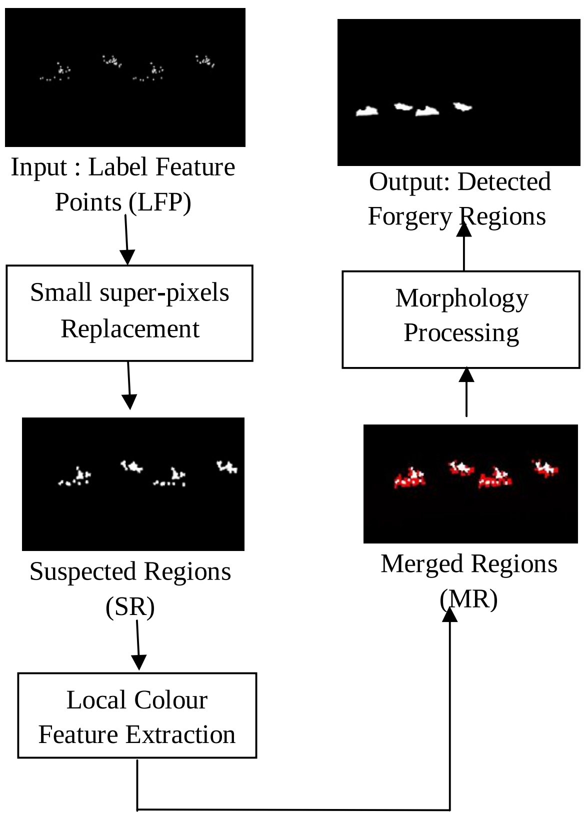



Fig. 3: Flow chart of the Forgery Region Extraction algorithm

When this local color feature is same as that of the suspected regions, then the neighbor super pixels are merged into the corresponding suspected regions. This merging process results in merged regions (MR). Finally, to generate the detected copy-move forgery regions, morphological operation is applied to this merged region. Fig.4 shows the flowchart of the Forgery Region Extraction Algorithm.

**Algorithm: Forgery Region Extraction**
**STEP-1:** Load the Labeled Feature Points (LFP), apply the SLIC algorithm with the initial size S to the host image to segment it into small superpixels as feature blocks, and replace each labeled feature point with its corresponding feature block, thus generating the Suspected Regions (SR).
**STEP-2:** Measure the local color feature of the superpixels neighbor to the SR, called neighbor blocks; when their color feature is similar to that of the suspected regions, we merge the neighbor blocks into the corresponding SR, therefore creating the merged regions (MR).
**STEP-3:** Apply the morphological close operation into MR to finally generate the detected forgery regions.

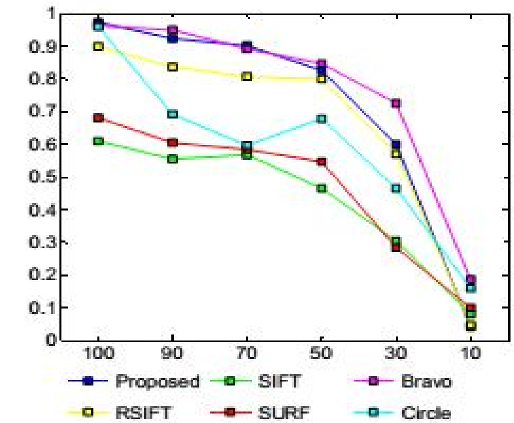
## 5. EXPERIMENTAL RESULTS

**1) Down sampling:** Total 48 forged host images are present in the dataset. These images are scaled down from 90% to 10% in steps of 20%. So here we have to test the total of 48×5=240 images.

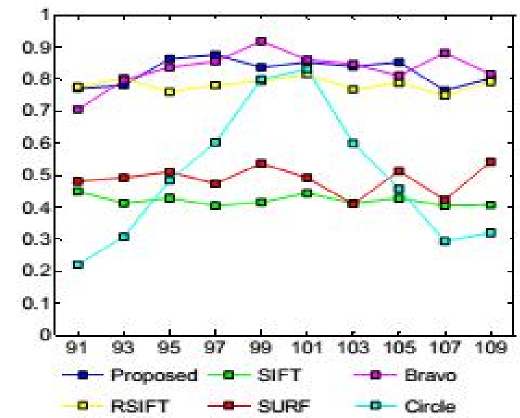
**2) Scaling:** The regions which are copied are scaled by using the scale factor varying from 91% to 109% in steps of 2%, and the scale factor is about 50%, 80%, 120%, and 200%. As well. So here we have to test the total of 48×14=672 images.

**3) Rotation:** the regions which are copied are rotated by the rotated angle varying from 2º to 10º, in steps of 2º,and the rotation angles are about 20º, 60º and 180º as well. So here we have to test the total of 48×8=384 images.

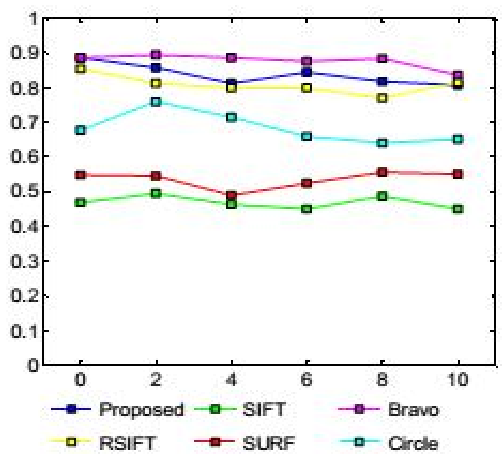
**4) JPEG compression:** the JPEG compressed images are the forgery images. The compression can be with a quality factor varying from 100 to 20,in steps of -10. So here we have to test the total of 48×9=432 images



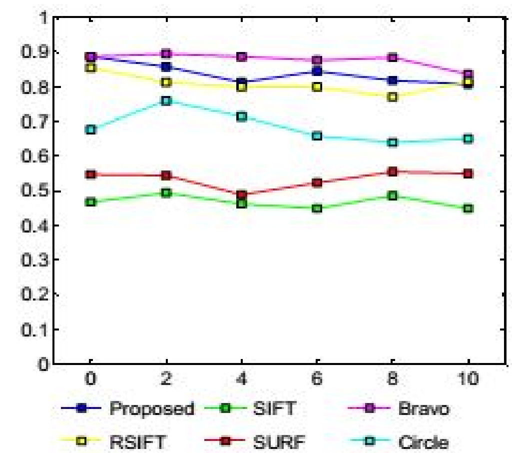
(a) Down - Sampling



(b) Scaling

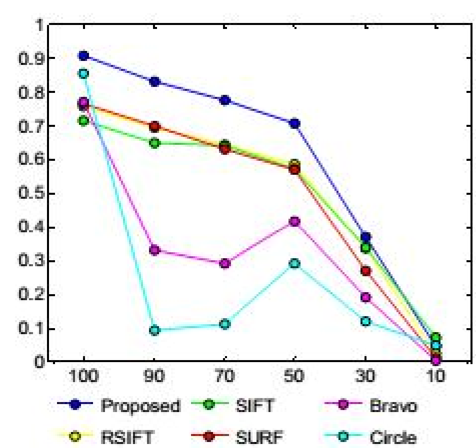


(c) Rotation

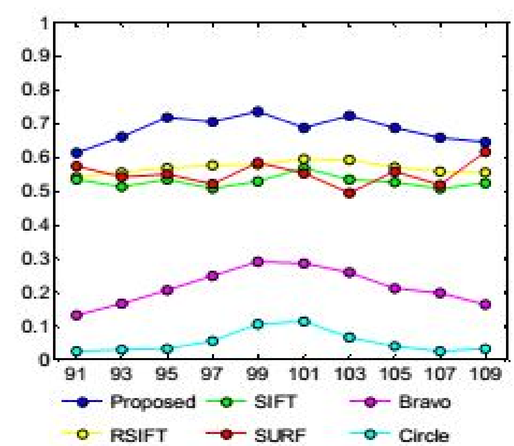


(d) JPEG-Compression

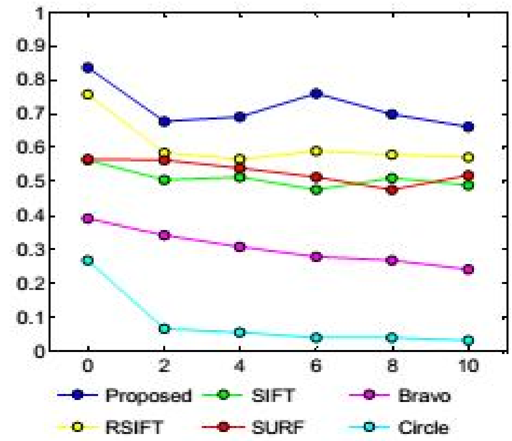
Fig. 4: Precision results at the pixel level (a) Down-sampling; (b) Scaling; (c) Rotation; and (d) JPEG Compression



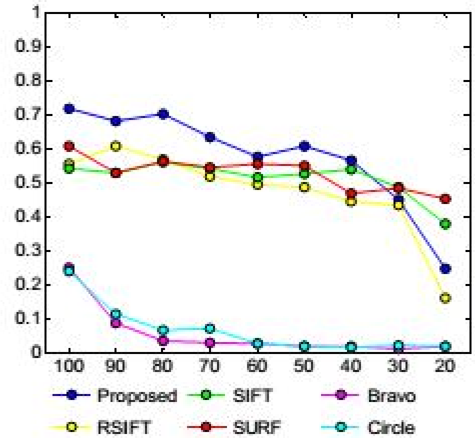
(a) Down - Sampling



(b) Scaling

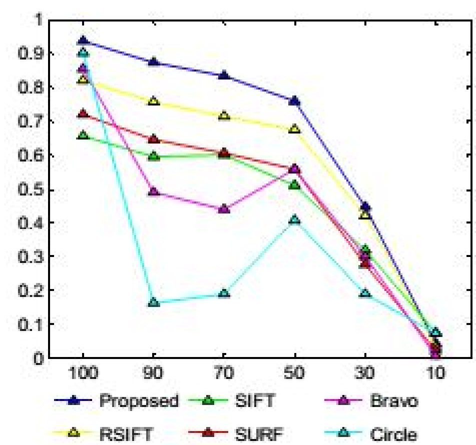



(c) Rotation

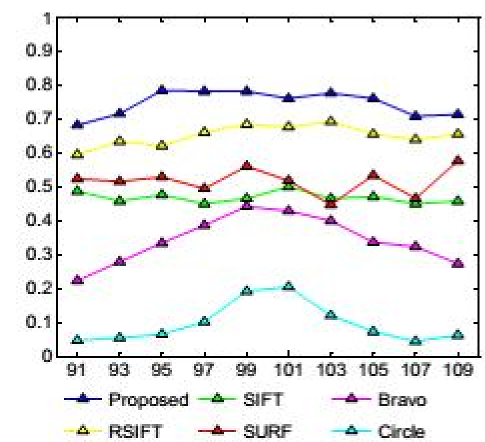



(d) JPEG-Compression

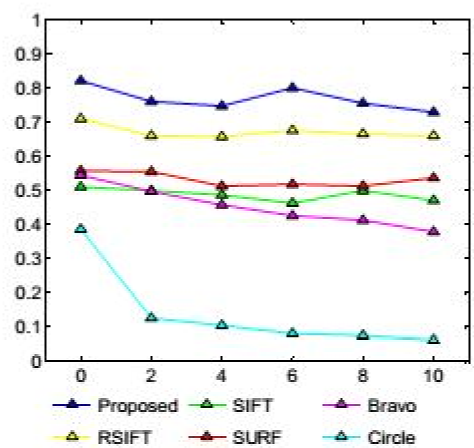
Fig. 5: Recall results at the pixel level (a) Down-sampling; (b) Scale; (c) Rotation; and (d) JPEG Compression



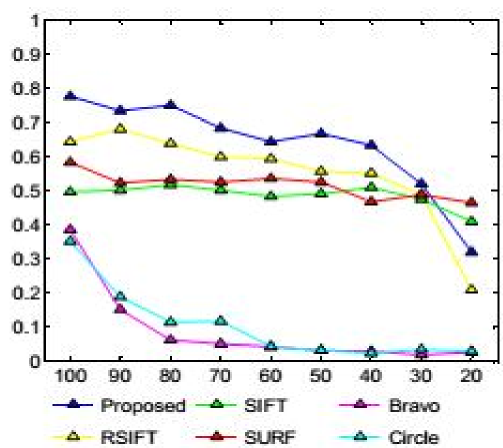

(a) Down - Sampling




(b) Scaling




(c) Rotation




(d) JPEG-Compression

Fig. 6: $F_1$ scores at the pixel level (a) Down-sampling; (b) Scale; (c) Rotation; and (d) JPEG Compression

## 6. Conclusion

This work proposes for Image forgery detection using adaptive over segmentation and feature point matching. In forgery detection method proposes block based and key points integrates scheme, first the proposed adaptive over segmentation algorithm segments the host image into non overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, and the forgery region extraction algorithm, which replaces the feature points with small super pixels as feature blocks and then merges the neigh boring blocks that have similar local color features into the feature blocks to generate the merged regions.

## References

[1] Q.-C. Yang And C.-L. Huang, "Copymove Forgery Detection In Digital Image," In Advances In Multimedia Information Processing-Pcm 2009, Ed: Springer, 2009, Pp. 816-825.
[2] B. Mahdian And S. Saic, "Blind Methods For Detecting Image Fakery," Ieee Aerospace And Electronic Systems Magazine, Vol. 25, Pp. 18-24, 2010.
[3] B. Shivakumar And L. D. S. Santhosh Baboo, "Detecting Copy-Move Forgery In Digital Images: A Survey And Analysis Of Current Methods," Global Journal Of Computer Science And Technology, Vol. 10, 2010.
[4] K. N. Qureshi And A. H. Abdullah, "A Survey On Intelligent Transportation Systems," Middle East Journal Of Scientific Research, Vol. 15, 2013.
[5] W. Lu, W. Sun, J.-W. Huang, And H.-T. Lu, "Digital Image Forensics Using Statistical Features And Neural Network Classifier," In Machine Learning And Cybernetics, 2008 International Conference On, 2008, Pp. 2831-2834.
[6] S. Bayram, B. Sankur, N. Memon, And İ. Avcibaş, "Image Manipulation Detection," Journal Of Electronic Imaging, Vol. 15, Pp. 041102-041102-17, 2006.
[7] A. C. Popescu And H. Farid, "Exposing Digital Forgeries By Detecting Traces Of Resampling," Signal Processing, Ieee Transactions On, Vol. 53, Pp. 758-767, 2005.
[8] A. E. Dirik, S. Bayram, H. T. Sencar, And N. Memon, "New Features To Identify Computer Generated Images," In Image Processing, 2007. Icip 2007. Ieee International Conference On, 2007, Pp. Iv-433-Iv-436.
[9] M. Kharrazi, H. T. Sencar, And N. Memon, "Blind Source Camera Identification," In Image Processing, 2004. Icip'04. 2004 International Conference On, 2004, Pp. 709-712.
[10] M.-J. Tsai And G.-H. Wu, "Using Image Features To Identify Camera Sources," In Acoustics, Speech And Signal Processing, 2006. Icassp 2006 Proceedings. 2006 Ieee International Conference On, 2006, Pp. Ii-Ii.
[11] M.-J. Tsai And C.-S. Wang, "Adaptive Feature Selection For Digital Camera Source Identification," In Circuits And Systems, 2008. Iscas 2008. Ieee International Symposium On, 2008, Pp. 412-415.
[12] Y. Sutcu, S. Bayram, H. T. Sencar, And N. Memon, "Improvements On Sensor Noise Based Source Camera Identification," In Multimedia And Expo, 2007 Ieee International Conference On, 2007, Pp. 24-27. [13] R. Bausvs And A. Kriukovas, "Digital Signature Approach For Image Authentication," Electronics & Electrical Engineering, 2008.
[14] T. Chen, J. Wang, And Y. Zhou, "Combined Digital Signature And Digital Watermark Scheme For Image Authentication," In Info-Tech And Info-Net, 2001. Proceedings. Icii 2001-Beijing. 2001 International Conferences On, 2001, Pp. 78-82.
[15] X. Zhou, X. Duan, And D. Wang, "A Semifragile Watermark Scheme For Image Authentication," In Multimedia Modelling Conference, 2004. Proceedings. 10th International, 2004, Pp. 374-377.
[16] M. Sridevi, C. Mala, And S. Sanyam, "Comparative Study Of Image Forgery And Copy-Move Techniques," In Advances In Computer Science, Engineering & Applications, Ed: Springer, 2012, Pp. 715-723.
[17] S. Rawat And B. Raman, "A Chaotic System Based Fragile Watermarking Scheme For Image Tamper Detection," Aeu-International Journal Of

Electronics And Communications, Vol. 65, Pp. 840-847, 2011.

[18] M. Kirchner And R. Bohme, "Hiding Traces Of Resampling In Digital Images," Information Forensics And Security, Ieee Transactions On, Vol. 3, Pp. 582-592, 2008.

[19] H. Shah, P. Shinde, And J. Kukreja, "Retouching Detection And Steganalysis," Ijeir, Vol. 2, Pp. 487- 490, 2013.

[20] R. Granty, T. Aditya, And S. Madhu, "Survey On Passive Methods Of Image Tampering Detection," In Communication And Computational Intelligence (Incocci), 2010 International Conference On, 2010, Pp. 431-436.

[21] M. Sridevi, C. Mala, And S. Sandeep, "Copy–Move Image Forgery Detection In A Parallel Environment," 2012.

[22] W. Luo, J. Huang, And G. Qiu, "Robust Detection Of Region-Duplication Forgery In Digital Image," In Pattern Recognition, 2006. Icpr 2006. 18th International Conference On, 2006, Pp. 746-749.

[23] J. Wang, G. Liu, H. Li, Y. Dai, And Z. Wang, "Detection Of Image Region Duplication Forgery Using Model With Circle Block," In Multimedia Information Networking And Security, 2009. Mines'09. International Conference On, 2009, Pp. 25-29.

[24] N. D. Wandji, S. Xingming, And M. F. Kue, "Detection Of Copy-Move Forgery In Digital Images Based On Dct," International Journal Of Computer Science Issues (Ijcsi), Vol. 10, 2013.

[25] S. Bayram, H. T. Sencar, And N. Memon, "An Efficient And Robust Method For Detecting Copy-Move Forgery," In Acoustics, Speech And Signal Processing, 2009. Icassp 2009. Ieee International Conference On, 2009, Pp. 1053-1056