International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Analysis of Digital Image Forgery Detection using Adaptive Over-Segmentation Based on Feature Point Extraction and Matching

Ch. SUDARSHAN[1], U. SATHISH KUMAR[2]

[1](M.Tech.) Dept of CSE,Acharya Nagarjuna University, Guntur, AP, (522510), INDIA
[2]Assistant Professor (,M.Tech,(Ph.d)), Dept of CSE,Acharya Nagarjuna University, Guntur, AP, (522510), INDIA

Abstract--- *The innovation of the web has presented the unimaginable development and improvements in the prestigious research fields, for example, pharmaceutical, satellite symbolism, picture handling, security, biometrics, and genetics. The methods introduced in the 21st century has made the human life more comfortable and secure, however the security to the original reports has a place with the verified individual is stayed as worried in the digital image processing area. In this paper, two methods are proposed to detect the forged region of an image such as Adaptive over-segmentation and feature point matching. Thus Adaptive over-segmentation is used to extract the features by both block-based and key point-based forgery detection methods. Firstly, the host image is segmented into non-overlapping and irregular blocks adaptively. Then these block as compared to extract the feature points of a host image; this procedure can approximately indicate the suspected forgery regions. To trace out the forged region efficiently, the forgery region extraction algorithm is used to replaces the features point with the super pixels as feature blocks and then merges the neighboring blocks that have similar local color features into the feature block to generate the merged region this merged region is processed into morphological operation to detect the extracted forged regions in an image. In cut-paste image forgery detection, image forensic techniques are used to detect the global and local contrast enhancement, identifying the use of histogram equalization.*

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 21st 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 21st 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 21st 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.

Copy-move forgery, which is to paste one or several copied region of an image into other part of the same image. During the copy and move operations, some image processing methods such as rotation, scaling, blurring, compression, and noise addition are occasionally applied to make convincing forgeries. Earlier blocked based forgery detection was used to detect forged image but this algorithm faced some drawbacks such as the host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases and it was less efficient as it take more time to be process. To avoid such drawbacks along with the blocked based forgery, we proposed an image-blocking method called Adaptive Over-Segmentation that divided the host image into non overlapping blocks adaptively with the help of two algorithm those are Simple Linear Iterative Clustering (SLIC) to segment the host image into irregular blocks and Discrete Wavelength Transform (DWT) which is employed to analyze the frequencies of the super pixel. Further the image block formed are pass to the Block Feature Extraction method where the block feature are extracted by using Scale Invariant Feature Transform (SIFT) as it possessed constant and better performance compared with the other extraction method. Further the process of Block Feature Matching is carried out which used Simple Linear Iterative Clustering (SLIC) for calculating super pixel and Discrete Wavelength Transform for finding super pixel from one block and

checking other for other blocks. When the features are extracted and matched then we get to know which regions the host image has been forged.

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 adaptive over-segmentation and have purpose matching during this paper. The adaptive 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

Now day's fake images have become more in society. Tampering images are common for making controversies. For example, it can be used for sensational news, spread political news and rumors. As the quality of pictures suffers, it's necessary to plot techniques so as to verify their genuineness and trait of pictures.

Picture sterilization is characterized as "adding, changing, or deleting some vital options from a picture while not exploit any obvious trace. There are totally different techniques used for formation a picture. Taking under consideration the ways wont to create cast pictures, digital image forgery are often isolated into 3 primary classifications: Copy-Move forgery, Image splice, and Image resampling.

A. Copy-Move Forgery

In copy move forgery, in original image some part of the image with any size is copies and pasted in that only in some area of image it can be show in figure1. As the copied part originated from the same image, its essential properties such as noise, color and texture don't change and make the recognition process troublesome.

B. Image Forgery using Splicing

Image splicing uses cut-and-paste systems from one or a lot of pictures to make another pretend image. once conjunction is performed exactly, the borders between the spliced regions will visually be unbearable. Splicing, however, disturbs the high order Fourier statistics. These insights will so be utilized as a locality of identifying phony. Figure 2, demonstrates an honest sample of image conjunction during which images the photographs the images of the shark and also the eggbeater ar unified into one picture.

Fig 1. (a) original Image (i) ; (b) copy Image (ii); (c) forged image

C. Image Resampling

To make associate astounding fake image, some elite regions got to undergo geometric transformations like rotation, scaling, stretching, skewing, flipping and then forth. The interpolation step plays a vital role within the resampling method and introduces non-negligible applied mathematics changes. Resampling introduces specific periodic correlations into the image. These correlations are often utilized to acknowledge phony caused by resampling. In Figure three, the image on the left is that the original image whereas the one on the proper is that the cast image obtained by rotation and scaling it.

Fig 2. (a) The real image (b) final result of image retouching

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

For the forgery detection process lot of importance is given from the past years. In this paper adaptive over segmentation and feature point matching methods are used to detect the forgery region. The overall overview of this method is explained in the Fig.1.

- Adaptive over-segmentation method is used to segment the host image. The image is divided into non-overlapping and irregular blocks. The segmented blocks are called as image blocks (IB).
- The irregular block segmentation can be done by the Scale Invariant Feature Transform (SIFT) technique, SIFT is applied to each block to get the perfect block features (BF).

- The main important parameter of the proposed method is detecting the suspected forgery region, it can be detected by performing the matching between block features with one another. The block features which are matched are named as Labeled Feature Points (LFP). The LFP will plays a major role in detecting the forgery because it is used as a reference. In the final forgery region extraction method is proposed to detect the forgery region from the host image.

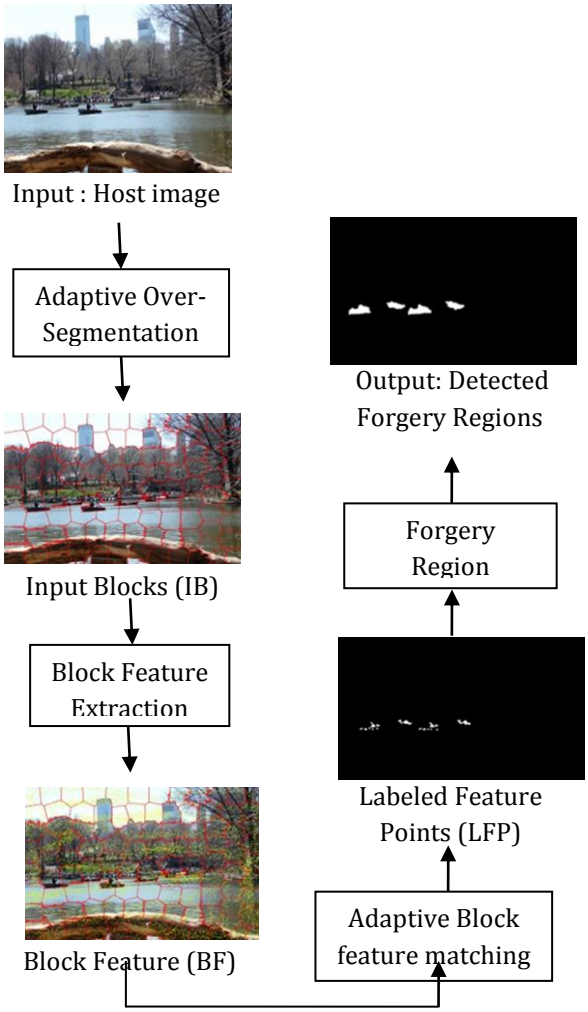


Fig.3: The proposed copy-move forgery detection scheme framework

A. Adaptive over segmentation algorithm

When the size of the host image is increased the matching computation of the overlapping blocks will become difficult. To overcome this problem we are implementing adaptive over segmentation. By using this method the image is divided into non-overlapping and irregular regions called as image blocks. The use of non-overlapping segmentation compared to the overlapping method is to reducing the computational complexity and compared to the regular blocks irregular blocks can give the better performance like we can find the more forgery region. In the process of this method finding the initial size of the super pixels in SLIC method is very difficult. Basically in the copy-move forgery detection the sizes and content will be different when it is compared with the host images. In the proposed method different superpixels sizes will produce different forgery results.

To get the relationship between the frequency distribution of host images and the initial size of the superpixels a large number of experiments are performed. By using the haar wavelet 4-level DWT technique is applied to the host image then the image I divided into the low-frequency energy E_{LF} and high-frequency energy E_{HF} can be calculated using (1) and (2), respectively. The percentage of the low-frequency distribution P_{LF} in (3) can be calculated by using the low-frequency E_{LF} and high-frequency energy E_{HF}. The initial size of the superpixels can be defined in (4)

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

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

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

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

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

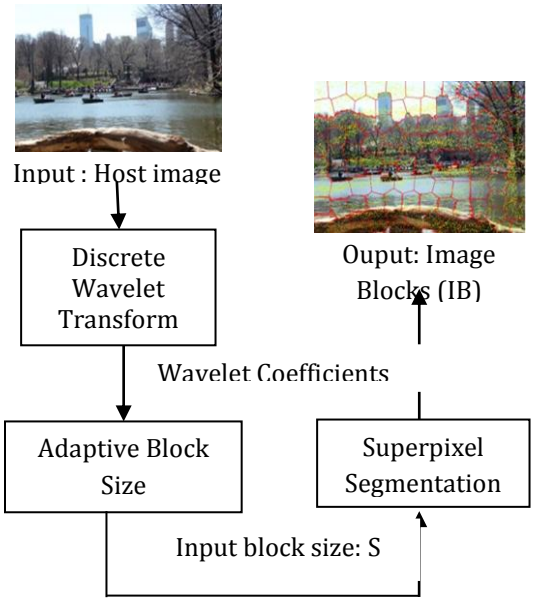


Fig.4: The adaptive over-segmentation flowchart.

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

In the adaptive over segmentation the host image is divided into image blocks after that the block features are extracted from the image blocks by using the block feature extraction algorithm. The image block content is mainly affected by these feature extraction and these features are non-resistance to the various image transformation techniques. So in this method the feature points are extracted from the each image block as block features and these are not affected by image scaling, rotation, and JPEG compression. The main feature point extraction methods which are used in this proposed method are SIFT and SURF. Compared to the previous techniques this method is robust. When the experiment results are compared SIFT will give better performance compared to the other feature extraction methods. So in this every block will contain the irregular block region information and the extracted SIFT feature points.

C. Block Feature Matching Algorithm

In the existing system if there are so many other matching pairs in one mutual position then only the block matching process will give the specific block pair as a output and if there are same shift vectors then the threshold value is calculated then the matched blocks are which specified to the same shift vector are identified as the regions of copied or moved. In the proposed algorithm we are considering the block features which consist of different feature points so a different method is used to locate these matched blocks.

Algorithm: Block Feature Matching algorithm

Input: Block Features (BF);
Output: Labeled Feature Points (LFP).
STEP-1:.After generating blocks load the features of blocksBF={BF1,BF2,….BFN} where N is denoted as number of image blocks. And find correlation between the blocks.
STEP-2: By distribution correlation coefficient TRb is calculated for block matching threshold.
STEP-3: With help of TRb threshold matched blocks (MB)are located.
STEP-4: suspected forgery regions are indicated in the matched blocks (MB) by labeling the matched features points.

D. Forgery Region Extraction Algorithm

After gathering the LFP (labeled feature points) then we have to locate the forgery region. The extracted LFP regions are taken as the forgery regions. To get the more accuracy of the forgery region forgery region algorithm is used. The LFP region is replaced with the small super pixels to get the suspected regions (SR). The superpixels are segmented from the host image. To get the more precision and recall rates the LFP of the super pixels that are neighbors of the suspected regions (SR) are also measured.

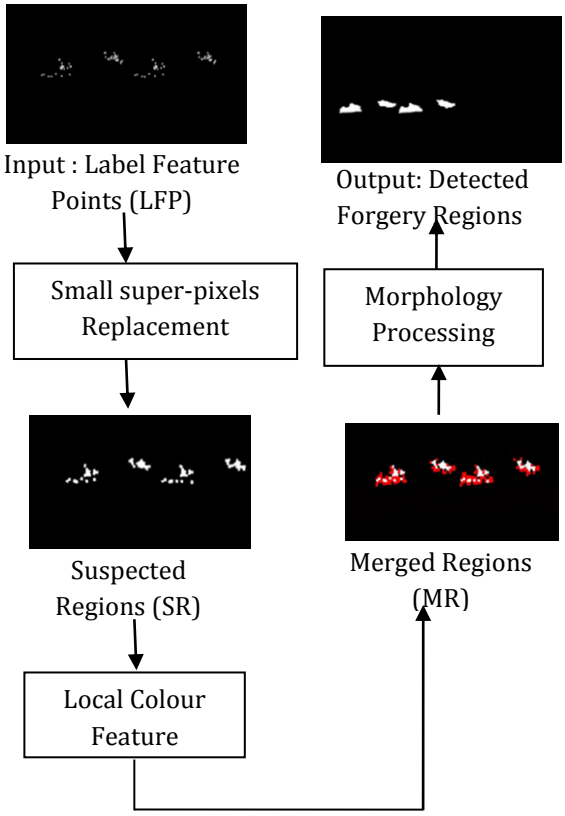


Fig. 5: Flow chart of the Forgery Region Extraction algorithm

If the LFP is same as suspected regions then the super pixels which are neighbor are merged into the corresponding suspected region. These results are considered as the merged regions (MR). the final step is detecting the copy-move forgery regions this step was done by applying morphological operations on the merged regions. The final flowchart of the forgery region extraction algorithm is shown in fig.4

Algorithm: Forgery Region Extraction

STEP-1: Load the Labeled Feature Points (LFP), apply the SLIC calculation with the underlying size S to the host picture to section it into small superpixels as highlight squares, and supplant each named include point with its relating highlight piece, in this manner producing 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) 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.

2) 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.

3) Scaling or Noise: 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.

4) Median filter: 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.

In this section, a series of experiments square measure conducted to evaluate the effectiveness and lustiness of the planned image forgery detection theme exploitation adaptive over-segmentation and have purpose matching. Within the following experiments, the image dataset in [22] is employed to check the proposed methodology. This dataset is made supported forty eight high-resolution uncompressed PNG true color pictures, and the average size of the pictures is 1500*1500. within the dataset, the copied regions square measure from the classes of living, nature, man-made and mixed, and that they vary from to a fault swish to highly textured; the copy-move forgeries square measure created by copying, scaling and rotating semantically substantive image regions.

Fig 6: original image

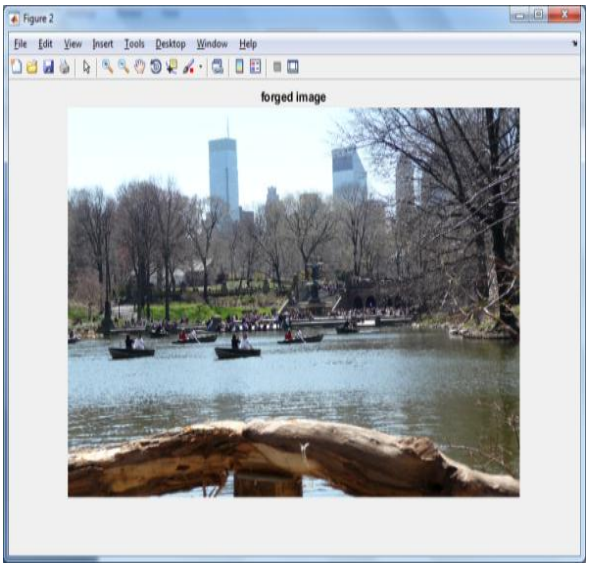


Fig 7: forged image

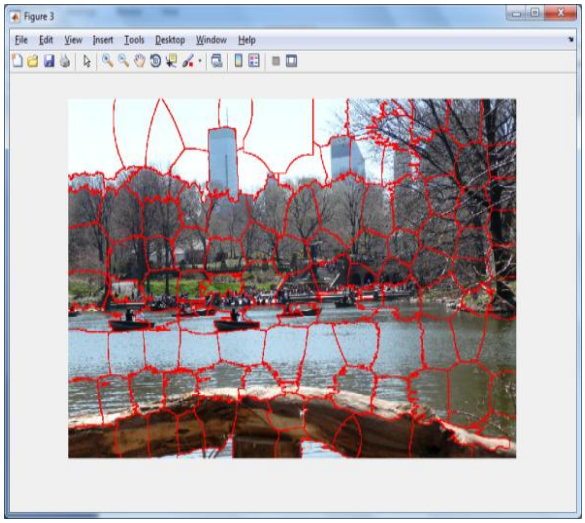


Fig 8: Adaptive over segmentation

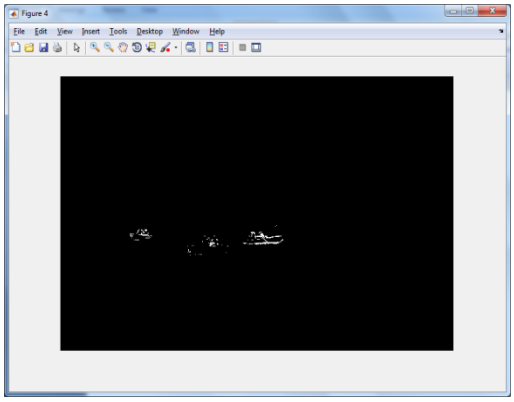


Fig 9: label feature points

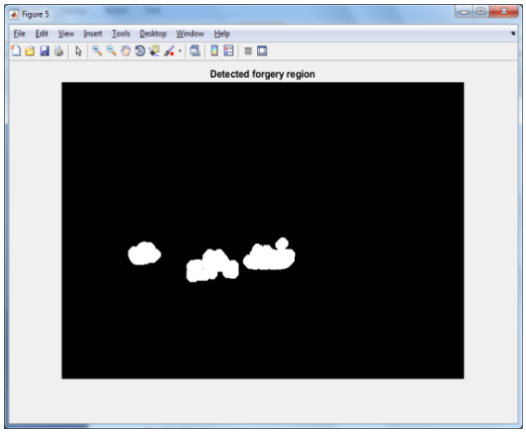


Fig 10: Morphed detected forgery region

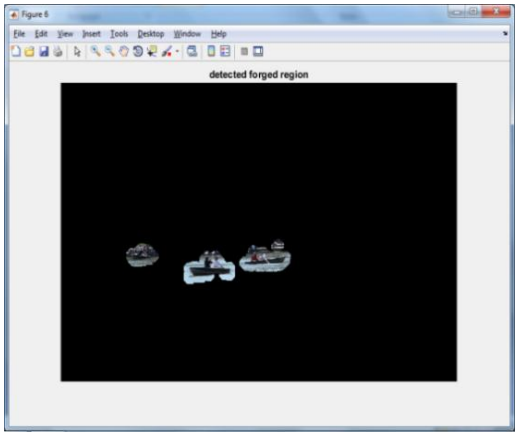
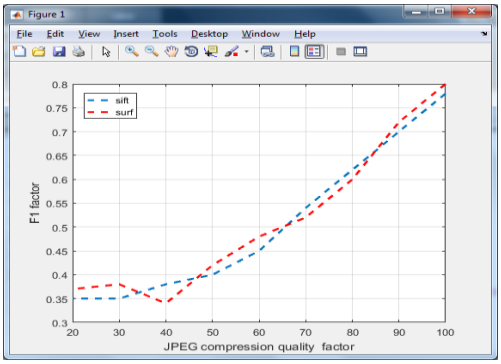
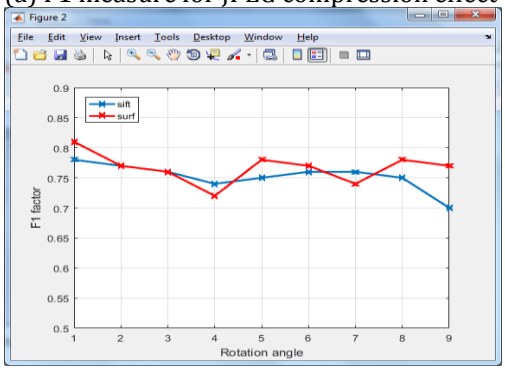


Fig 11: final detected forged region.

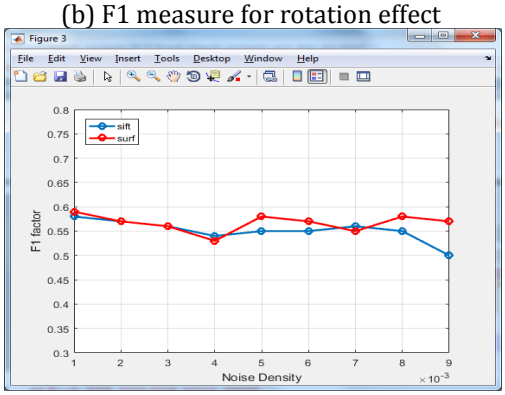
Fig 12: Analysis of F1 Measure (a) JPEG Compression, (b) Rotation, (c) Noise Scale and (d) Median filter.



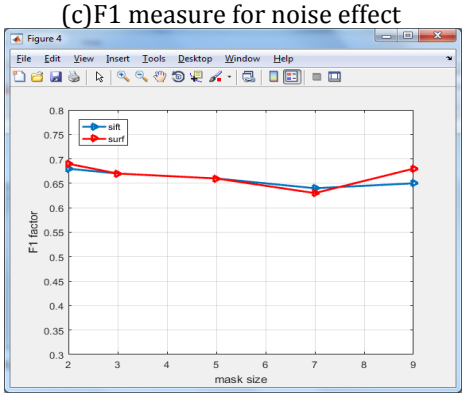
(a) F1 measure for JPEG compression effect



(b) F1 measure for rotation effect

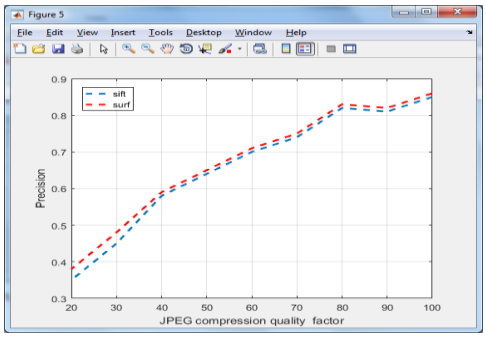


(c)F1 measure for noise effect

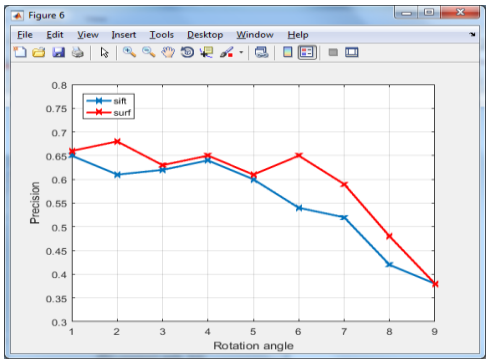


(d) F1 measure for median filter effect

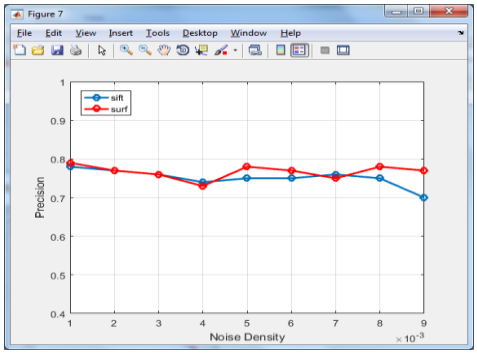
Fig 13: Analysis of Precision and Recall at the pixel level (a) JPEG Compression, (b) Rotation, (c) Noise Scale and (d) Median filter.



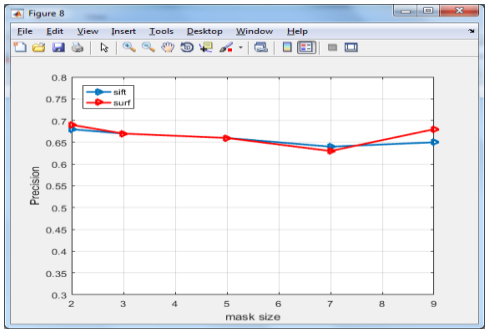
(a)JPEG compression effect



(b) Rotation effect



(c) Noise effect.



(d)Median filter effect.

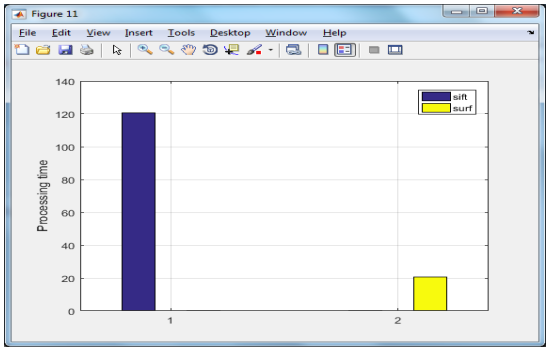


Fig 8: Processing time SIFT and SURF

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

[13] T. Chen, J. Wang, And Y. Zhou, "Combined Digital Signature And Digital Watermark Scheme For Image Authentication," In Info-Tech And Info- yesrNet, 2001. Proceedings. Icii 2001-Beijing. 2001 International Conferences On, 2001, Pp. 78-82.

BIOGRAPHIES

Ch. SUDARSHAN received the Bachelor of Technology degree in Computer Science engineering from Rajive Gandhi university of Knowledge and Technology in 2015. Currently pursuing M.tech in Computer Science Engineering from Acharya Nagarjuna University. His areas of interest include in computer science engineering specialized in image processing and Data mining.

Mr. U.SATHISH KUMAR is currently working as assistant professor in Acharya Nagarjuna University from last 3 years. Currently he is pursuing his Ph.D degree. His research interest includes in Computer Science and Engineering in Data mining, image processing and Soft computing.