International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue14
November 2017

# Advanced Adaptive Over-Segmentation and Feature Point Matching For Image Forgery Detection

A Raghu Vardhan Babu
raghu.ammananna@gmail.com

## Abstract

*Image forgery means manipulation of digital image to conceal meaningful information of the image. The detection of forged image is driven by the need of authenticity and to maintain integrity of the image. A copy–move forgery detection theme victimization adaptive over segmentation and have purpose feature matching is proposed. The proposed scheme integrates both block-based and key point-based forgery detection methods. 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, we propose the forgery region extraction algorithm which replaces the features point with small super pixels as feature blocks and them merges the neighboring blocks that have similar local color features into the feature block to generate the merged regions. Finally, it applies the morphological operation to merged regions to generate the detected forgery regions. In cut-paste image forgery detection, proposed digital image forensic techniques capable of detecting global and local contrast enhancement, identifying the use of histogram equalization.*

***Key words**: Copy-move forgery detection; Adaptive over-segmentation; Feature point matching and extraction; Cut-paste forgery detection.*

## I. INTRODUCTION

The world is getting advanced day by day as the technology is growing rapidly. According to the type of wish he needed, human develops different software's. Hence likewise now many image editing software are available. Using these tools the images get edited. This editing may have a positive face as well as a negative face. The negative face may cause for a human life itself. Now different editing tools are available that can edit the image in any way as they wish. Many morphological operations can be occurred in an image. it can be used as a misleading tool for hiding facts and evidences. This is because today digital images can be manipulated in such perfection that forgery cannot be detected visually. In fact, the security concern of digital content has arisen a long time ago and different techniques for validating the integrity of digital images have been developed. In the fields such as forensics, medical imaging, e-commerce, and industrial photography, authenticity and integrity of digital images is essential. In medical field physicians and researchers make diagnoses based on imaging. The introduction and rapid spread of digital manipulation to still and moving images raises ethical issues of truth, deception, and digital image integrity. With professionals challenging the ethical boundaries of truth, it creates a potential loss of public trust in digital media. This motivates the need for detection tools that are transparent to tampering and can tell whether an image has been tampered just by inspecting the tampered image. Image tampering is a digital art which needs understanding of image properties and good visual creativity. One tampers images for various reasons either to enjoy fun of digital works creating incredible photos or to produce false evidence. No matter whatever the cause of act might be, the forger should use a single or a combination series of image processing operations. These manipulations in an image are a serious issue regarding the authenticity, integrity, and reliability of the image.

## II. FORGERY TECHNIQUES

More and more researchers have begun to focus on the problem of digital image tampering. Of the existing types of image tampering, a common manipulation of a digital image is copy-move forgery.

**Copy-move forgery:** which is to paste one or several copied region(s) of an image into other part(s) 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. Because the copy and move parts are copied from the same image, the noise component, color character and other important properties are compatible with the remainder of the image; some of the forgery detection methods that are based on the related image properties are not applicable in this case.

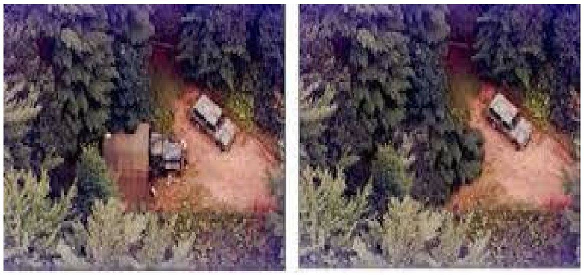

Fig.1. Left is the original, right is the tampered image.

Fig. 1 shows an example of copy-move forgery where the leaves are duplicated to hide a vehicle from the image. Because the copy and move parts are from the same image, the noise component, color character and other properties are compatible with the remainder of the image. Some of the forgery detection methods that are based on the related image properties are not applicable in this case.

**Image-splicing** It is defined as a paste-up produced by sticking together photographic images. Splicing is a technique which involves composite of two or more images to create a new fake image.

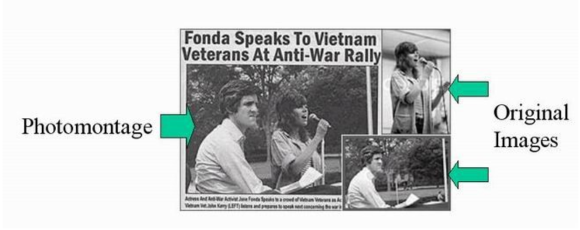

Fig.2. Example of splicing

**Resize** This operation performs a geometric transformation which can be used to shrink or enlarge the size of an image or part of an image. Image reduction is performed by interpolating between pixel values in local neighborhoods. Cropping It is a technique to cut-off borders of an image or reduces the canvas on which an image is displayed. Generally this kind of operation is used to remove border information which is not very important for display.

**Noising or Blurring** Tampering images with operations described above like image splicing, scaling, rotating can be clear to a viewer in the form of artifacts like improper edges, aliasing defects and tone variations. These obvious traces of tampering can be made imperceptible by applying small amount of noise or blur operations in the portions where the tampering defects are visible. This project focuses on copy-move forgery that can be done very easily by using the tools such as Cloning in Photoshop. In this type of tampering, portions of an image are copied and pasted in other portions of the same image to conceal a person or object in the scene.

## III. LITERATURE SURVEY

Amruta Jagtap et al [1] this paper Proposes a Verifying the integrity of images and detecting traces of tampering without requiring extra prior knowledge of the image content or any embedded watermarks is an important research field. An attempt is made to survey the recent developments in the field of digital image forgery detection. And a novel copy–move forgery detection scheme using adaptive over-segmentation and feature point matching. Also it explained the scheme integrates both block-based and key point-based forgery detection methods. 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, we propose the forgery region extraction algorithm, which replaces the feature points.

with small super pixels as feature blocks 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.

A. J. Fridrich et al [2] described to the existing methods, the copy-move forgery detection methods can be categorized into two main categories: block-based algorithms and feature key point-based algorithms. This work comes under block-based forgery detection methods. The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. And proposed a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions.

Sree lakshmi M. et al [3] proposes for a Method Image features in an image can be added up or removed, without leaving any obvious traces in the image. Thus the method called forensic detection is used to detect such manipulations occurred in an image by recovering the history of an image. Here recovers the history of filtered JPEG image using an effective linear classifier that discriminates the forensic image with its trained data. Copy- move forgery is a type of image forgery where a portion of image gets copied and pasted at another location of the same image, which cannot be detected by naked eye. The method to detect such forgery is to initially segment the image using adaptive block segmentation and features are extracted from each image blocks and compare each blocks to one another to found out the match. Label the matched points to extract the forged region. Hence forged region is detected.

Musaed Alhussein et al [4] the image tampering includes both splicing and copy-move forgery. First, the image was decomposed into three color channels (one luminance and two Chroma), and each channel was divided into nonoverlapping blocks. Local textures in the form of local binary pattern (LBP) were extracted from each block. The histograms of the patterns of all the blocks were concatenated to form a feature vector. The feature vector was then fed to an ELM for classification. The ELM is a powerful and fast classification approach. The experiment was performed using two publicly available databases. The experimental results showed that the proposed method achieved high detection accuracy in both the databases.

H. Huang, W. Guo, and Y. Zhang[5] Key point-based methods An alternative to the block-based methods, keypoint-based forgery detection methods are proposed, where image keypoints are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. Two methods have been applied to achieve this, namely, the Scale-Invariant Feature transform (SIFT) and the Speeded Up Robust Fetures (SURF). SIFT is applied to host images to extract feature points, which are then match to one another. When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points are defined as the forgery region. SURF is also applied to extract image feature instead of SIFT. Though these methods locate matched key points, most of them cannot detect forgery regions very well and therefore, the detection results are not so satisfactory and also the recall rate is low. Most of the block based forgery detection methods have similar framework, the difference being the method employed to extract the block features. Although these methods are effective they have three drawbacks. First, as the host image is divided into overlapping regular blocks, they become computationally expensive with increase in image size. Secondly, these methods cannot address significant geometrical transformations of the forged regions. Thirdly, their recall rate is low, since the blocking method is of regular shape. The keypoint based methods overcome the first two drawbacks, they reduce computational complexity and also successfully detect forgeries even when there are geometrical transformations, but the recall rate is very poor in these methods.

B.L.Shivakumar et al. (2011) [6] proposed a method that detects the duplication region using SURF key points which are extracted from the images. It detects duplication region with different size. The result shows that the proposed method can detect copy-move forgery with minimum false match for images with high resolution. A few small copied regions were not successfully detected.

Radhakrishna Achanta et al. (2012) [7] have proposed a in-depth performance analysis of modern superpixel techniques. They performed an empirical comparison of five state-of-the-art algorithms. In addition, it proposed a new method for generating super pixels based on k-means clustering, SLIC, which has been shown to outperform existing super pixel methods. SLIC adheres to boundaries as well as or better than previous methods. At the same time, it is faster and more memory efficient, improves segmentation performance

## IV. PROPOSED METHOD

This paper proposes, a novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching. The proposed scheme integrates both the traditional block-based forgery detection methods and key point based forgery detection methods. Similar to block-based forgery detection methods, we propose an image-blocking method called the Adaptive Over-Segmentation algorithm to divide the host image into non-overlapping and irregular blocks adaptively. Then, similar to the key point-based forgery detection methods, the feature points are extracted from each image block as block features instead of being extracted from the whole host image as in the traditional key point base methods. Subsequently, the block features are matched with one another to locate the labeled feature points, which can approximately indicate the suspected forgery regions. To detect more accurate forgery regions, we proposed the Forgery Region Extraction algorithm, which replaces the feature points with small super pixels as feature blocks and, then, merges the neighboring blocks with similar local color features into feature blocks, to generate the merged regions; finally, it applies a morphological operation into the merged regions to generate the detected forgery regions.

Adaptive over segmentation divide the image into non-overlapping and irregular blocks. The latter extracts feature points from each block as block features and the block features are matched with one another to locate labeled feature points. This approximately determines the forgery regions. proposed a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions. The RGB color components and direction information as block features. As an alternative to the block-based methods, key point based forgery detection methods were proposed, where image key points are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. The Scale-Invariant Feature Transform (SIFT) was applied to the host images to extract feature points , which were then one another.

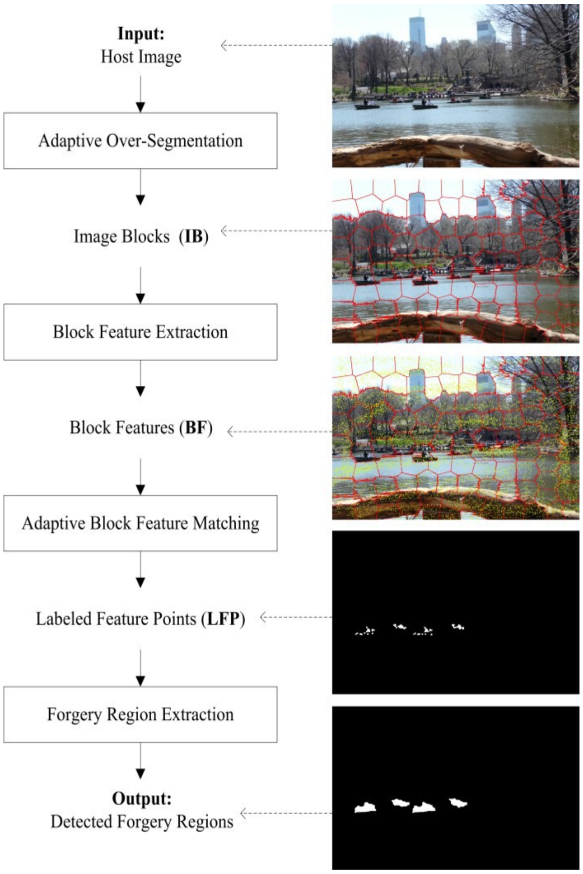
Input:
Host Image
Adaptive Over-Segmentation
Image Blocks (IB)
Block Feature Extraction
Block Features (BF)
Adaptive Block Feature Matching
Labeled Feature Points (LFP)
Forgery Region Extraction
Output:
Detected Forgery Regions

Fig.3. Framework of the proposed copy-move forgery detection scheme.

**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.

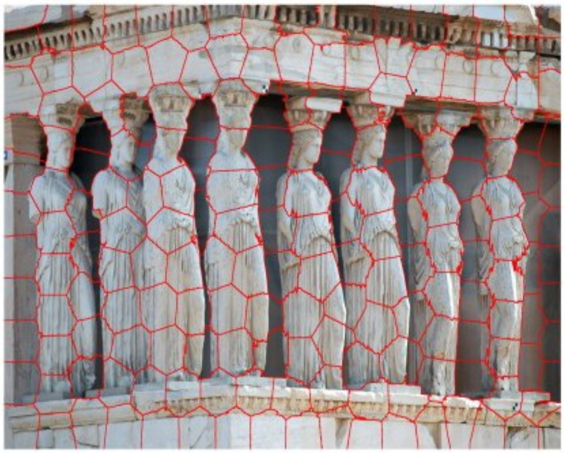

Fig.4. Non-overlapping and irregular blocking.

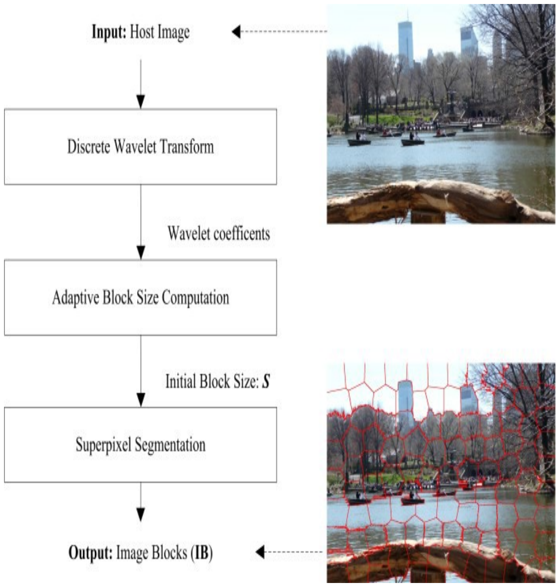
Input: Host Image
Discrete Wavelet Transform
Wavelet coefficents
Adaptive Block Size Computation
Initial Block Size: S
Superpixel Segmentation
Output: Image Blocks (IB)

Fig.5. Flowchart of the Adaptive Over-Segmentation algorithm.

In summary, the flow chart of the proposed Adaptive Over-Segmentation method is shown in Fig.5. First, we employed the DWT to the host image to obtain the coefficients of the low- and high-frequency sub-bands of the host image. Then, we calculated the percentage of the low-frequency distribution, according to which we determined the initial size *S*, using. Finally, we employed the SLIC segmentation algorithm together with the calculated initial size *S* to segment the host image to obtain the image blocks (IB). LF P

**Block Feature Extraction** 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.

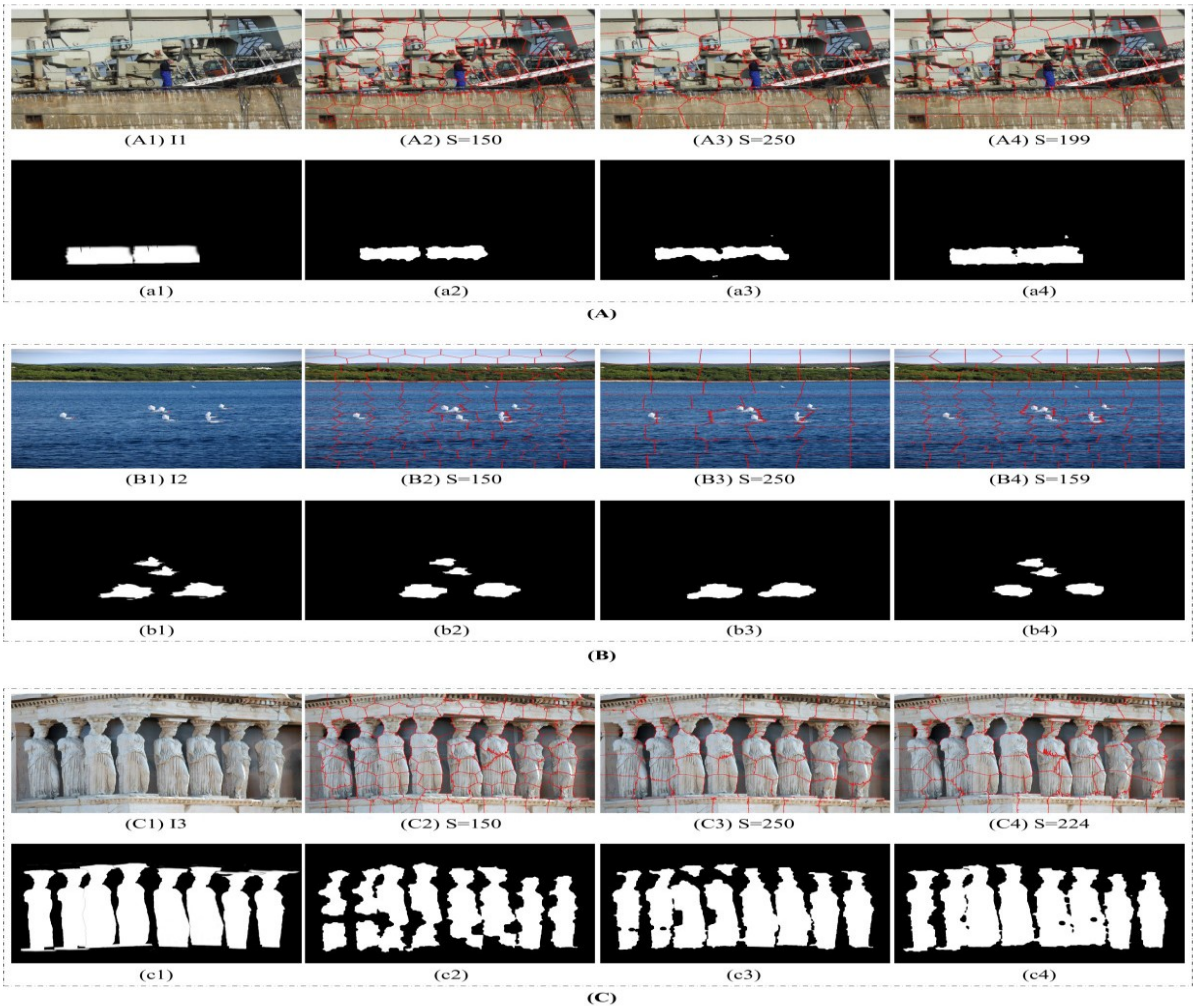

Fig.6. Superpixels of different initial sizes and the corresponding forgery detection results (A1), (B1), and (C1).

The copy-move host images, I1, I2 and I3; (a1), (b1),(c1) The corresponding forgery regions of I1, I2 and I3, respectively. (A2), (B2), (C2) The host images are blocked into superpixels with initial size $S$=150; (a2),(b2), (c2) The corresponding detected forgery regions when $S$ =150 .
(A3), (B3), (C3) The host images are blocked into superpixels with initial size $S$=250 ; (a3),(b3), (c3) The corresponding detected forgery regions when $S$=250 .
(A4), (B4), (C4) The host images are blocked into superpixels with the proposed Adaptive Over-segmentation method, by which the initial superpixel sizes are calculated as , S=199,S=159, and ,S=224 respectively; (a4), (b4), (c4) The corresponding detected forgery regions with the proposed Adaptive Over-segmentation method.

**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. The detailed steps are explained as follows. Algorithm: Block Feature matching algorithm Input: Block Features (BF); Output: Labeled Feature Points (LFP).

STEP-1: Load the Block Features BF ={BF1,BF2,... 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.

**Forgery Region Extraction Algorithm**

Although we have extracted the labeled feature points (LFP), which are only the locations of the forgery regions, we must still locate the forgery regions. Considering that the super pixels can segment the host image very well, we proposed a method by replacing the LFP with small super pixels to obtain the suspected regions (SR), which are combinations of labeled small super pixels. Furthermore, to improve the precision and recall results, we measure the local color feature of the super pixels that are neighbors to the suspected regions (SR); if their color feature is similar to that of the suspected regions, then we merge the neighbor super pixels into the corresponding suspected regions, which generates the merged regions (MR). Finally, a close morphological operation is applied to the merged regions to generate the detected copy-move forgery regions. Fig. 6 shows the flow chart of the Forgery Region Extraction algorithm, which is explained in detail as follows.

**Algorithm: Forgery Region Extraction**

**Input:** Labeled Feature Points (LFP)
**Output:** Detected Forgery Regions.
**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 super pixels 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 super pixels 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.

Fig.7. forgery Input Image

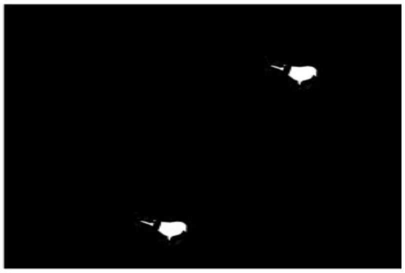

Fig.8. the ground-truth forgery regions of the corresponding host image

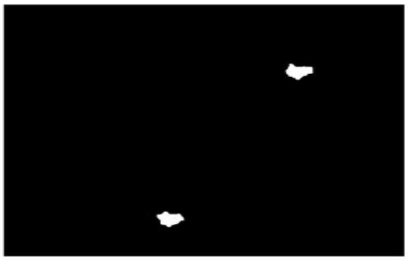

Fig.9. the detected forgery regions of the corresponding images, using the proposed forgery detection scheme

## V. CONCLUSION

In contrast of block –based algorithms and key point based algorithms, and feature point matching detects the forgery region more accuracy overcomes the drawbacks of the existing methods. Digital forgery images created with copy move operations are challenging to detect. In this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching. The Adaptive Over Segmentation algorithm is proposed to segment the host image into non-overlapping and irregular blocks adaptively according to the given host images; using this approach, for each image, we can determine an appropriate block initial size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Then, in each block, the feature points are extracted as block features, and the Block Feature Matching algorithm is proposed, with which the block features are matched with one another to locate the labeled feature points.

## VI. REFERENCES

[1] Amruta Jagtap, H. A. Hingoliwala, H. A. Hingoliwala, “Survey Paper on Advanced Techniques for Image Forgery Detection”, International Journal of Science and Research (IJSR), Vol 4 Issue 12, 2015.

[2] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," 2003.

[3] Sreelakshmi. M, Amrutha M, “Forgery and Forensic Detection Using Adaptive over segmentation and DCT of JPEG Images”.

[4] Chi-Man Pun, Chen Yuan, Xiu-Li Bi,” Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching”.

[5] H. Huang, W. Guo, and Y. Zhang, “Detection of copy–move forgery in digital images using SIFT algorithm,” in Proc. Pacific-Asia Workshop Comput. Intell. Ind. Appl. (PACIIA), Dec. 2008, pp. 272–276.

[6] B. L. Shivakumar and S. S. Baboo, “Detection of region duplication forgery in digital images using SURF,” IJCSI Int. J. Comput. Sci. Issues,vol. 8, issue 4. no. 1, pp. 199–205, 2011.

[7] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic science international,* vol. 171, pp. 180-189, 2007.

[8] 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.

[9] 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.

[10] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," *WSEAS Transactions on Signal Processing,* vol. 5, pp. 188-197, 2009.

[11] S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *Information Hiding*, 2010, pp. 51-65.

[12] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," *Ieee*

*Transactions on Information Forensics and Security,* vol. 8, pp. 1355-1370, Aug 2013.

[13] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, 2011, pp. 1880-1883.

[14] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in *Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on*, 2008, pp. 272-276.

[15] X. Y. Pan and S. Lyu, "Region Duplication Detection Using Image Feature Matching," *Ieee Transactions on Information Forensics and Security,* vol. 5, pp. 857-867, Dec 2010.

[16] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," *Information Forensics and Security, IEEE Transactions on,* vol. 6, pp. 1099-1110, 2011.

[17] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in *Computer Vision–ECCV 2006*, ed: Springer, 2006, pp. 404-417.

[18] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *Ieee Transactions on Information Forensics and Security,* vol. 7, pp. 1841-1854, Dec 2012

[19] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," *IEEE Trans Pattern Anal Mach Intell,* vol. 34, pp. 2274-82, Nov 2012.

## Author Profile

He received his M.Tech degree in DSCE from Jaya Prakash narayan College of Engineering, B.Tech degree in Electronics and Communication Engineering from Jaya Prakash narayan College of Engineering, and His interested areas are Image Processing and communications.