International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

An adaptive segmentation based approach for image forgery detection using efficient feature matching

Shilpa.K.R[1], T.Ashwini[2]

[1] Assistant professor, Dept. of ECE, BITM, Ballari, Karnataka, India
[2] PG Student [DE], Dept. of ECE, BITM, Ballari, Karnataka, India

---

Abstract - ***In the today world digital images are popular sources of information. Digital images can be easily modified using powerful image editing software. The process of creating flexible or emulating documents with the aim of altering the details to earn the profit from the forged image is known as Image forgery. Copy move forgery is the process of creating a forged item by copying a region of the image and pasting it into another region in the same image. An adaptive segmentation based approach for image forgery detection using efficient feature matching the proposed scheme integrates both block-based and key point-based forgery detection methods. Adaptive segmentation devide image into non overlapping blocks 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 superpixels 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.***

Key Words: ***Digital Image, Copy-Move Forgery Detection,Adaptive Over-Segmentation, Local Color Feature, Forgery Region Extraction***

1.INTRODUCTION

Nowadays digital image forgery is easy to perform, because of the development of computer technology and image processing software's**.** Though digital images are a widespread source of information but the big problem in digital image is to maintain the reliability of the image. More and more researches have begun in last some years to focus on the problem of digital image tempering. In the existing type of image tampering a common method is copy-Move forgery. it is just past one or more copied regions of an image into other parts of the same image.

In some image processing method like rotation, scaling, blurring compression and noise addition, Occasionally applied to make convincing forgeries during copy and move operations. Some properties like noise component, color character and other important properties are compatible with the remainder of the image, because of the copy and move parts are copied from the same image. so that some of the detection method is not applicable in this case. In last some years, many forgery detection method have been has been proposed for copy move forgery detection. Based on existing model the copy move forgery detection method can be categories into two main parts-one is block based algorithms and another is feature key point-base algorithms.

In existing block based forgery detection method we divide the input image into overlapping and regular image blocks; then by the help of matching blocks of image pixels or transform coefficients tempered region is obtained.

a forgery detection method is proposed by Fridrich et al. [1] in which the input image was divided into over-lapping rectangular blocks, from which we get the tempered region by the help of quantized discrete cosine transform(DCT) coefficients of the blocks matching. To reduce the feature dimensions Popescu and Farid [2] applied Principal Component Analysis (PCA). Luo et al. [3] used the RGB color channels and direction information as block features. Li et al. [4] implements Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract the image features. To obtain image features Bayram et al. [7] implemented the Fourier-Mellin Transform (FMT) features. Wang et al. [8, 9] implemented the mean intensities of circles with different radii around the block center to represent the block features.Ryu et al. [11, 12] implemented Zernike moments as block features. Bravo-Solorio and Nandi [13] implemented information entropy as block features.

The other alternative existing proposed method was key point-based forgery detection, where key points of the image are pull out and matched over the complete image to resist some image transformations while identifying duplicate regions.In [14-16, 18], the Scale-Invariant Feature Transform (SIFT) [20] was implemented to the host images to pullout the feature points, which were then matched to one another. If we get the value of the shift vector is greater than the threshold, the set of corresponding SIFT feature were known as the forgery region. Though, these approaches can locate the matched key points, but still most of them cannot locate the forgery regions very well; so that they cannot get the more accurate result and same time a high recall rate.

Almost all Block based forgery detection method use a identical framework, the only difference in their approaches is applying different feature extraction method for extraction of block features. The existing algorithm are effective in forgery detection but they have three main drawback,

1)since the host image is divided into overlapping rectangular blocks, so it becomes very expensive as the size of the image increase;2)these methods are not able to identify significant geometrical transformations of the forgery regions; and 3)the recall rate of these methods are very low. The first two problem we can fix in key point based forgery detection, they can avoid the computational complexity and can successfully detect the forgery, even when some attacks applied in the host images but the recall rate what we get is very poor.

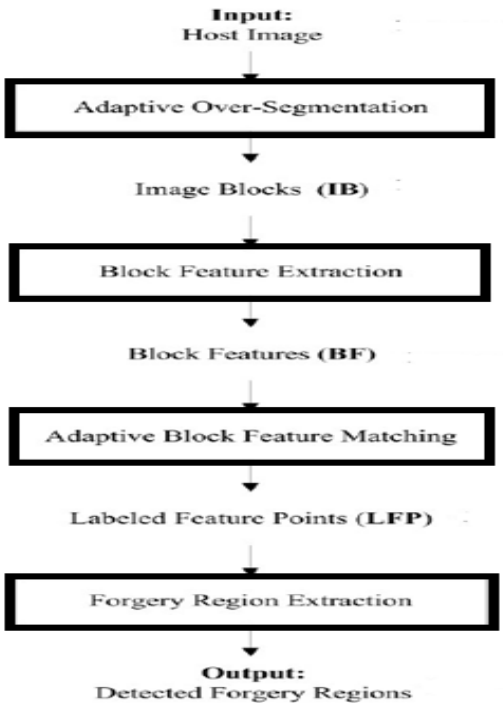
To overcome this problem in this paper we proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching. Our prosed model uses both the traditional block based method and key point-based forgery detection method. Here we propose an image-

blocking method known as adaptive over-segmentation algorithm to divide the host images into non-overlapping and irregular blocks adaptively. After then we apply key point-based forgery detection method which gives the feature point of each image block as block features instead of being extracted from the complete host image as in the old key point-base approaches.

To detect more accurately we proposed the Forgery Region Extraction algorithm, which gives super pixels as feature blocks in the place of feature points and after that we combined the neighboring blocks with similar local color features into feature block to build up merged regions. Last we do morphological operation into the obtained merged image.

2. IMAGE FORGERY DETECTION USING ADAPTIVE OVER-SEGMENTATION AND FEATURE POINT MATCHING

Here we are describing the image forgery detection using adaptive over segmentation and feature point matching. The figure 1 represents the framework of the proposed image forgery detection scheme. First we are applying over-segmentation method which divides the host image into non-overlapping and irregular blocks known as image blocks. Then we are applying the Scale Invariant Feature Transform (SIFT) in each block to pullout the SIFT feature points as Block Features (BF).The block features a are matched with one another, and the feature points that are successfully matched to one another are determined to be Labeled Feature Points (LFP),that indicates the suspected forgery regions.



1. Framework of the proposed copy-move forgery detection scheme

Adaptive Over-Segmentation Algorithm

The common approaches to region segmentation are based on intensity thresholding and work well for images with homogeneous objects of interest. However, many images contain noise, texture, and clutter, all of which hamper the effectiveness of these techniques. The application of threshold-based segmentation algorithms on images with nonhomogeneous objects of interest can result in segmentation that is too coarse or too fine. These results are defined as under segmentation and over segmentation, respectively. Split and merge

techniques can often be used to successfully deal with these problems.

For some images it is not possible to set segmentation process parameters, such as a threshold value, so that all the objects of interest are extracted from the background or each other without over-segmenting the data. Over-segmentation is the process by which the objects being segmented from the background are themselves segmented or fractured into subcomponents.

After an image is segmented, its adjacent regions can be merged to form a less fragmented segmentation based on their similarity. Similarity metrics can be defined as a function of intensity, color, size, texture, variance, and shared border ratio, among others. In addition, for any feature, different techniques can be derived to measure similarity. For instance, the difference in intensity between adjacent objects can be measured by two methods. In one method, the average of all the pixel intensities in one object can be compared to the average intensity of all the pixels in an adjacent object. This process is termed global contrast. Alternatively, local contrast can be computed by comparing the average intensity made up of just the pixels that are adjacent to the border between two objects. One or the other or the maximum of the two can be used. For another alternative, the size of the objects being compared could be used to select which contrast method is employed. Global contrast can be computed when small objects are being considered, and local contrast can be used for large objects.

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 super pixels 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 E_{HF} energy 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 super pixels can be defined as in (4)

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

$$E_{HF} = \sum_l (\sum |CD_i| + \sum |CH_i| + \sum |CV_i|), l = 1,2,\ldots,4 \quad (2)$$

Where CA_4 indicates the approximation coefficients at the 4th level of DWT; and CD_i, CH_i and CV_i indicate the detailed coefficients at the ith level of DWT, i=1, 2,..., 4 .

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

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

Where *S* means the initial size of the super pixels; $M \times N$ indicates the size of the host image; and P_{LF}means the percentage of the low-frequency distribution.

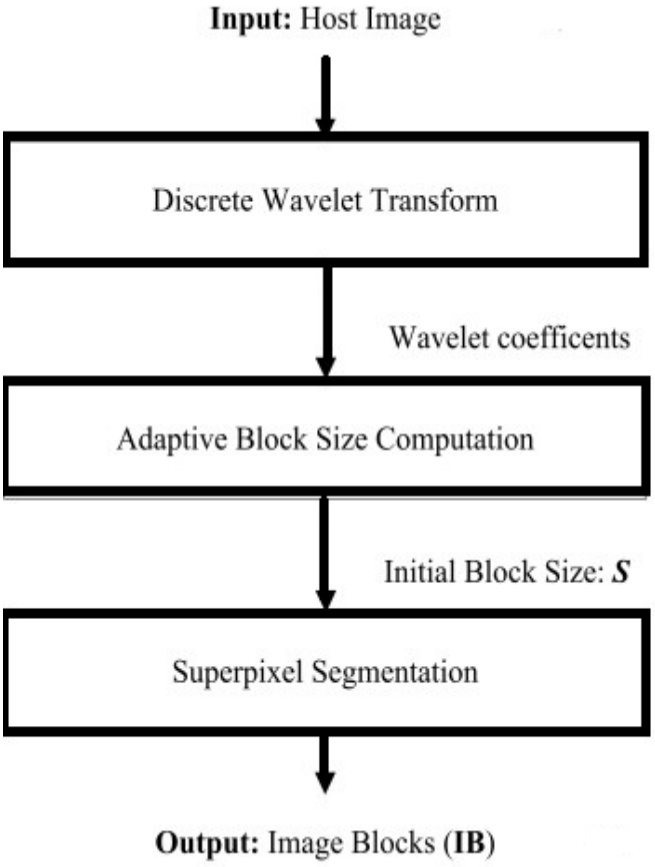


Fig 2: Flowchart of the Adaptive Over-Segmentation algorithm

Using the Adaptive Over-Segmentation method described above, the size of the host image I1 is $M1 \times N1 = 162 \times 1224$;according to (3), can be calculated, as P_{LF}_1 ; therefore, the adaptive initial size of the super pixels is calculated using (4), which yields S_1=199. Similarly, for the host image I2 in Fig. 4-(B1), with the size $M2 \times N2$=1306× 1950 , P_{LF}_2=39.89% and S_2=159; for the host image I3 IN fig

With the size $M3 \times N3 = 1936 \times 1$, P_{LF}_2=59.92% and S_3=224.

Block Feature Extraction Algorithm

Here we are extracting block features from the image block. The old block-based feature extraction method uses the pixels of the image as block features. Although those features mainly extract the contents of the image block which does not tell about location information. That's why in this paper we are extracting feature points from each image block as block feature and the obtain feature point should be not affected from various attacks like as scaling, rotation and compression.

The SIFT[20]and SURF [21] methods of feature point extraction have been used widely in the field of computer vision in last some years. This method is robust that means not affected from common image processing like rotation, blurring and compression. This two method was also used as feature extraction methods in the existing key point-based copy-move forgery detection methods.In our proposed algorithm,

we have selected SIFT method as the feature point extraction method to extract the feature points from each image.

C. Block Feature Matching Algorithm

After getting the block features, our next target is to locate the matched block through the block features. The block matching process outputs a specific block pair in most of the existing block-based methods, only if there are many other matching pairs in the same mutual position to assume that they have the same shift vector. 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. Fig. 3 shows the flowchart of the Block Feature Matching algorithm. In the matched block pairs the matched feature points are extracted and labeled to locate the position of the suspected forgery region.

STEP-1: Load the Block Features BF ,$\{BF_1, BF_2, \ldots.\}$ 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_B 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.

firstly, the correlation coefficient CC of the image blocks indicates the number of matched feature points between the corresponding two image blocks. Assuming that there are N blocks after the adaptive over-segmentation, we can generate N(N-1) / 2 correlation coefficients, which form the correlation coefficient map. Among the blocks, the two feature points are matched when their Euclidean distance is greater than the predefined feature points' matching threshold TR_P , which means that the feature point $fa(x_a, y_a)$ is matched to the feature point $fb(x_b, y_b)$only if they can meet the condition defined in (5).

$d(f_a, f_b).TR_P \leq d(f_a, f_i)$	(5)

where$d\ (f_a, f_b)$ means the Euclidian distance between the feature pointsf_a and f_b, as defined in (6);$d\ (f_a, f_i)$ means the Euclidian distances between the key points f_a and all of the other key points in the corresponding block, as defined in (7), i means the ith feature points in the corresponding block; in addition, TR_P indicates the feature points matching threshold. When TR_P becomes larger, the matching

accuracy will be higher, but at the same time, the miss probability will be increased. Therefore, in the experiments, we set $TR_p = 2$ to provide a good trade-off between the matching accuracy and miss probability.

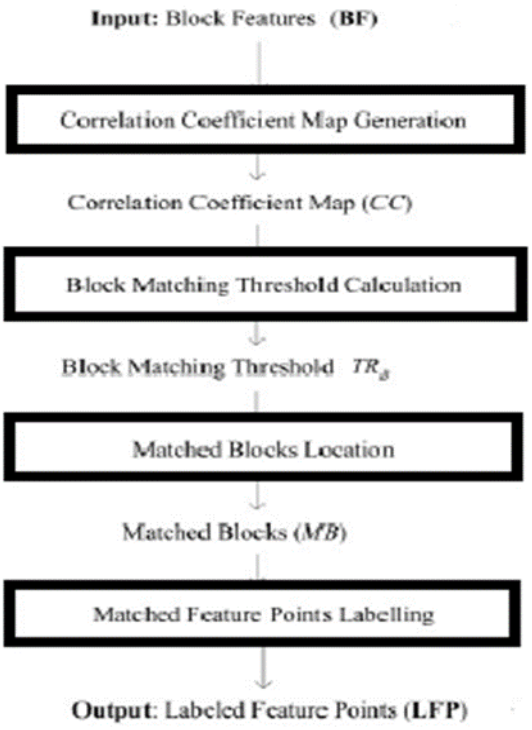


Fig 3: Flowchart of the Block Feature Matching algorithm

Labeled feature points (LFP) tells only the locations of the forgery regions, we must still locate the forgery regions. We know that the super pixels can segment the host image very well, so just we proposed a method by replacing the LFP with small super pixels to get the suspected regions (SR), which are combinations of labeled small super pixels. Additionally, 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). IN last we do morphological operation is applied to the merged regions to build the detected copy-move forgery regions. Fig. 4 shows the flow chart of the Forgery Region Extraction algorithm, which is explained in detail as follows.

Algorithm: Forgery Region Extraction

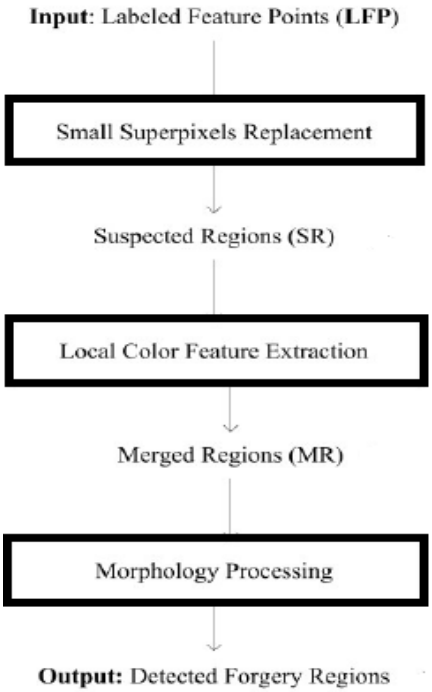
Input: Labeled Feature Points (LFP)

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.



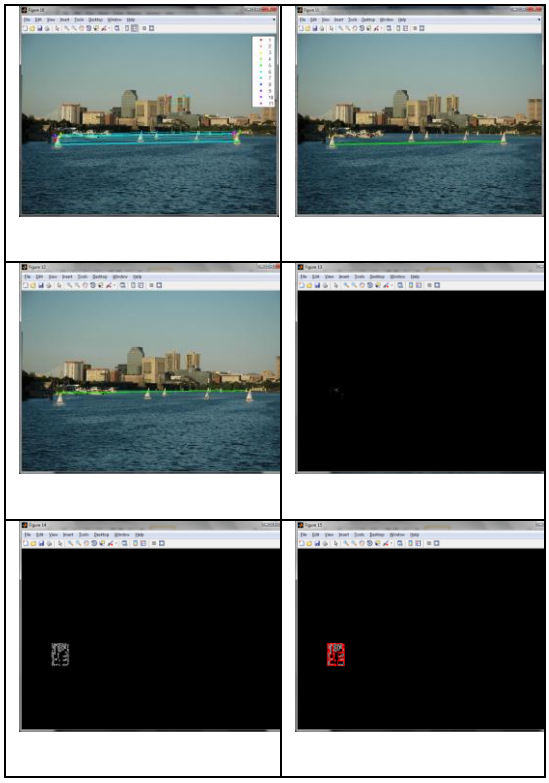
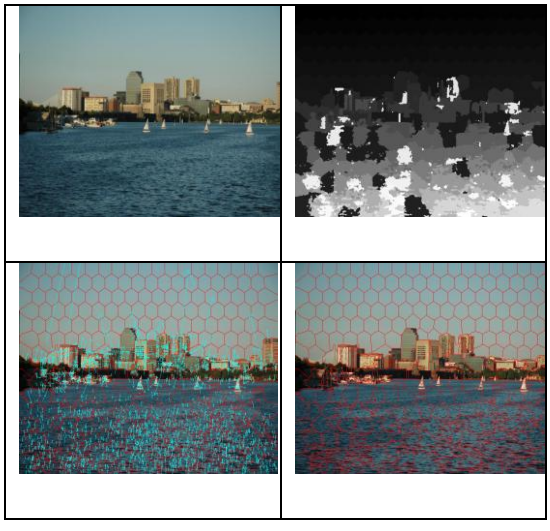


Fig 4:Flow chart of the Forgery Region Extraction algorithm

3. EXPIREMENTAL RESULTS



3. CONCLUSIONS

It's challenging to detect the digital forgery images created with copy-move operations. In this paper, here we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching. The Adaptive Over-Segmentation algorithm is used to segment the host image into non-overlapping and irregular blocks adaptively according to the given host images; using this approach, we can determine an appropriate block initial size to enhance the accuracy of the forgery detection results for each image, and, at the same time, reduce the computational expenses. Then, the feature points are extracted as block featuresin each block, and the Block Feature Matching algorithm is proposed, with which the block features are matched with one another to locate the labeled feature points; this procedure gives the detected region but not fully accurate. Subsequently, to spot the more accurate forgery regions, we use the Forgery Region Extraction algorithm, in which the labeled

feature points are substituted with small superpixels as feature blocks, and the neighboring feature blocks with local color features that are similar to the feature blocks are merged to generate the merged regions. Next, the morphological operation is applied to the merged regions to generate the detected forgery regions. We have done a series of experiment to evaluate the effectiveness and robustness of the proposed scheme using adaptive over-segmentation and feature point matching that is showing in the result part.

REFERENCES

[1] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in *in Proceedings of Digital Forensic Research Workshop*, 2003.
[2] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," *Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515,* 2004.
[3] 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.
[4] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in *Multimedia and Expo, 2007 IEEE International Conference on*, 2007, pp. 1750-1753.
[5] 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.
[6] X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in *Computer Science and Software Engineering, 2008 International Conference on*, 2008, pp. 926-930.
[7] 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.
[8] 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.
[9] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," *ActaAutomaticaSinica,* vol. 35, pp. 1488-1495, 2009.
[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] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in *Multimedia Information Networking and Security (MINES), 2010 International Conference on*, 2010, pp. 889-892.
[18] P. Kakar and N. Sudha, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features," *Information Forensics and Security, IEEE Transactions on,* vol. 7, pp. 1018-1028, 2012.
[19] B. Shivakumar and L. D. S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," *IJCSI International Journal of Computer Science Issues,* vol. 8, 2011.
[20] D. G. Lowe, "Object recognition from local scale-invariant features," in *Computer vision, 1999. The proceedings of the seventh IEEE international conference on*, 1999, pp. 1150-1157.
[21] H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in *Computer Vision–ECCV 2006*, ed: Springer, 2006, pp. 404-417.
[22] 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
[23] 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.

BIOGRAPHIES

Shilpa K.R received the B.E. degree in Electronics and Communication Engineering , and Completed the M.Tech in Electronics.

Ashwini T received the B.E. degree in Electronics and Communication engineering from UBTDTCE,Davanagere in (2012) - India and Pursuing the M.Tech in Digital Electronics BITM,Bellary.