

Feature Point Extraction by Adaptive Over-Segmentation and Feature Point Matching for Effective Digital Image Forgery Detection

Ms. Tabassum Sultana, Dr. Uma N Dulhare, Mr. Shaik Rasool

Abstract— The invention of the web has introduced the incredible growth and developments within the noted analysis fields like medication, satellite imaging, processing of image, security, biometrics, and biological science. The algorithms applied in the twenty 21st century has created the human life easier and secure, but the security is a major concern in the digital image processing domain. A new study is presented in this paper to detect forgery using the adaptive over-segmentation and feature point matching. Both block based and key point based forgery detection methods is integrated here. Adaptive over segmentation algorithm is used to segment the host image into non -overlapping and irregular blocks adaptively. Feature points are extracted from every block as block features and the block features are matched with one another to locate suspected forgery region. The feature points are gradually replaced by super pixels in the proposed Forgery Region Extraction algorithm and then neighboring blocks that have similar local color features are merged into the feature blocks to form merged regions; finally, morphological operation is applied to the regions which shows the detected forgery regions. The proposed forgery detection algorithm achieves much better detection results even under various challenging conditions than earlier methods in all aspects.

Index Terms— Copy-move, Image Forgery, Forgery detection, adaptive over-segmentation, neighboring blocks, super pixels, feature points.

1 INTRODUCTION

The digital image processing is the important research domain in the 21st century where its presence is clearly observed in varied 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 and a lot of research is carried out in the literature but still achieving the desired results is remained as an unsolved issue. The digital images are considered as the primary source of the medium used to meet the purpose of data transmission, data compression, data hiding and various other applicative research areas. Images can be used as an evidence for any event in the court of law, information broadcasting, the images broadcasted in tv news are accepted as the certificate for the truthfulness of that news. Digital images are being used in many applications ranging from military to medical diagnosis. Due to availability of advanced photo editing software image manipulation has become very easy to perform and at the same time difficult to detect. Therefore, the integrity and the authenticity of image is lost. To maintain the integrity of images a powerful and accurate forgery detection process is essential.

One of the most famous manipulations on digital image is copy-move forgery, in which a particular region is copied and pasted into another part of the same image. Previously Friedrich 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 [1]. Luo et al. for block feature used RGB colour components as well as direction information in this technique [2]. Li et al to get image features used two methods namely Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) [3]. Mahdian and Saic considered 24 blur-invariant moments for feature extraction [4]. Bayram et al. used transform technique Fourier-Mellin Transform (FMT) to get features [5]. Wang et al to get the Block features, considerations of mean intensity with different radii are considered [6]. Ryu et al. to get block features there is consideration of Zernike moments [7]. Bravo Solorio and Nandi to get block features considered Information Entropy [8]. I. Amerini, L. Ballan [9] 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 works by dividing an input image into overlapping regions of regular size blocks and then matches with the image pixels obtained from regions to get forged regions. Another is key point based forgery detection where image key points are extracted and matched over the whole image to resist some transformations while identifying duplicated regions.

In existing block-based forgery detection schemes, the host image was usually divided into overlapping regular blocks, with the block size being defined and fixed beforehand, Then, the forgery regions were detected by matching those blocks. In this way, the detected regions are always composed of regular blocks, which cannot represent the accurate forgery region

- Ms. Tabassum Sultana is currently pursuing M. Tech. program in Computer Science Engineering in MJCET, India,
E-mail: tabassumsultana30@gmail.com
- Dr. Uma N Dulhare is currently working as Professor in CSED, MJCET, India.
E-mail: prof.umadulhare@gmail.com
- Mr. Shaik Rasool is currently working as Assistant Professor in ITD, MJCET, India.
Email: rasool@outlook.com

well; therefore, the recall rate of the block-based methods is always very low. Also as the size of the host images increases, the matching computation of the overlapping blocks will be much more expensive.

Although key point based methods can reduce two problems but the recall rate is very poor.

To address these issues, the proposed scheme integrates both block based and key point based methods. As in block based forgery detection method, an image blocking method called adaptive over segmentation is used which can segment the host image into non-overlapping regions of irregular shape as image blocks.

Because host image is divided into non-overlapping regions of irregular shape and because the superpixels are perceptually meaningful atomic regions that can be obtained by over-segmentation, the simple linear iterative clustering (SLIC) algorithm is employed to segment the image into meaningful irregular superpixels, as individual blocks. Using the SLIC segmentation method, the non-overlapping segmentation can decrease the computational expenses compared with the overlapping blocks.

Adaptive Over-Segmentation method can determine the initial size of the superpixels based on the texture of the host image that can ensure not only that the superpixels can get close to the edges but also that the superpixels contains sufficient feature points to be used for forgery detection. Larger superpixels imply a smaller number of blocks, that can reduce the computational expense when the blocks are matched with one another. The initial size of the superpixels can be set to be relatively small, when the texture of the host image has more detail to ensure good forgery detection results for authenticity.

2 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

2.1 Types of Image Forgeries

The forgeries are classified into four major categories: image retouching, Image Splicing, Copy-Move (cloning), Morphing, Enhanced. These are shown in table 1

i. Image Retouching

The first type is image retouching, where this method is used for enhancing an image or reducing certain feature of an image in this method, the professional image editors change the background, fill some attractive colors, and work with hue saturation for toning and balancing.

ii. Image splicing

In this technique there is a composition of two or more image which are combined to create a fake image.

iii. Copy-Move





Copy Move Forgery is a technique in which a part of same image is copied and pasted into another part of that image itself. In Copy Move Attack, the intention is to hide or add

something in the original image with some other part of the same image.

iv. Morphing

In this type the image and video can be exposed into unique influence, where 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 IMAGE FORGERIES

Types	Detail	Appearance
Image retouching	An example of forgery where the original image and a forged image shows the difference [10].	
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 [11].	
Copy-Move (cloning)	The images show the copy-move attack and in left side image three rockets and in the forged image contains four rockets [12].	
Morphing	The left and right images are original the middle image is -morphed image [10].	

3 EXISTING APPROACHES

As demonstrated in this document, the numbering for sections upper case Arabic numerals, then upper case Arabic numerals, separated by periods. Initial paragraphs after the section title are not indented. Only the initial, introductory paragraph has a drop cap.

3.1 Detecting Duplicate Images

A technique that works by applying principal component analysis to very little mounted - size image blocks to yield a reduced dimension illustration was planned by Alin C Popescu et al. (2004), Whereas present state of art techniques has a

tendency to notice some duplicate footage (noises). Then the duplicate regions are detected by lexicographically sorting the complete image blocks. This will be very good applicable technique to yield a reduced dimension illustration. It's sensitive to jpeg lossy compression and to boot it's additive to noise [13].

3.2 Fast Copy-Move Forgery Detection

It is a methodology to discover copy-move forgery by dividing the image into overlapping blocks of equal size, and then extracting feature from every block and representing it as a vector and the extracted feature vectors are sorted using radix sort, which was planned by Hwei-jen sculpture et.al (2009). For every pair of adjacent feature vectors in the sorting list, difference (shift vector) of the positions is computed. For each of the shift vector accumulated number is evaluated. A huge accumulated number is detected as possible presence of a duplicated region. Radix sort dramatically reduces the time complexity and also enhances the potentiality of resisting of varied attacks like JPEG compression and noise. But this method does not perform well while dealing with rotation arbitrary angles [14].

3.3 Robust Copy-move Forgery

Sevinc Bayramet al. (2009) proposed to use Fourier- Mellin Transform (FMT) features that are invariant to scaling and translation. In this detection scheme counting of bloom filters is done instead of lexicographic sorting. It detects copy move forgery accurately irrespective of whether the image is turned, scaled or extremely compressed. This detection scheme improves the efficiency. However, the robustness of the method is reduced [15].

3.4 Detection Digital Images Using SURF

B. L. Shivakumar et al. (2011) proposed a method to detect copy move forgery based on SURF (Speeded up Robust Features) and KD- tree for matching of multidimensional data. Identification of the Copy move forgery can be detected by finding the duplicated regions using Speeded Up Robust Features (SURF) keypoints. These SURF keypoints are extracted from images. This method can detect duplicated regions with different sizes. The result shows that this method can detect copy move forgery for images with high resolution with minimum false match. But this method cannot successfully detect few small copied regions [16].

3.5 A Sift-based Forensic Method

Irene Amerini et al. (2011) proposed a method for image forgery detection by using SIFT algorithm. This 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 [17].

3.6 Exposing Transform-invariant Features

Pravin Kakar et al. (2012) has proposed a method based on transforming-invariant features. These features are obtained by the features from MPEG-7 image signature tools. In feature matching process it utilizes the inherent constraints in

matched feature pairs to improve the detection of duplicated regions. 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 [18].

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.

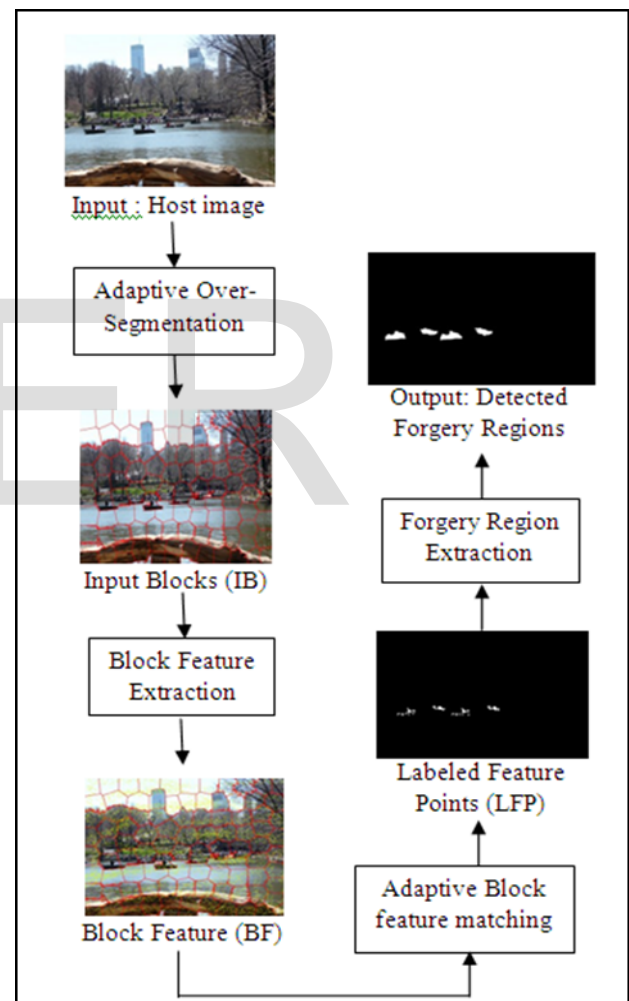


Fig.1: The proposed copy-move forgery detection scheme framework

- 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 Speeded Up Robust Features technique, where it is

applied to each segmented block to extract the block features (BF) in a reliable way.

- The suspected forgery regions indication is 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.

4.1 Adaptive over segmentation algorithm

The Adaptive Over-Segmentation algorithm, which can segment the host image into non-overlapping regions of irregular shape as image blocks is proposed. Then the forgery regions can be detected by matching those non-overlapping and irregular regions. The non-overlapping segmentation can decrease the computational expenses compared with the overlapping blocking; further 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 [19] 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 sizes of the super pixels can give different forgery detection results; accordingly, different host images should be blocked into super pixels of different initial sizes, which is pertained to the forgery detection results.

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

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

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

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

Many experiments are performed 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. A four-level DWT, using the 'Haar' wavelet, on the host image is performed; then, the low-frequency energy ELF and high-frequency energy EHF can be calculated using (1) and (2), respectively. With the low-frequency energy ELF and high-frequency energy EHF, the percentage of the low-frequency distribution PLF using (3) is calculated, according to which the initial size S of the superpixels can be defined as in (4)

where S is the initial size of the superpixels; $M \times N$ shows the size of the host image; and P_{LF} stands for the percent of the low-frequency distribution.

The Adaptive Over-Segmentation method divides the host image into blocks with initial sizes adaptively according to the given host images, with which each image can be specified to be an appropriate block size to increase the forgery detection results as shown in Fig. 2.

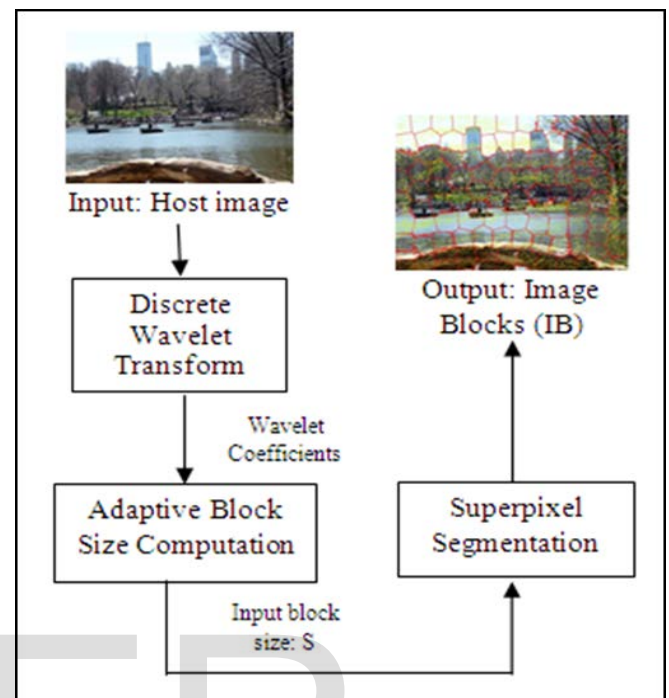


Fig.2: The adaptive over-segmentation flowchart

4.2 Block Feature Extraction Algorithm

After the image is divided into image blocks, block features are extracted from each image blocks (IB). The existing block-based forgery detection methods extracted features of the same dimension as the block features or directly used the pixels of the image block as 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 paper, the feature points are extracted from each image block as block features which are 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. Therefore, in this paper SURF is used for feature point extraction. Therefore, each block feature contains irregular block region information and the extracted feature points.

4.3 Block Feature Matching Algorithm

After obtaining the block features, matched blocks are to be located through block features. 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, if they have the same shift vector. When shift vector exceeds a threshold which is user specified,

the matched blocks that contributed to that specific shift vector are demonstrated as regions that might have been copied and moved. In our algorithm, because the block feature consists of a set of feature points, a different method is proposed 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 $BF = \{BF1, BF2, BFN, \dots\}$, where N is the number of image blocks; and compute the correlation coefficients CC of the image blocks.

STEP-2: Compute block matching threshold TRB according to the distribution of correlation coefficients.

STEP-3: Find the matched blocks MB with respect to the block matching threshold TRB

STEP-4: Label the feature points that are matched in the matching blocks MB to represent the suspected forgery regions.

4.4 Forgery Region Extraction Algorithm

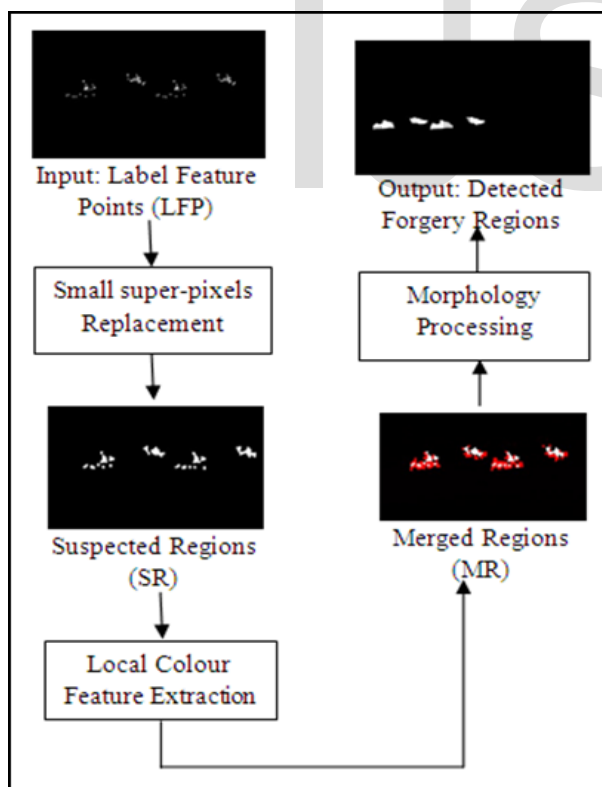


Fig. 3: Flow chart of the Forgery Region Extraction algorithm

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 replacing labeled feature points as-superpixels by applying SLIC algorithm. 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. 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. 3 shows the flow-chart of the Forgery Region Extraction Algorithm.

Algorithm: Forgery Region Extraction

STEP-1: Load the Labeled Feature Points (LFP), implement the SLIC algorithm with the initial size S to the host image to divide it into small superpixels as feature blocks, and substitute each labeled feature point with its matching feature block, thus yielding the Suspected Regions (SR).

STEP-2: Evaluate the local color feature of the superpixels neighbor to the SR, called neighbor blocks; when their color feature resembles to that of the suspected regions, the neighbor blocks are merged into the corresponding Suspected Region, therefore creating the merged regions (MR).

STEP-3: Implement the morphological close operation into MR to finally generate the detected forgery regions.

5 CONCLUSION

In this study, a methodology to support image forensics by detecting copy move forgery efficiently and accurately has been proposed. To detect the more accurate forgery regions, Forgery Region Extraction algorithm is proposed. The feature points are gradually replaced by super pixels in the proposed Forgery Region Extraction algorithm and then neighboring blocks that have similar local color features are merged into the feature blocks to form merged regions; finally, morphological operation is applied to the regions which shows the detected forgery regions. The proposed forgery detection algorithm can achieve much better detection results even under various challenging conditions than earlier methods in all aspects.

REFERENCES

- [1] Jessica Fridrich, David Soukal, and Jan Lukáš, "Detection of Copy-Move Forgery in Digital Images" Q.-C. Yang and C.-L. Huang, "Copy-move Forgery Detection in Digital Image," In Advances in Multimedia Information Processing-Pcm 2009, Ed: Springer, 2009, Pp. 816-825.
- [2] 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. B. Mahdian And S. Saic, "Blind Methods for Detecting Image Fakery," *Ieee Aerospace and Electronic Systems Magazine*, Vol. 25, Pp. 18-24, 2010.
- [3] 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. 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] 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.
- [5] 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.
- [6] 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.
- [7] S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *Information Hiding, 2010*, pp. 51-65.
- [8] 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.
- [9] 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.
- [10] H. Shah, P. Shinde, And J. Kukreja, "Retouching Detection and Steganalysis," *Ijeir*, Vol. 2, Pp. 487- 490, 2013. M.-J. Tsai And G.-H. Wu, "Using Image Features to Identify Camera Sources," In *Acoustics, Speech and Signal Processing, 2006. Iccasp 2006 Proceedings. 2006 Ieee International Conference On*, 2006, Pp. li-li.
- [11] 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. [12] M. Sridevi, C. Mala, And S. Sandeep, "Copy-Move Image Forgery Detection in A Parallel Environment," 2012.
- [12] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," *Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515*, 2004.
- [13] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," *WSEAS Transactions on Signal Processing*, vol. 5, pp. 188-197, 2009.
- [14] 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.
- [15] 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.
- [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] 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.
- [18] 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.