Image Forgery Detection Using Adaptive Oversegmentation and Feature Matching

Harish Patil
Master of Technology, Student
Department of Electronics and Telecommunication
K. J. Somaiya College of Engineering,
Mumbai, India
harish.patil@somaiya.edu

Nitin S. Nagori
Assistant Professor
Department of Electronics and Telecommunication
K. J. Somaiya College of Engineering,
Mumbai, India
nitin.nagori@somaiya.edu

***Abstract*-Image tampering has become a common phenomenon with easy growing accessibility of advanced image editing software and powerful computing hardware. One of the most common types of image forgeries is the copy-move forgery (CMF), where a region from an image is replaced with another region from the same image. An image with copy-move forgery contains a couple of regions whose contents are identical. An efficient technique that automatically detects duplicated regions in a digital image by applying a component analysis to small image blocks or segments to yield a reduced dimension image is needed. Feature extraction is an effective way in reducing the dimensionality and increasing the computational efficiency. In this paper a novel copy–move forgery detection scheme using adaptive oversegmentation and feature point matching is implemented. This scheme integrates both block-based and keypoint-based forgery detection methods.**

Index Terms - Image tampering, CMF, Feature Extraction, keypoint based, block based, SIFT.

I. INTRODUCTION

With development of computer technology digital image forgery has become a serious issue. Digital images are a popular source of information, and the reliability of digital images is thus becoming an important problem to solve. Sophisticated digital cameras and photo-editing software packages are found everywhere. As a result, it has become easy to create forgeries that are difficult to distinguish from authentic photographs. A common practice in tampering with an image is to copy and move portions of the image to conceal a person or object in the scene. During the copy and move operations, some image processing methods such 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. In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-move forgery detection methods can be categorized into two main categories: block-based algorithms and feature keypoint-based algorithms [1]. In this paper a technique that can efficiently detect and localize duplicated regions in an image is presented. This technique works by first applying a Principal Component Analysis (PCA) on small fixed-size image blocks to yield a reduced dimension representation. This representation is robust to minor variations in the image due to additive noise or lossy compression. Duplicated regions are then detected by lexicographically sorting all of the image blocks. A similar method for detecting duplicated regions based on lexicographic sorting of Discrete Cosine Transform (DCT) block coefficients was proposed. As an alternative to the block-based methods, keypoint-based forgery detection methods were proposed, where image keypoints are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. In the Scale-Invariant Feature Transform (SIFT) was applied to the host images to extract feature points, which were then matched to one another. When the value of the shift vector

(a) (b)

Figure 1 Example of a typical copy-move forgery. Left: the original image. Right: the tampered image [2].

exceeded the threshold, the sets of corresponding SIFT feature points were defined as he forgery region. In the Speeded Up Robust Features (SURF) were applied to extract features instead of SIFT. However, although these methods can locate the matched keypoints, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate. Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features.

II. WORKFLOW FOR A TYPICAL COPY MOVE FORGERY DETECTION

A large number of Copy Move Forgery Detection methods have been proposed, most techniques follow a common pipeline. Jessica Fridrich, David Soukal, and Jan Lukas [2] proposed two techniques. One method is based on exact match for detection and other one is based on an approximate match. The first algorithm is for identifying those segments in the image that match exactly by ordering and matching of pixel representation of blocks. Given an original image, there exist

two processing alternatives. CMFD methods are either keypoint-based methods or block-based methods. The common processing pipeline for the detection of copy-move forgeries is shown below:

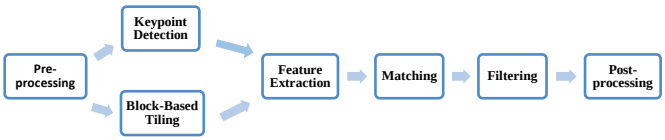


Figure 2 Common processing pipeline for the detection of copy-move forgeries

The explanation of each step is given below:

1) Pre-processing: The scope of pre-processing is the improvement of the image data and enhancement in the feature which is important for further detection. The image is converted into grayscale when applicable. Most pre-processing methods operate on grayscale images, and as such require that the colour channels be first merged.

2) Keypoint Detection: In key-point based methods, feature vectors are computed only for key-points in the image such as regions with entropy etc. without any image subdivision. Similar features within an image are afterwards matched. A forgery shall be reported if regions of such matches cluster into larger areas.

3) Block-Based Tiling: Block-Based tiling methods divide the image in rectangular regions. For every region, a feature vector will be computed and then similar feature are matched subsequently. There are four algorithms [3] for Block-Based Tiling. These algorithms are moment-based, dimensionality reduction-based, intensity-based, and frequency domain-based features and explained as follows:

3.(a) Moment-based:

Three distinct approaches within this class were evaluated. Mahdian and Saic proposed the use of 24 blur-invariant moments as features (Blur). Wang et al. used the first four Hu moments (Hu) as features. Finally, Ryu et al. recently proposed the use of Zernike moments (Zernike).

3.(b) Dimensionality reduction-based:

The feature matching space was reduced via principal component analysis (PCA). Bashar et al. [4] proposed the Kernel-PCA (KPCA) variant of PCA. Kang et al. computed the singular values of a reduced-rank approximation (SVD).

3.(c) Intensity-based:

The first three features used are the average red, green and blue components. Additionally, Luo et al. [5] used directional information of blocks (Luo) while Bravo-Solorio et al. consider the entropy of a block as a discriminating feature (Bravo). Lin et al. (Lin) computed the average gray-scale intensities of a block and its subblocks. Wang et al. used the mean intensities of circles with different radii around the block center.

3.(d) Frequency-based:

Fridrich et al. [3] proposed the use of 256 coefficients of the discrete cosine transform as features (DCT). The coefficients of a discrete wavelet transform (DWT) using Haar–Wavelets were proposed as features by Bashar et al. Bayram et al. [6] recommended the use of the Fourier-Mellin Transform (FMT) for generating feature vectors.

4) Feature Extraction: Feature extraction involves reducing the amount of resources required to describe a large set of data. When performing analysis of image one of the major problems stems from the number of variables involved. Feature extraction is basically a method for constructing combinations of the variables to describe the accuracy of the data sufficiently.

5) Matching: High similarity between two feature descriptors is interpreted as a cue for a duplicated region. For block-based methods, most authors propose the use of lexicographic sorting in identifying similar feature vectors [4]. In lexicographic sorting a matrix of feature vectors is built so that every feature vector becomes a row in the matrix. Other authors use the Best-Bin-First search method derived from the kd-tree algorithm [5] to get approximate nearest neighbours.

6) Filtering: Filtering schemes have been proposed in order to reduce the probability of false matches. For instance, a common noise suppression measure involves the removal of matches between spatially close regions. Neighbouring pixels often have similar intensities, which can lead to false forgery detection. Different distance criteria were also proposed in order to filter out weak matches. For example, several authors proposed the Euclidean distance between matched feature vectors [6]. In contrast, Bravo-Solorio and Nandi [7] proposed the correlation coefficient between two feature vectors as a similarity criterion.

7) Post-processing: The goal of this last step is to only preserve matches that exhibit a common behaviour. The most widely used post-processing variant handles outliers [10] by imposing a minimum number of similar shift vectors between matches. A shift vector contains the translation (in image coordinates) between two matched feature vectors.

Therefore, after studying different algorithms for Copy-Move Image Forgery Detection as a part of literature survey the algorithms are compared and summarized in the table below:

TABLE I
COMPARISON BETWEEN DIFFERENT COPY-MOVE IMAGE FORGERY ALGORITHMS

Title	Method	Advantages	Disadvantages
Detection of Copy-Move Forgery in Digital Images[2]	Block based method. Image is divided to blocks and forged parts are detected with exact and appropriate match.	It can detect images with distortion format.	Slow detection process.
Exposing digital forgeries by detecting duplicated image. regions[3]	Block based method. PCA applied to obtain reduced dimensional representation.	More reliable to detect noisy and lossy images.	Sometimes it failed to detects difficult forgeries.
Robust Method for Detection of Copy-Move Forgery in digital images.[4]	Key-point based technique. Wavelet transform technique is used and computes phase correlation to detect similarity.	Lower computational complexity	Duplicated regions through angles and scaled regions cannot detect.

Title	Method	Advantages	Disadvantages
Segmentation-Based Image Copy-Move Forgery Detection Scheme [5]	Key-point based technique. Extracted key points from patches and matched for duplicated regions.	Segment image into semantically independent patches. An accurate estimation of transform matrix is obtained by EM based algorithm [8]	Re-estimation of transform matrix is complex.
Region Duplication Detection Using Image Feature Matching [6]	Key point based method. By calculating SIFT key-points finds pixels within the duplicated regions.	Reliable than other key point techniques	Sometimes it gives vague results.
A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery[11]	Key point based method. Key points are extracted and key point localization is done for detection.	Good at determine the Geometric transformation.	Not good at detection phase with respect to cloned image patch with high uniform texture.

After studying the comparison between different algorithms above, Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching addresses the above mentioned drawbacks by minimizing the computational size and complexity while detecting forgery, also the scheme can robustly respond to noisy and lossy images along with geometric transformations of the forgery regions.

III. Copy move forgery

In a Copy-Move forgery, a part of the image itself is copied and pasted into another part of the same image. This is usually performed with the intention to make an object "disappear" from the image by covering it with a segment copied from another part of the image. Textured areas, such as grass, foliage, gravel, or fabric with irregular patterns, are ideal for this purpose because the copied areas will likely blend with the background. Because the copied parts come from the same image, its noise component, color palette, dynamic range, and most other important properties will be compatible with the rest of the image and thus will not be detectable using methods that look for incompatibilities in statistical measures in different parts of the image. Another Example of the Copy-Move forgery is given in Figure 3

Figure 3 original version of the Jeep(left) with Forged test image "Jeep" (right) [3]

An obvious forgery can be seen in which a truck was covered with a portion of the foliage left of the truck (compare the forged image with its original). It is still not too difficult to identify the forged area visually because the original and copied parts of the foliage bear a suspicious similarity. Figure 4 shows another Copy-Move forgery that is much harder to identify visually.

Figure 4 Test image "Golf" with an unknown original [3]

A visual inspection of the image did not reveal the presence of anything suspicious Any Copy-Move forgery introduces a correlation between the original image segment and the pasted one. This correlation can be used as a basis for a successful detection of this type of forgery. Because the forgery will likely be saved in the lossy JPEG format and because of a possible use of localized image processing tools, the segments may not match exactly but only approximately.

The following are the requirements for the detection algorithm:

1. The detection algorithm must allow for an approximate match of small image segments
2. It must work in a reasonable time while introducing few false positives (i.e. detecting incorrect matching areas).

The framework of the implemented image forgery detection scheme is given as follows:

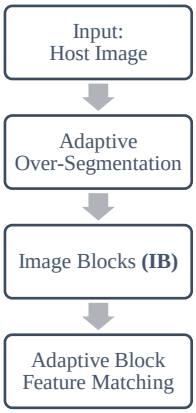


Figure 5 Framework of the copy-move forgery detection scheme up to segmentation [1]

IV. Adaptive Over-Segmentation Algorithm

In the copy-move forgery detection scheme, Adaptive Over-Segmentation algorithm is first implemented, which is similar to the traditional block-based forgery detection methods and can divide the host image into blocks. In previous years, a large amount of block-based forgery detection algorithms have been proposed [3]. Of the 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 well; as a consequence, the recall rate of the block-based methods is always very low, for example, as in [8] and [9]. Moreover, when the size of the host images increases, the matching computation of the overlapping blocks will be much more expensive. To address these problems, the Adaptive Over segmentation method is implemented, 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.

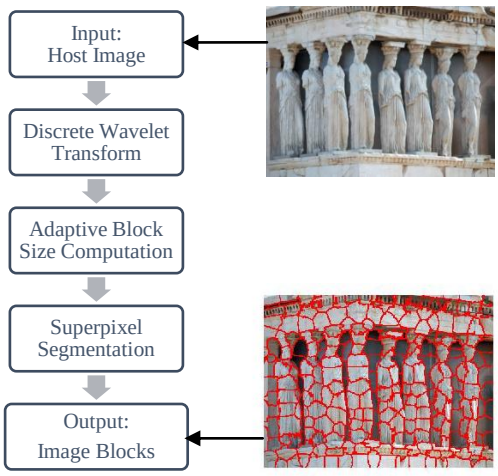
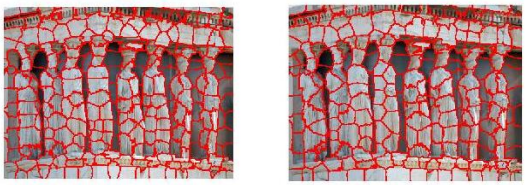


Figure 6 Flowchart of the Adaptive Over-Segmentation algorithm.

Because the host image must divided into nonoverlapping 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 [4] to segment the host image into meaningful irregular superpixels, as individual blocks. The SLIC algorithm adapts a k-means clustering approach to efficiently generate the superpixels, and it adheres to the boundaries very well. Using the SLIC 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 superpixels in SLIC is difficult to decide. For different host images the host images and the copy-move regions are of different sizes and have different content, and in the forgery detection method, different initial sizes of the superpixels can produce different forgery detection results. In general, when the initial size of the superpixels is too small, the result will be a large computational expense; otherwise, when it is too large, the result will be that the forgery detection results are not sufficiently accurate. Therefore, a balance between the computational expense and the detection accuracy must be obtained when employing the SLIC segmentation method for image blocking. In general, the proper initial size of the superpixels is very important to obtain good forgery detection results for different types of forgery regions.



(a) (b)

Figure 7 Host image segmented into number of superpixels S = 250 (a) S = 158 (b) for obtaining the image blocks.

Adaptive Over-Segmentation method that can determine the initial size of the superpixels adaptively based on the texture of the host image. When the texture of the host image is smooth, the initial size of the superpixels can be set to be relatively large, which can ensure not only that the superpixels can get close to the edges but also that the superpixels will contain sufficient feature points to be used for forgery detection; furthermore, larger superpixels imply a smaller number of blocks, which can reduce the computational expense. In this method, the Discrete Wavelet Transform (DWT) is employed to analyze the frequency distribution of the host image. When the low-frequency energy accounts for the majority of the frequency energy, the host image will appear to be a smooth image; otherwise, if the low-frequency energy accounts for only a minority of the frequency energy, the host image appears to be a detailed image. DWT is performed using the 'Haar' wavelet on the host image; then, the low-frequency energy E_{LF} and high-frequency energy E_{HF} can be calculated using (1) and (2), respectively. With the low-frequency energy E_{LF} and high-frequency energy E_{HF}, then calculate the percentage of the low-frequency distribution P_{LF} using (3), according to which the initial size S of the superpixels can be defined as in (4).

$$E_{LF} = \sum |CA_4| \tag{1}$$

$$E_{HF} = \sum_i (|CD_i| + \sum |CH_1| + \sum_{i=1,2,\ldots,4} |CV_1|, \tag{2}$$

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

$$P_{LF} = \frac{ELF}{ELF+EHF}.100\% \tag{3}$$

The initial size of the superpixels S is given as:

$$S = \begin{cases} \sqrt{0.02xMxN} & P_{LF} > 50\% \\ \sqrt{0.01xMxN} & P_{LF} \leq 50\% \end{cases} \tag{4}$$

Where M × N indicates the size of the host image; P_{LF} means the percentage of the low-frequency distribution. In summary, the flow chart of the Adaptive Over-Segmentation method is shown in Fig. 6. DWT is employed to the host image to obtain

the coefficients of the low and high-frequency sub-bands of the host image. Percentage of the low-frequency distribution P_{LF} using is calculated (3), according to which the initial size *S* is determined, using (4). Finally, SLIC segmentation algorithm is employed together with the calculated initial size S to segment the host image to obtain the image blocks (IB). These image blocks are then required to be 'matched' with a certain threshold. To calculate the block matching threshold TR_B, first the different elements of the correlation coefficients are sorted in ascending order as $CC_S = \{CC_1, CC_2, CC_3, \cdots\cdots, CC_t\}$, where $t \leq N(N-1)/2$. Then, the first derivative and second derivative of CC_s, $\nabla(CC_s)$ and $\nabla^2(CC_s)$ as well as the mean value of the first derivative vector $\nabla(CC_s)$ are calculated. The minimum correlation coefficient from among those whose second derivative is larger than the mean value of the corresponding first derivative vector. The selected correlation coefficient value is defined as the block matching threshold TR_B.

$$\nabla^2(CC_s) > \nabla(CC_s) \quad (5)$$

V. Implementation

The host images are 20 high quality true colour JPEG images with 300 dots per inch (dpi) and these 20 images are of 4 resolutions each, that is 737x492, 2048x1536, 1800x1394 and 800x800

The Adaptive Over-Segmentation algorithm is implemented as per the following steps:

1) Feature extraction is performed by employing Scale Invariant Feature Transform (SIFT) on the input host images.
2) Discrete Wavelet Transform (DWT) is employed to obtain the coefficients of the low and high-frequency sub-bands of the host images.
3) The SLIC segmentation algorithm is employed together to segment the host image.
4) The algorithm calculates the initial size of the superpixels for all images per resolution and also to obtain the image blocks (IB).
5) The obtained image blocks are used to calculate the block matching threshold TRB for different resolutions

VI. Results

For a set of 20 images of resolution 737x492

Table II
Percentage Of Low-Frequency Distribution Per 20 Images

Image no	E_{LF}(coefficient)	E_{HF}(coefficient)	P_{LF}(%)
1	8.51	9	48.6
2	3.574	11	24.5
3	3.198	11	22.524
4	10	6.3009	61.34
5	6.53	6.009	52.07
6	4.624	10	31.619
7	7.265	8.15	47.1
8	5.087	4.24	54.54
9	9.564	9.235	50.875
10	4.009	5.25	43.29
11	8.35	7.59	52.38
12	9.25	10.85	46.01
13	3.71	6.11	37.77
14	7.49	10	42.82
15	5.64	8.31	40.43
16	4.51	9.77	31.58
17	8.11	8.46	48.94
18	6.58	6.74	49.39
19	3.811	4.432	46.23
20	7.469	6.96	51.76

It is found that the maximum variation of P_{LF} is between 22.5 to 61.3.

Separating images with P_{LF} above and below 50%,
for 792x492

Table III

Total images with P_{LF}>50%	14	S_1
Total images with $P_{LF}\leq$50%	6	S_2

Similarly, for a dataset of 20 images with resolutions 2048x1536, 1800x1394 and square resolution of 800x800 each. For 2048x1536

Table IV

Total images with P_{LF}>50%	13	S_1
Total images with $P_{LF}\leq$50%	7	S_2

For 1800x1394

Table V

Total images with P_{LF}>50%	13	S_1
Total images with $P_{LF}\leq$50%	7	S_2

For 800x800

Table VI

Total images with P_{LF}>50%	11	S_1
Total images with $P_{LF}\leq$50%	9	S_2

According to the values obtained above, superpixels for different resolutions are as follows:

Table VII
Number Of Superpixels For Different Resolutions

Resolution(MxN)	P_{LF}	Number of Superpixels (S)
737x492	≤50%	60.21
737x492	>50%	85.15
2048x1536	≤50%	177.36
2048x1536	>50%	250.82
1800x1394	≤50%	224.01
1800x1394	>50%	158.4
800x800	≤50%	100
800x800	>50%	141.42

It is seen the number of superpixels significantly changes with the change in resolution and not significantly with the change in P_{LF} variation. Therefore the MxN size that is the resolution of the image is taken into consideration for superpixel calculation.

Determination of Threshold for matching: To calculate the block matching threshold TR_B, the host image is converted into 256 RGB scale shown in figure 8 to determine the threshold the correlation coefficient value is defined as the block matching threshold TR_B and is stated in equation (5)

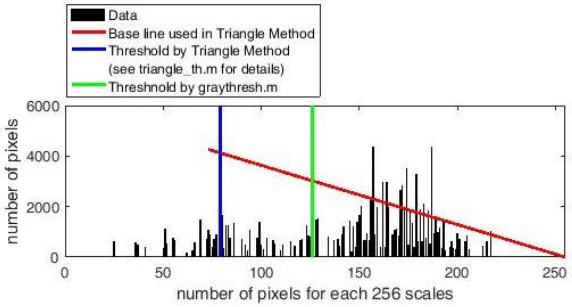


Figure 8 Threshold of images by Triangular Threshold method

For 20 images of different resolutions each the calculated threshold TR_B(unitless) is as follows:

TABLE VIII
THRESHOLD VALUES FOR 20 IMAGES OF DIFFERENT RESOLUTIONS

Resolution (MxN)	Aspect Ratio	Threshold (TR_B)
737x492	3:2	0.58802
2048x1536	4:3	0.49633
1800x1394	5:4	0.61818
800x800	1:1	0.54733

It is observed that the threshold value for lowest resolution 737x492 and highest resolution 2048x1536 is between 0.49 to 0.61 which has 0.11 difference, it is a low difference but consistent and can be improved in the future.

VII. CONCLUSION

In this paper, for a given 20 host images the Adaptive Oversegmentation algorithm is implemented and the initial size of the superpixels is calculated for segmentation of the host images. It is found that the variation of superpixels is dependent on the resolution of the image. The segmented image blocks are then used to determine the threshold values which range from 0.49 to 0.61 for 4 different resolutions.

REFERENCES

[1] [1] Chi-Man Pun, Xiao-Chen Yuan, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching", IEEE Transactions on Information Forensics And Security, Vol. 10, No. 8, Aug 2015.
[2] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, and Elli Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 6, December 2012.
[3] Jessica. Fridrich, "Methods for "Methods for Tamper Detection in Digital Images", Proc. ACM Workshop on Multimedia and Security, Orlando, FL, October 30−31, 1999, pp. 19−23.
[4] Radhakrishna Achanta, Appu Shaji, Kevin Smith, Aurelien Lucchi, Pascal Fua, and Sabine Susstrunk, "SLIC Superpixels Compared to State-of-the-Art Superpixel Methods", IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 34, No. 11, November 2012.
[5] Pravin Kakar,, Sudha, Senior Member, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 3, June 2012.
[6] Guohui Li, Qiong Wu, Dan Tu, Shaojie Sun "A Sorted Neighborhood Approach For Detecting Duplicated Regions In Image Forgeries Based On Dwt And Svd", IEEE Conference National University of Defense Technology, Changsha, China, 2007.
[7] Vivek Kumar Singh, R.C. Tripathi, "Fast and Efficient Region Duplication Detection in Digital Images Using Sub-Blocking Method", International Journal of Advanced Science and Technology Vol. 35, October, 2011.
[8] Harpreet Kaur, Kamaljit Kaur, "A Brief Survey of Different Techniques for Detecting Copy-Move Forgery", International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, ISSN: 2277 128X Issue 4, 2015.
[9] Joshi Chintal J, Prof. Shailendra K Mishra, "Investigating the Possibility of Recognizing the Forgery by Using Spatial & Transform Domain", International Journal of Advance Research in Computer Science and Management Studies Volume 3, Issue 5, May 2015.
[10] B.L.Shivakumar and Lt. Dr. S.Santhosh Baboo, "Detection of Region Duplication Forgery in Digital Images Using SURF" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011 ISSN (Online): 1694-0814.
[11] 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," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.
[12] Database MICC-F220, website http://lci.micc.unifi.it/labd/2015/01/copy-move-forgery-detection-and-localization/