Improved Copy move forgery detection approach-A Comparative study

S. Devi Mahalakshmi (Associate Professor) [1],
Dr. K. Vijayalakshmi (Professor) [2]
Department of Computer Science and Engineering
[1]Mepco Schlenk Engineering College, Sivakasi
[2]Ramco Institute of Technology, Rajapalayam
sindhanadevim27@gmail.com

Abstract - In recent years, digital images are in use in a wide range of applications and for multiple purposes. There are many types of image forgery, the most important and popular type is called copy move forgery, which uses the same image in the process of forgery. Copy–Move and cut-paste forgeries are common type of tampering, where part of an image is copied and pasted to another place to add a new object or to hide/remove an object already present. Most of the copy move forgery detection methods are interest point-based, where the significant key points are extracted and compared to each other to locate similar regions and another category of method called block-based, where the image is divided into overlapping blocks and then features are extracted and compared to find similar regions. In this paper a new hybrid approach is proposed that exploits the block based and the key point based approach for copy-move forgery detection hence it is considered as "hybrid" method. In this paper two approaches have been presented, one with regular regions and another one with irregular image regions for forensic detection of copy move forger and their performance is analyzed and reported. In the first approach, the key points are extracted from the image, and a set of connected triangles are built onto these points to model the foreground regions. Then the triangle region matching is done using their inner angles, color information and area of the triangle regions to locate the copy move tampered regions. In the second approach an adaptive over segmentation method is employed so that the input image is divided into non overlapping regions of irregular shape and key points are extracted from the resultant segmented irregular blocks. For similarity matching of regions a method based on correlation is employed. A comparative study was made by conducting experiments on MICC F220 and MICC F2000 databases.

Index Terms – Copy-Move Forgery Detection, SIFT, SLIC, DWT, adaptive over-segmentation, Delaunay triangles, SURF, forgery region extraction.

1. NTRODUCTION

In recent years, digital images are in use in a wide range of applications and for multiple purposes. They also play an important role in the storage and transfer of visual information, especially the secret ones. With this widespread usage of digital images, in addition to the increasing number of tools and software of digital images editing, it has become easy to manipulate and change the actual information of the image. Therefore, it has become necessary to check the authenticity and the integrity of the image by using modern and digital techniques, which contribute to analysis and understanding of the images content, and then make sure of their integrity.

Digital images in the modern world play very important role in areas like forensic investigation, insurance processing, surveillance systems, intelligence services, medical imaging and journalism. But the basic requirement is that the images should be authentic. The authenticity of photographs has an essential role as these photos are popularly used as supporting evidences and historical records in growing number and wide range of applications from forensic investigation, journalistic photography, criminal investigation, law enforcement, insurance claims and medical imaging.

In the past few years, there has been a growing interest in the development of detection of editing in images. With the advancement of technology and availability of fast computing resources, it is not very difficult to manipulate or forge the digital images. For editing the photos digitally, there are numbers of different photo editing software and tools available.

Image editing is a technique to improve look and feel of photographs and compose two or more different photographs or graphics to make something more appealing, interesting and unique concept. It is very difficult to prove that a particular photograph is forged and also sometimes it is impossible to identify. Each image has its own unique characteristics or properties. When an image is edited, the characteristics of an image are changed. Then the changes in the characteristics are examined and whether the image is edited or not is determined. Any alteration in an original image in bad faith is regarded as Image forgery.

Digital image forgery detection techniques are categorized into active and passive approach. In active approach, the digital image requires some pre-processing techniques such as watermark embedding or signature generation at the time of creating an image, which would limit their application in practice. Moreover, there are more digital images in internet without digital signature or watermark. In such scenario active approach could not be used to find the forgery of the image. Unlike the watermark-based and signature-based methods; the passive technology does not need any digital signature generated or watermark embedded into the image in advance.

One of the main objectives of Image Forensics techniques is to understand what kind of tampering has been applied. Images can be doctored in several ways [28]: photo-compositing, re-touching, enhancing are only some examples of typical image alterations. Although many tampering operations generate no visual artifacts in the image, they will nevertheless affect its inherent statistics.

The rest of the paper is organized as follows: Section 2 explains the related CM works, Section 3 explains the proposed system in details, Section 4 presents the experimental results and finally, Section 5 concludes the paper.

2. RELATED WORK

Copy-Move is a specific type of image tampering, where a part of the image is copied and pasted into another part of the same image (Figure 1).

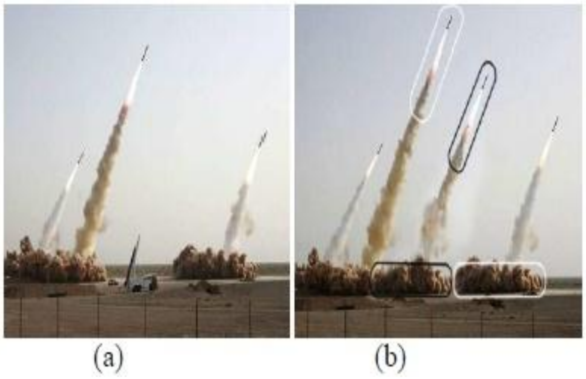


Figure 1. An example of copy-move forgery: (a) three missiles in original image (b) four missiles in tampered image.

In previous years, many forgery detection methods have been proposed for copy-move forgery detection. Among the existing methods, the copy-move forgery detection methods can be categorized into two main kind: block-based approaches [1]–[13] and feature key point-based algorithms [14]–[19].

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. In Fridrich et al. [1] forgery detection method the input image is segmented into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks are obtained and used for matching to identify the tampered regions. Popescu and Farid [2] applied Principal Component Analysis (PCA) to reduce the feature dimensions. Luo et al. [3] used the RGB color components and direction information as block features. Li et al. [4] used Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract the image features. Mahdian and Saic [5] calculated the 24 Blur-invariant moments as features. Kang and Wei [6] calculated the singular values of a reduced-rank approximation in each block. Bayram et al. [7] used the Fourier-Mellin Transform (FMT) to obtain features. Wang et al. [8], [9] used the mean intensities of circles with different radii around the block center to represent the block features. Lin et al. [10] used the gray average results of each block and its sub-blocks as the block features. Ryu et al. [11], [12] used Zernike moments as block features. Bravo-Solorio and Nandi [13] used information entropy as block features.

As an alternative to the block-based methods, keypoint based forgery detection methods were proposed, in which keypoints are extracted from the query image and matched over the entire image to resist some image transformations. In [14]–[16] and [18], the Scale-Invariant Feature Transform (SIFT) [20] was applied to the host images to extract feature points, which were then matched to one another. When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points were defined as the forgery region. In [17] and [19], the Speeded Up Robust Features (SURF) [21] 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 [22]. An interesting work by Christlein et al. [22] compares and evaluates the results obtained with different approaches to the problem of copy-move forgery detection.

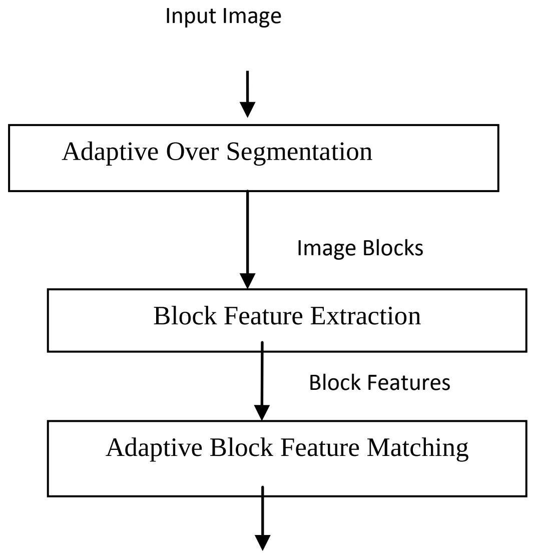
Most of the existing block-based forgery detection algorithms use a similar approach, but they employ different feature extraction methods to extract the block based features. Even though these algorithms are effective in forgery detection, they have few limitations such as 1) the query image is divided into over-lapping rectangular blocks, which would makes this approach as computationally expensive for larger size images; 2) These methods cannot address significant geometrical transformations of the forgery regions; and 3) their recall rate is low because their blocking method is a regular shape. Many of the existing keypoint-based forgery detection methods evade the first two issues, that is they reduce the computational complexity and can successfully detect the forgery, even when some attacks exist in the host images; but the recall rate of the existing keypoint-based forgery methods were very poor.

3. PROPOSED APPROACH

In this paper two approaches have been proposed that combines both the block and key point based forgery detection approaches. In the first approach, the input image is divided into irregular blocks using Simple Linear Iterative Clustering (SLIC) algorithm, an adaptive over segmentation algorithm then matching of similar region is done using a method based on correlation and color features. In the second approach the key points are extracted from the image, and a set of connected triangles are built onto these points to model the foreground regions. Then matching of similar triangle regions is performed using their inner angles, color information and area of the triangle regions to locate the copy move tampered regions.

3.1. Adaptive over segmentation based copy move forgery detection

The proposed approach (Figure 2) is similar to the traditional block based forgery detection methods that divides the input image into blocks of non overlapping regions but the regions are of irregular shape. Then feature points were extracted from each image block as a block feature and block features are matched to locate forged region using the labeled feature points. To identify the forged region more accurately local color features are used. The non overlapping segmentation using the SLIC method can decrease the computational expenses compared with the overlapping blocking. Irregular and meaningful region can characterize the forged region more accurately than regular regions.



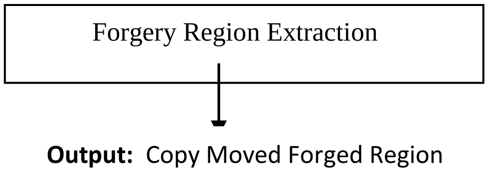


Figure 2. Irregular block based copy move forgery detection-Proposed approach.

A. Adaptive Over-Segmentation

Simple Linear Iterative Clustering (SLIC) algorithm is used to segment the input image into meaningful irregular superpixels, as individual blocks. Superpixels are perceptually meaningful atomic regions that can be obtained by over segmentation.

The SLIC algorithm adapts a k-means clustering approach to efficiently generate the superpixels, which is more memory efficient, adheres to the boundaries very well. Here the performance of the segmentation is improved by limiting the search space to a region proportional to the superpixel size, the number of distance calculations is reduced which intern decreases the complexity to be linear in the number of pixels N. Hence SLIC approach improves the performance of segmentation algorithms. This algorithm also provides a complete control over the size and compactness of the superpixels by using a weighted distance measure by considering both color and spatial proximity simultaneously. In general, the proper initial size of the superpixels is very important in SLIC approach to obtain good forgery detection results for different types of forgery regions.

SLIC performs clustering of pixels in the five-dimensional space by combining 3D color space and 2D image plane to generate compact, nearly uniform superpixels efficiently. Here the local clustering of pixels is done in the 5-D space defined by the L, a, b values of the CIELAB color space and the pixel coordinates x, y.

In SLIC, the clustering procedure begins with an initialization step where ‘S’ regularly spaced k initial cluster centers $C_i=[l_i \; a_i \; b_i \; x_i \; y_i]^T$ were sampled and they were moved to seed locations corresponding to the lowest gradient position in a 3 × 3 neighborhood. This is done to avoid placing them at an edge position and also to reduce the probability of choosing a noisy pixel as center of superpixel. While clustering, each pixel in the image is associated with the nearest cluster center whose search area overlaps with this pixel. After all the pixels are associated with the nearest cluster center, a new center is computed as the average $[\, l \; a \; b \; x \; y]^T$ vector of all the pixels belonging to the cluster. The residual error E between the new cluster center locations and previous cluster center locations is estimated using

L2 norm. Then iteratively repeat the process of clustering and recomputing the cluster center until error converges, but it has been proven that 10 iterations are suffices for most of the images to obtain the segmented irregular shapes. The resultant clusters in the labxy color-image plane space correspond to SLIC superpixels. This introduces a problem while defining the distance measure D which computes the distance between a pixel i and cluster center C_k in the above clustering based algorithm. A pixel's color is represented in the CIELAB color space $[l\ a\ b]^T$, whose range of possible values is known from the color model specifications. On the other hand the pixel's position $[x\ y]^T$ range may be different for different sized images. Thus defining D to be the 5D Euclidean distance in Labxy space will lead to inconsistencies in cluster formation for different superpixel sizes.

In the adaptive over-segmentation method the initial size of the superpixels is determined adaptively based on the texture of the host image. When the texture of the host image is smooth or nearly smooth, the initial size of the superpixels must be set to be relatively large, to ensure that the superpixels selected will contain sufficient feature points to be used for forgery detection; Moreover, selecting larger superpixels imply a smaller number of blocks, which can reduce the computational expense while performing block matching. On the other hand, when the texture of the host image has more detail, then the initial size of the superpixels can be selected as relatively small, to ensure good forgery detection results.

B. Adaptive Block Size Computation using DWT

In the proposed method, the Discrete Wavelet Transform (DWT) is used to select the appropriate size for the superpixels by analysing the frequency distribution of the host image. From that analysis, it is proven that when the low-frequency energy accounts for the majority of the frequency energy, the appearance of the host image will be a smooth image; otherwise, if the low-frequency energy accounts for only a minority of the frequency energy, then the host image appears to be a detailed image.

To obtain initial superpixel value a four-level DWT is performed on the host image, using the 'Haar' wavelet, to obtain the coefficients of the low- and high-frequency sub-bands of the host image. Then, the low-frequency energy E_{LF} and high-frequency energy E_{HF} are calculated. Low Frequency Energy E_{LF} is estimated by calculating the summation of the fourth level of approximation coefficients obtained through DWT. High Frequency Energy is obtained by calculating the summation of four levels of detailed coefficients such as horizontal coefficients, vertical coefficients, and diagonal coefficients. With the estimated low-frequency energy E_{LF} and high-frequency energy E_{HF}, the percentage of the low-frequency distribution P_{LF} is estimated , according to which the initial size *S* of the superpixels is also defined as shown in Equations (1), (2), (3), (4) and (5)

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

Where CA_4 is the 4th level approximation coefficients.

$$E_{HF}=\sum_i(\sum|CD_i|+\sum|CV_i|+\sum|CH_i|) \qquad (2)$$

Where i = 1, 2, 3, 4. (Summation of 4 levels detailed coefficients that is horizontal, vertical and diagonal).

$$P_{LF} = (E_{LF}\ /\ \text{Total Energy}) *100 = (E_{LF}\ /\ (E_{LF} + E_{HF}))*100 \qquad (3)$$

$$S=\sqrt[2]{M*N*0.02} \quad \text{if } P_{LF} > 50\% \qquad (4)$$

$$S=\sqrt[2]{M*N*0.01} \quad \text{if } P_{LF} \leq 50\% \qquad (5)$$

Finally SLIC segmentation algorithm together with the calculated initial size S, segment the input image into irregular non overlapping image blocks.

C. Block Feature Extraction

Block feature extraction process is employed for the calculation of the similarity between the features extracted from the irregular block regions based on Scale Invariant Feature Transform (SIFT) process. The process identifies the key points from the image blocks. The key points extracted from the irregular blocks were matched based on distance calculated. The derivative of the images is calculated. The calculated values give the changes in the color and the gray scale values of the image which indicates the information in the image.

SIFT is an algorithm to detect and describe local features in images. To perform reliable recognition, it is important that the features extracted from the image should be detectable even under changes in the image scale, noise and illumination. Such key points usually present on image regions with high-contrast, such as object edges.

D.Block Feature Matching

The block features obtained from the previous step is used to calculate the correlation coefficients of the image blocks. Correlation Coefficients of the image block indicate the number of matched feature points between the corresponding two image blocks. If there were N blocks after adaptive over segmentation (N*(N-1))/2 correlation coefficients can be generated 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 point matching threshold TR_p as shown in Equation (6). TR_p is set to 2 to provide a good trade-off between the matching accuracy and miss probability.

$$d(fa, f_b) \cdot TR_p \leq d(f_a, f_i) \qquad (6)$$

Where d (fa, f_b) is the Euclidean distance between the feature points f_a and f_b and d(f_a, f_i) is the Euclidean distance between the keypoints f_a and all of the other keypoints in the corresponding block as stated in equation (7) and (8) respectivly.

$$d(fa, f_b) = \sqrt[2]{(xa - xb)^2 + (ya - yb)^2} \qquad (7)$$

$$d(fa, f_i) = \sqrt[2]{(xa - xi)^2 + (ya - yi)^2} \qquad (8)$$

Where $i = 1, 2, ...n; i \neq a, i \neq b$

Block matching threshold and feature point matching threshold are calculated in order to avoid false matching and improve the accuracy rate in the detection of copy moved forged part.

To calculate the block matching threshold TR_B the first derivative and second derivative of the correlation coefficients as well as the mean value of the first derivative vector are calculated. Minimum correlation coefficient is selected among those whose second derivative is larger than the mean value of the corresponding first derivative vector.

When the correlation coefficient of the block pair is larger than the $TR_{B,}$ the corresponding block pair is determined to be the matched block. The matched feature points in the matched blocks are labeled to indicate the suspected forgery regions. The equation 4.11 indicates that the two feature points were matched when their Euclidean distance is greater than feature point matching threshold in order to avoid false matching among the blocks. With these two block matching threshold and feature point matching threshold most of the false matching can be avoided.

E. Forgery Region Extraction

To locate the forgery region more accurately forgery region extraction algorithm is used. Replace the labeled feature points with the small superpixel in order to obtain the suspected regions. For each suspected region the 8 neighboring blocks are defined as with θ = {45°, 90°, 135°, 180°, 225°, 270°, 315°, 360°}, then the local color feature of the superpixels that are neighbors to the suspected regions are extracted. Using this color features the neighboring superpixels are merged into the corresponding suspected regions. Finally, a close morphological operation is applied to the merged region that fills the gaps in the merged regions to generate the detected copy-move forgery regions with the shape of the region unchanged. TR_{sim} is the threshold to measure the similarity between the local color features. Finally, the structural element that is used in the close operation is defined as a circle whose radius is related to the size of the input image.

3.2. Copy Move Forgery Detection using Triangle Regions

The steps involved in the proposed copy-move forgery detection approach are shown in the Figure 3.

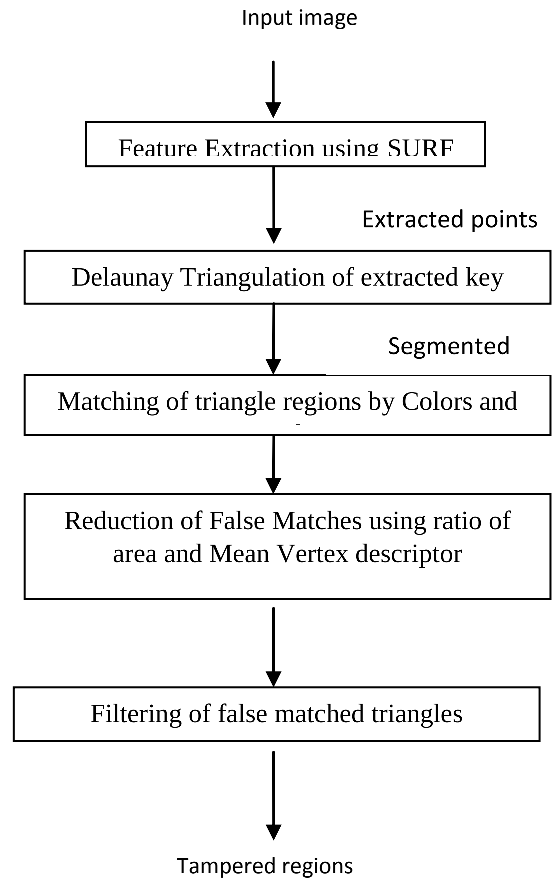

Input image
Feature Extraction using SURF
Extracted points
Delaunay Triangulation of extracted key
Segmented
Matching of triangle regions by Colors and
Reduction of False Matches using ratio of area and Mean Vertex descriptor
Filtering of false matched triangles
Tampered regions

Figure 3. Improved Copy move forgery detection using triangle regions

A. Feature Extraction and Delaunay Triangulation of key points

In the proposed work all the objects in a scene are represented as a set of connected triangles which is popularly used in computer graphics for the representation of 2D scenes and these triangles are analyzed to find matching triangles and thereby matching copy moved regions in the image. In the feature extraction stage, the interest keypoints and their features are extracted using SURF (Speeded-Up Robust Features) algorithm which produces 64 dimensional feature representation, with reduced time for feature computation and matching and exhibits increased robustness. Hence the SURF features are employed for the extraction of points of interest of the image.

After the extraction of key points, the Delaunay Triangulation is built onto the extracted key points. While there are numerous algorithms for triangulations of key points, the most flattering geometric property of the Delaunay triangulation called Delaunay criterion makes it very useful. For a set of points in 2-D space, a Delaunay triangulation of these points ensures that the circumcircle associated with each triangle contains no other key points in its interior. Figure 4 shows two examples for Delaunay Triangulation where the circumcircle associated with triangle T1 and T2 are empty. No other points present in their interior. This triangulation is called Delaunay triangulation.

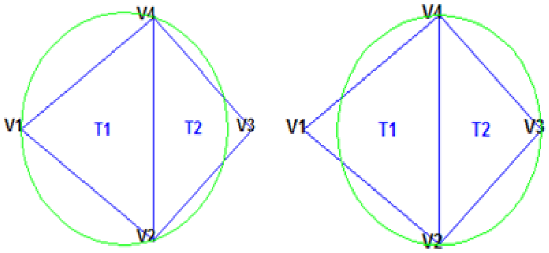


Figure 4. Example of Delaunay Triangulation.

Delaunay triangles (Dyer et al. 2009) are said to be "well shaped" because of satisfying the empty circumcircle property, according to which triangles with large internal angles are selected over ones with small internal angles to perform triangulation of key points. Also, the Delaunay triangulation connects key points in a nearest-neighbor approach. These two characteristics, well-shaped property and the nearest-neighbor selection have important implications in connected triangle representation and motivate the use of Delaunay triangulations in scattered key points. Generally no key points are extracted from the outer parts of the image, and so uniformly arbitrary points are added onto the borders of the image which aids to include the image region near the vertical or the horizontal borders in triangulation.

B. Triangle Region Matching

Once the Delaunay Triangulation is done on key points they are processed to find matching triangles by using inner features of the triangles (such as color), their geometrical properties (angles), the feature of the vertices that compose the triangles (local descriptors) and mean vertex descriptors of those triangle pair.

i. Matching of triangle regions by Colors and Angles

To find possible copy-moved regions, that is matched region or matching triangles the proposed system search for similar triangles in the first level by analyzing two different features: color and angles.

Calculation of Dominant color features

In this method, the inner content of the triangles that is the color detail is analyzed. The first N dominant colors are extracted from each triangle. For that, each color channel is quantized using B number of bins and a 3D histogram is built using the pixels within the triangle where N is selected as 4 from experiments with bin size B = 8. The dominant colors of each triangle are selected based on the N most frequent values of the histogram. Therefore, each triangle is represented by 3*N values (N values per channel). Here the triangles are sorted according to the L1 norm of their color vectors. The sorted list of triangles is scanned and then the features of each triangle are compared with the next triangles in the list, within a fixed window. There are two types of window methods available, such as fixed and adaptive window. Here the fixed window method is followed, because an adaptive window approach proved to be slower than the fixed window approach, without improving results. This fixed window size is computed as a percentage of the total number of triangles available for matching.

Calculation of Angles

In this method, the geometric property of the triangles (angles) is analyzed. The inner angles of each triangle are computed and angles are ordered in counterclockwise starting from the maximum one.

Triangle matching by color and angles

To find the similarity between two triangle regions two measures such as the Sum of the Absolute Deviation (SAD) of the color vectors and of the angles of triangle are being used. If i and j (j>i) are the indexes of the two triangles to be compared with the SAD of color vector and angles as stated in Equation (9) and (10)

$$\sum_{t=1}^{3}\left|C_t^i - C_t^j\right| \le ColorTH\ ,where(\ j-i\ )<W_s \qquad (9)$$

$$\sum_{l=1}^{3}\left|a_t^i - a_l^j\right| \le \ AngelTH, where(j-i)<W_s \qquad (10)$$

where Ws is the fixed window size (a percentage of the number of triangles), C is the color vector (made of 3*n values), a_t are the angles in radians (in which the angles are sorted as described above), color TH is the color threshold (set as 0), AngleTH is the angle threshold (set as 0.25) by empirical analysis. The size of the fixed window is chosen as Ws=Ntri/50, where Ntri is the number of triangles obtained from the input image given.

If these two measures are below the threshold, ColorTH and AngleTH for any two triangles, then the two triangles are considered as similar. It is proven that the inner angles of similar triangles are equal, even if one of the two triangle region is rotated or scaled with respect to the other one, if the angles are taken in the correct order. Thus by locating such similar triangle regions in the given image, the proposed method is capable of finding copy move forgery even if the tampered regions are subjected to geometric transformation.

ii. Matching of Triangle Regions by Mean Vertex Descriptors

In this method, the property of the vertices that forms the triangles, that are the points of interest of the image is analyzed. For a list of pairs of triangles, compute the Mean Vertex Descriptor (MVD) as the average value of the feature vectors extracted onto the geometric vertices of the triangles. The Mean Vertex Descriptor V_{mi} is obtained as shown in Equation (11).

$$V_{mi}=\frac{V_{1i}+V_{2i}+V_{3i}}{3} \qquad (11)$$

where Vj = 1…3 corresponds to 3 vertices of triangle formed, i = 1…N where N is the number of the Delaunay Triangles inside the image. To locate the possible tampered regions, the triangles are ordered according to the L1 norm of their MVDs and the MVD of each triangle is compared to the next ones in the list, within a fixed window of size Ws. If the L1 distance of their corresponding MVD is lower than a threshold, then the two triangles are considered as matched triangles.

If j and k are the indexes of the two triangles to be compared and V_{mj}, V_{mk} are the corresponding MVDs thrn the two triangles are compared as shown in Equation (12).

$$\left|V_{mj}-V_{mk}\right|\leq VertexTH \qquad (12)$$

where VertexTH is the vertex threshold (set as 0.25).

Once the reduced list of matching pairs of triangles is obtained, the image region corresponds to those triangles regions are considered to be the tampered image.

C. Filtering False Match – Stage- I

While doing triangle region matching sometimes, the false matches may be obtained. False matching reduction is achieved using ratio of the area of the triangle pairs. In this method, the geometric property of the triangle (such as area) is analyzed to find false matches. For a set of matching triangles, area of those triangles is estimated. Let A_j and A_k be the area of two triangles j and k, to reduce false matched triangle pairs, compare the triangles for similarity only if the ratio between their areas satisfying the condition stated in Equation (13).

$$r_A=\frac{min\left(A_{j,}A_k\right)}{max\left(A_{j,}A_k\right)}\geq 0.25 \qquad (13)$$

This approach limits the maximum detectable scale (to 2) but removes 20-25% of wrong matches. After the matching process, there will be a reduced list of pairs of triangles available.

D. Filtering False Match - Stage -II

False matching of triangles is reduced using the ratio of areas of the pairs of triangles taken as given in Equation (13). In addition to this reduction, the proposed work applies a filtering method where the false matched triangles are further reduced by considering the pixel region around the centroid of the triangles to be matched.

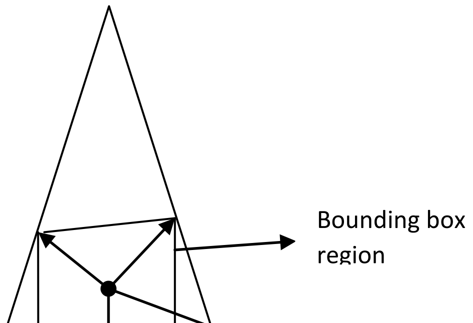


Figure 5. Bounding rectangle construction for filtering

For a set of matching triangles, the centroid is calculated. Then a bounding rectangle region is formed as shown in Figure 5, around the centroid of the triangle and the pixels within this bounded region are taken into account for further processing. For each matched triangles, the mean value of pixel inside the bounded region is estimated. If the difference between the mean values of two matched triangles is below a threshold value, then those two triangles are considered similar. If j and k are the indexes of the two triangles to be compared and M_j, M_k are mean values estimated for the corresponding bounding region then the two triangles are compared as shown in Equation (14)

$$\left|M_j-M_k\right|\leq MeanTH \qquad (14)$$

where Mean TH is the mean threshold (Value in the range 40 to 60).

The matched triangles that are not satisfying the above conditions are eliminated. This estimate identifies the similar regions correctly even if they are subject to geometric transformation such as rotation or scaling. The bounding region obtained using the above approach will be of same size even if one of the regions is rotated with any degree of rotation angle. Similarly the similarity of the two regions are measured with a threshold value MeanTH this estimate will identify the similar regions even if one of the regions is rescaled.

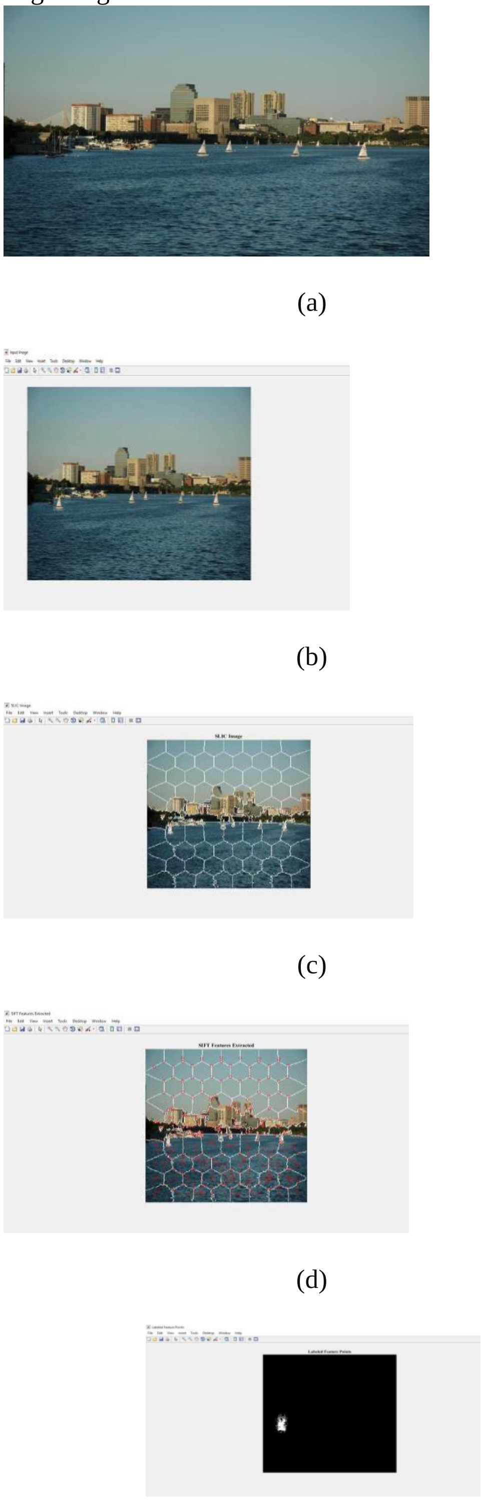
4. EXPERIMENTAL RESULTS

DATA SET

Experiments are conducted using the two ground truth databases MICC F220 and MICC F2000 for CMFD algorithms. They consist of 220 and 2000 images, respectively. In each of these datasets, half of the images are tampered.

A. Results for Detecting Copy-Move Image Forgery using irregular blocks

Figure 4 shows the results for detecting Image Copy-Move Forgery using irregular blocks. The original image and the tampered image are shown in figure 6(a) and (b) respectively. Some part of the original image has been copied to other areas to get the tampered image. Figure 6(c) is the SLIC segmented tampered image. Figure 6(d) shows the SIFT Feature extraction for the tampered image. Figure 6(e) and 6(f) shows the detected copy move forged region.



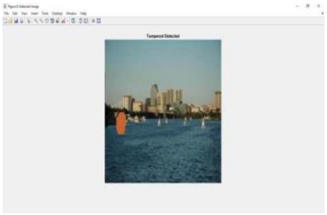
(a)

(b)

(c)

(d)

(e)

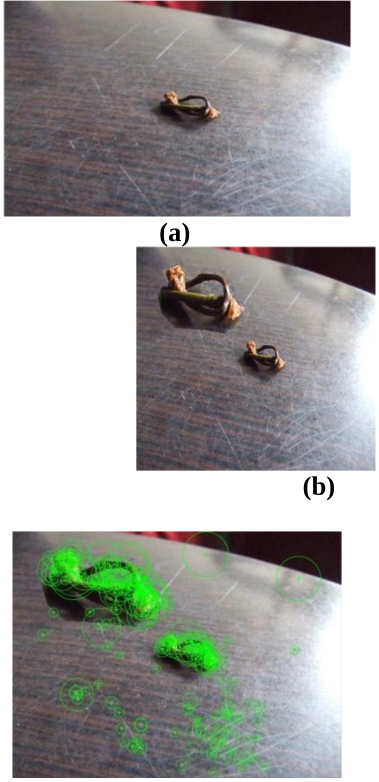


(f)

Figure 6 Results for copy-move forgery detection (a) Original image (b) Tampered image with copy move forgery (c) SLIC segmented tampered image (d) SIFT feature extraction (e)&(f) Tampered region detection

B. Results for Detecting Copy-Move Image Forgery using triangular blocks

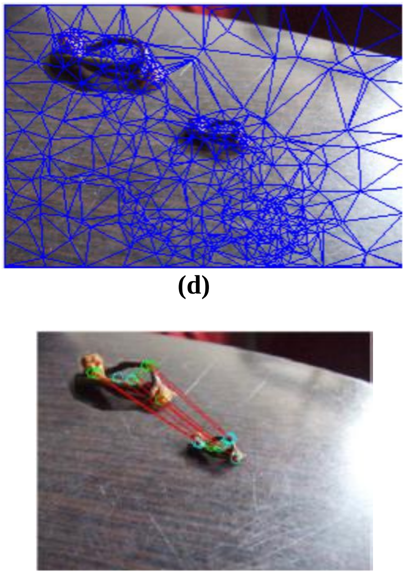
In copy-move forgery, some part of the image has been copied and pasted on the other side of the same image. Figure 7 shows the results for copy-move forgery detection where Figure 7(a) shows the original image and 7(b) shows the tampered image with copy move forgery 7(c) shows the Feature Extraction, 7(d) shows the Delaunay Triangulation and 7(e) shows the result of tampered region detection.



(a)

(b)

(c)



(d)

(e)

Figure 7.

Figure 7. Results for copy-move forgery detection (a) Original image (b) Tampered image with copy move forgery (c) SURF feature extraction (d) The Delaunay Triangulation (e) Tampered region detection

C. Performance Analysis of Proposed Work for Copy Move Forgery Detection

i. Performance Metrics

Two different metrics are used to evaluate the performance of the proposed system at pixel level:

- Recall
- Precision

To compute these three metrics, the source and the destination areas of every copy moves as binary masks of the whole dataset are saved. The "reference area" A_R is the ground truth. The detected area A_D is the output mask of the proposed methods, created as a binary mask in which the pixels that are inside the matching triangles are set to 1.

Recall

Generally the performance measure recall also known as sensitivity is the fraction of relevant instances that have been retrieved over total relevant instances in the image. Here Recall is defined as the ratio of the number of pixels in the intersection of the detected area A_D and the reference area A_R, and the number of pixels in reference area A_R as shown in Equation (6.7).

$$R = \frac{n(A_D \cap A_R)}{n(A_D)} \qquad (6.7)$$

where R – Recall value, A_R - Reference Area, A_D - Detected Area.

When this ratio R tends to 1, the detected tampered area A_D covers the whole A_R implies that the forgery detection by the proposed system nearly 100% accurate, but there is no information about pixels outside A_R. If it tends to 0, A_D and A_R have a smaller intersection leads to false detection.

Precision

Usually precision is the fraction of relevant instances among the retrieved instances. Precision is computed as the ratio of the number of pixels in the intersection of the detected area A_D and the reference area A_R, and the number of pixels in A_D as given in Equation (6.8). When P tends to 0, the whole detected area has no intersection with the reference hence A_D is wrongly detected region. If it tends to 1, fewer pixels of A_D are labeled outside A_R .

$$P = \frac{n(A_D \cap A_R)}{n(A_D)} \qquad (6.8)$$

where P – Precision.
A_R - Reference Area.
A_D - Detected Area.

For the analysis of the results in image level the following two metrics are used.

True Positive Rate (TPR) is computed as the ratio of the number of images detected correctly and the total number of images considered.

False Positive Rate (FPR) is computed as the ratio of the number of images detected wrongly and the total number of images considered.

ii. Performance analysis

Experiments have been conducted and the detection rate of for Copy move forgery detection using triangle blocks based approach is compared with the existing system Edoardo Ardizzone et al. 2015 as shown in Table 1. At pixel level the Precision and Recall are determined for the tested images and stated in Table 1. The tabulated results proved that the proposed system with additional filtering precision is better than the existing method.

Table 1. Performance analysis of Copy-move forgery detection using Precision and Recall

Forgery Detection Methods	**Precision (%)**	**Recall (%)**
Copy move forgery detection using triangle matching	84	66
Proposed Method (with filtering)	**90**	**74**

(Source : Edoardo Ardizzone et al. 2015)

Table 2. Performance analysis of Copy-move forgery detection using TPR and FPR (Proposed Vs Existing Work)

Forgery Detection Methods	**True Positive Rate (%)**	**False positive Rate (%)**

Copy move forgery detection using triangle matching	83	17
Proposed Method (with filtering)	**88**	**12**

(Source :Edoardo Ardizzone et al. 2015)

Similarly Table 2 presents TPR and TNR estimates at image level. The tabulated results shows that the proposed system with filtering approach to reduce the false matches the TPR is improved and also the reduction in false matching of triangle region decrease the false positive rate. From the results it is observed that the proposed work for copy move forgery detection using two level filtering performs well than the existing work Edoardo Ardizzone et al. 2015 by employing two levels of false matching reduction. Hence it out performs the existing system.

In Table 3 the performance of the adaptive irregular block based copy move forgery approach is compared with the copy move forgery detection using triangle blocks based method with additional filtering. It is proven that the performance of the irregular block based scheme is better than the triangle block based method.

Table 3: Performance Analysis of adaptive irregular block based method versus copy move forgery detection using triangle blocks based method with additional filtering**.**

Method	**Precision**	**Recall**
Triangle blocks based method with additional filtering**.**	90	74
Adaptive irregular block based method	96.9	100

5. CONCLUSION & FUTURE WORK

The proposed method is used to find whether the image is forged one or not. This work deals with the detection of copy-move forgery. Two key point based approaches one using Speeded-Up Robust Features (SURF) with triangulation algorithm where the Delaunay Triangulation can be built onto the extracted SURF keypoints. Matching process between triangles was done using the features of the triangles (colors), shapes of the triangles (angles) and the local feature vectors extracted onto the vertices of the triangles (local descriptors). To reduce those false positives, filtering is applied. Finally, the tampered regions of the image can be identified. This method is robust to geometric transformations like scaling, rotation. Another approach where the adaptive over segmentation algorithm is employed to segment the input image into non-overlapping and irregular blocks adaptively according to the texture of the input 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 suspected forgery regions. Next, the morphological operation is applied to the suspected regions to generate the forged regions. Experiments conducted using and performance of both the approaches are analysed. The proposed work focuses only on detection of Copy-Move Forgery. The future work is to identify other attacks such as Enhancing and Splicing Attack and to find copies also in case of some other type of transformations like anisotropic deformations. Another idea is to develop some post-processing techniques, to recover some missing matches. The proposed approach can further applied to other types of media, such as video and audio.

REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukáš, “Detection of copy–move forgery in digital images,” in *Proc. Digit. Forensic Res. Workshop*, Cleveland, OH, Aug. 2003.

[2] A. C. Popescu and H. Farid, “Exposing digital forgeries by detecting duplicated image regions,” Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep. TR2004-515, 2004.

[3] W. Luo, J. Huang, and G. Qiu, “Robust detection of region-duplication forgery in digital image,” in *Proc. 18th Int. Conf. Pattern Recognit. (ICPR)*, Aug. 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 *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2007, pp. 1750–1753.

[5] B. Mahdian and S. Saic, “Detection of copy–move forgery using a method based on blur moment invariants,” *Forensic Sci. Int.*, vol. 171,nos. 2–3, pp. 180–189, 2007.

[6] X. B. Kang and S. M. Wei, “Identifying tampered regions using singular value decomposition in digital image forensics,” in *Proc. Int. Conf. Comput. Sci. Softw. Eng.*, Dec. 2008, pp. 926–930.

[7] S. Bayram, H. T. Sencar, and N. Memon, “An efficient and robust method for detecting copy–move forgery,” in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, Apr. 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 *Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES)*, Nov. 2009, pp. 25–29.

[9] J. W. Wang, G. J. Liu, Z. Zhang, Y. W. Dai, and Z. Q. Wang, “Fast and robust forensics for image region-duplication forgery,” *Acta Automat. Sinica*, vol. 35, no. 12, pp. 1488–1495, 2009.

[10] H. J. Lin, C. W. Wang, and Y. T. Kao, “Fast copy–move forgery detection,” *WSEAS Trans. Signal Process.*, vol. 5, no. 5, pp. 188–197, 2009.

[11] S. J. Ryu, M. J. Lee, and H. K. Lee, “Detection of copy-rotate-move forgery using Zernike moments,” in *Information Hiding*. Berlin, Germany: Springer-Verlag, 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 Trans. Inf. Forensics Security*, vol. 8, no. 8, pp. 1355–1370,Aug. 2013.

[13] S. Bravo-Solorio and A. K. Nandi, “Exposing duplicated regions affected by reflection, rotation and scaling,” in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP)*, May 2011, pp. 1880–1883.

[14] 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.

[15] X. Pan and S. Lyu, “Region duplication detection using image feature matching,” *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 4, 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,” *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 1099–1110, Sep. 2011.

[17] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, “Image copy–move forgery detection based on SURF,” in *Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES)*, Nov. 2010, pp. 889–892

[17] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, “Image copy–move forgery detection based on SURF,” in *Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES)*, Nov. 2010, pp. 889–892.

[18] P. Kakar and N. Sudha, “Exposing postprocessed copy–paste forgeries through transform-invariant features,” *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 3, pp. 1018–1028, Jun. 2012.

[19] 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.

[20] D. G. Lowe, “Object recognition from local scale-invariant features,” in *Proc. 7th IEEE Int. Conf. Comput. Vis.*, Sep. 1999, pp. 1150–1157.

[21] H. Bay, T. Tuytelaars, and L. Van Gool, “SURF: Speeded up robust features,” in *Computer Vision*. Berlin, Germany: Springer-Verlag, 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 Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.

[23] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Süsstrunk, “SLIC superpixels compared to state-of-the-art superpixel methods,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 34, no. 11, pp. 2274–2282,Nov. 2012.

[24] Dyer, R, Zhang, H &Möller, T 2009, ‘A survey of Delaunay structures for surface representation’, GrUVi Lab, Burnaby, BC, Canada, School Comput. Sci., Tech. Rep. TR 2009-01, 2009.

[25] Ardizzone, E, Bruno, A &Mazzola, G 2015, ‘Copy-move forgery detection by matching triangles of keypoints’, IEEE Transaction on Information Forensics and Security, vol. 10, no. 10, pp. 2084-2094.

[26] E. Ardizzone, A. Bruno, and G. Mazzola, “Detecting multiple copies in tampered images,” in *Proc. 17th IEEE Int. Conf. Image Process. (ICIP)*, Sep. 2010, pp. 2117–2120.

[27] In an Iranian image, a missile too many, http://thelede.blogs.nytimes.com/2008/07/10/in-an-iranian-image-a-missile-too-many/

[28] H. T. Sencar and N. Memon, “Overview of state-of-the-art in digital image forensics,” *Algorithms, Archit. Inf. Syst. Secur.*, vol. 3, pp. 325–348, Dec. 2008.