Iranian Journal of Electrical and Electronic Engineering

Journal Homepage: ijeee.iust.ac.ir

Research Paper

Detection of Copy-Move Forgery in Digital Images Using Scale Invariant Feature Transform Algorithm and the Spearman Relationship

A. Fattahi* and S. Emadi*(C.A.)

Abstract: Increased popularity of digital media and image editing software has led to the spread of multimedia content forgery for various purposes. Undoubtedly, law and forensic medicine experts require trustworthy and non-forged images to enforce rights. Copy-move forgery is the most common type of manipulation of digital images. Copy-move forgery is used to hide an area of the image or to repeat a portion in the same image. In this paper, a method is presented for detecting copy-move forgery using the Scale-Invariant Feature Transform (SIFT) algorithm. The spearman relationship and ward clustering algorithm are used to measure the similarity between key-points, also to increase the accuracy of forgery detection. This method is invariant to changes such as rotation, scale change, deformation, and light change; it falls into the category of blind forgery detection methods. The experimental results show that with its high resistance to apparent changes, the proposed method correctly detects 99.56 percent of the forged images in the dataset and reveals the forged areas.

Keywords: Copy-Move Forgery, SIFT Features, Spearman-Based Similarities, Ward Linkage Method, Feature Transform Algorithm.

1 Introduction

WITH the development of image-editing software, digital images forgeries have become easier, but detecting forged images can be very challenging. As a result, the identity of these images is lost. Previously, certain attempts have been made to locate and detect forgery in digital images, including digital signature and watermarking [1-4]. Providing a secure method for detecting all or part of the watermark pattern is one of the main objectives of watermarking algorithms. A pattern in a watermarking digital image is hidden in such a way that the watermarked image looks identical to the original one when seen. However, analyzing the watermarked image using a decomposition program can prove the existence of a watermark pattern. However, the main limitation of digital signature and watermarking is that the images must be preprocessed before release so that the hash value can be calculated, or the watermark can be embedded in the image; this limits the scope of application. Therefore, blind detection of digital images, which is a type of forgery detection without reliance on previous information of the image, has become a critical subject in confirmation and detection of the identity of images.

Recently, image forgery has fallen into two categories; active and passive approaches. The active approach takes advantage of digital watermarking and digital signature or a combination of both. However, in active approach, the detector is provided with prior information about the image, for instance, the camera by which the image has been taken. Tampering can be detected in passive approaches. Here, the detector has no previously-provided information about digital signature or watermarking. The case for which no information is available about the camera by which the image has been taken is called blind image.

In turn, the passive approach is classified into three types, Copy-move forgery, Image Splicing, and Image

Iranian Journal of Electrical and Electronic Engineering, 2020.
Paper first received 26 February 2019, revised 20 November 2019, and accepted 29 November 2019.
* The authors are with the Department of Computer Engineering, Yazd Branch, Islamic Azad University, Yazd, Iran.
E-mails: ms.fattahi@iauyazd.ac.ir and emadi@iauyazd.ac.ir.
Corresponding Author: S. Emadi.

Retouching [5-7]. Copy-move is a type of image forgery in which a part of an image is copied and pasted to another location in the same image [8]. Since the copied portion belongs to the same image, important characteristics such as dispersion of noise, color, texture, and light must be compatible with the other parts of the image, thus, making the forgery even more difficult to detect. An image-forgery detector must be invariant to certain changes such as scale, rotation, and view angle. The problem here is that most of the existing methods do not deal with all these changes or have high computational costs. For example, the method in [9] cannot detect rotation and scale change, while [10] can detect a small amount of rotation and scale change. Copy-move forgery detection methods can be categorized into block-based approach and keypoint-based approach. The image in block based methods is divided into certain rectangular regions, while the keypoint-based methods extract feature point only on certain regions of an image without any subdivisions. Feature extraction in keypoint-based method, without any image subdivision, is done by different methods such as SIFT and SURF. Moreover, unlike the block-based approach, Keypoint-based methods extract the distinctive local features from the image.

Accuracy and efficiency are, in fact, the two key issues in copy-move forgery detection approaches. This is because they must receive fewer errors, time and memory requirements corresponding to different image sizes and distortions. The computation time is determined by the feature set complexity and the feature vector size [11]. The feature size factor in block-based methods can result in extremely high memory use, particularly for large images. Keypoint-based methods overpass in space and time complexity. This is because the number of the keypoints being extracted is smaller than the number of image blocks. This makes the whole subsequent processing extremely light. Hence, coping with these two issues is absolutely challenging.

In this paper, image forgery has been investigated using the Scale Invariant Features Transform (SIFT) algorithm and Spearman relationships. The result of this improved method of copy-move forgery detection is successful reduction in false alarms with more accurate outcomes. Initially, the keypoints and their features are extracted using SIFT algorithm. Then, the vector of similarity between the keypoints is formed using the Spearman relationship. Finally, after obtaining similar keypoints, the image is evaluated using Ward-type clustering and the forged places are displayed.

Our contribution is that we employ spearman distance for detecting similarity that not used and then match and filter them to obtain a small vector. According to this, our proposed method reduces computational time and raises the *precision* of the forgery detection. In other words, one of the most crucial features of the proposed algorithm is prevention of excessive search in vector space of the image and finding several repetitive points in the image.

The rest of the paper is organized as follows. The next section, is described related works. Section 3 is described the proposed methodology based on proposed method. Then, the simulation and experimental results are presented, and, finally, future studies and suggestions are presented in the concluding section.

2 Related Works

The problem encountered by copy-move forgery detection is that all the multiple detection methods pursue the same goal; a copy-move forgery specifies the correlation between the original image area and the copied region. Several methods have been developed to search for this correlation which divides the image into overlapping blocks. Then, a feature extractor is applied to the blocks in order to display the small-sized blocks. Soni *et al*. [12], presents a detailed review and critical discussions on each of copy-move forgery detection techniques from 2007 to 2017 based on various standard databases, issues, challenges and future directions. They described the keypoint-based algorithms are more helpful for region duplication that involves region transformations. But in highly uniform areas, keypoint-based techniques are unable to detect forgery. In [13] and [14], the mean of the red, green, and blue colors, along with the four other features calculated from overlapping blocks, is selected and obtained by distributing luminance energy in four different directions. Another solution is shown in [15], in which the features are represented by singular value decomposition (SVD), which is applied to low-frequency coefficients (LFCs) from block-based discrete wavelet transformation (DWT). Mahdian and Saic [16], proposed a method to display blocks via the calculation of blur invariance. Their specific goal was to find the features invariant to the display of fading artifacts and a forger that can apply them to the image in order to make forgery detection more difficult. Then, they used the principal component analysis (PCA) and k-tree to reduce the number of features and identify the interest areas, respectively. Dixit *et al*. [17], proposed a method based on SWT-SVD to copy-move forgery, in which blocks are extracted using SVD. They also used Stationary Wavelet Transforms (SWT) to find features similarity between the blocks and managed to detect blurred out edges which make it difficult to detect the forgery. Dixit and Naskar [18], in another research classified the forgery techniques into three- way and used a set of parameters for analyzing the schemes and evaluating and comparing their performances. This approach can be used as a standard benchmark for efficiency comparison of copy–move forgery detection technique and depending on the user requirements can be helped a user to select the most optimal technique. Dybala *et al*. [19], introduced a technique to detect

forgery in which the copied section has been edited using two distinct tools Healing brush and Poisson cloning in Adobe Photoshop. Two more algorithms have been developed in [9, 20, 21] based on small-sized block display and fast sorting in order to improve the efficiency of copy-move forgery detection. Fridrich *et al*. [20], in particular, applied a discrete cosine transform (DCT) to each block. Then, the repeated areas were identified by lexicographic sorting through the DCT block coefficients and similar block grouping with the same spacing in the image. Popescu and Farid [9] applied PCA to the image blocks in order to produce a dimension-reduced display; then, the repeated areas were detected using lexicographic sorting and grouping of all the image blocks. Another related approach is proposed by Bayram *et al*. [10]; while Mellin Fourier transform is applied to each block, a decision on forgery is made when more than a specified number of blocks are connected to each other and the distance between the pairs of the blocks is the same. The creation of a misleading forgery often requires changing the size, rotation, or stretching of a part of the image. For example, while creating an image by combining two different objects, an object may need to be resized; this process requires a re-sampling of the original image that shows the periodic cyclic communication between the neighboring pixels. The presence of these correlations, owing to re-sampling, can be used to detect the events which have occurred in the image–not to identify the specific manipulations; therefore, a good forgery detector must be robust against certain changes such as rotation and scale change, and some manipulations such as JPEG compression, addition of Gaussian noise, and Gamma correction. Most of the existing methods cannot deal with all these manipulations simultaneously and often have high computational costs. For instance, the method in [9] is specifically unable to detect rotation and scale changes, while the methods in [10, 20] can only detect rotation and minor scale changes according to the report in [22]. In [23], the authors have tried to use the Zernike moment to overcome this limitation in the detection of copy-move forgery; however, their approach is effective solely when the copied region has only rotation. This issue has also been discussed and analyzed in [24], in which the effects of the changes in rotation, JPEG compression, and Gaussian noise manipulation have been investigated on copy-move forgery detection. Christlein *et al*. [25] provide a general comparison of the above-mentioned copy-move forgery detection methods. The performance of each method has been evaluated on a copied segment with and without geometric change. Today, local visual features (i.e., SIFT, SURF, FAST, etc.) are used extensively to recover images and to detect objects due to the robustness against certain geometric changes such as rotation, scale change, and light change. In fact, SIFT features are used to recognize fingerprints [26], retrieve shoeprints [27] and detect copy-move forgery [28-33]. Since these algorithms are based on the extraction of the keypoints and they extract points with high entropy in the image, they significantly contribute to the increase in the accuracy and reduction of the number of comparisons as well as the implementation time of the algorithm in the copy-move detection steps; they also overcome the problems of the previous methods to a considerable extent. Hayat and Qazi [34], proposed a forgery detection method that first reduces the features via discrete wavelet transform (DWT) to give an approximate image from the lowest energy sub-band. Then the approximate image divided to fixed sized square blocks for correlation based comparison based on the discrete cosine transform (DCT). In comparison to others method, this approach consists of a mask-based tampering method in order to extract the part to be substituted as forgery in the original image and have highest average accuracy. Chen *et al*. [35], presents a novel block sampled matching with region growing algorithm (BSMRG) to detect the copy-move regions efficiently assuming that the copy-move forgery region is larger than a predefined region size. They partitioned test image according to the predefined region size into non-overlapped blocks. Then to find a pair of matched blocks, they compared this blocks with the upper-left blocks. Experimental results show that the proposed BSMRG can detect duplicated regions using best computation performance. Sadeghi *et al*. [36], present a method based on SIFT for detecting copy-move forgery that can be authenticate image accurately. They used SIFT to extract keypoints and used Euclidean distances for finding similar keypoints. Finally, they indicate which part of the image have been tempered with. Results show that the method is robust against JPEG compression, rotation, noise, and scaling. Alamro and Yusoff [37], propose a combination of two feature extraction methods DWT and SURF to detect a copy-move forgery in image. DWT and SURF are used to reduce image dimension and to extracting the key features from the image respectively. Hilal *et al*. [38], combined the DCT and the PCA methods in order to account for low contrast segments in an image. In this approach, PCA is used to extracting of important features. Then image separate into blocks in order to Local contrast for each block is calculated and those blocks which exceeded the fixed contrast are kept. 2D-DCT is applied to each block and local feature matrix is extracted so that autocorrelation is evaluated. Finally, if the correlation value exceeds a threshold than those blocks are considered to be duplicate. Resmi and Vishnukumar [39], proposed two stages efficient method to detect copy-move forgery in digital images. In the first stage, the RGB image convert in to grayscale image using standard color space conversion, then grayscale image divided into non-overlapping patches using SLIC algorithm [40] and the features of these patches are compared with other patches to find the matching areas. In the second stage, the SIFT algorithm

is used to keypoint extraction from each block. Then the number of keypoints in a region is divided by the total number of pixels in that region to determine if it is a smooth region or a keypoint region. Alberry *et al*. [41] utilized SIFT and Fuzzy C-means algorithms for feature extraction and clustering, respectively. They optimized FCM algorithm for clustering the SIFT keypoints to decrease time complexity. They also used MICC-220 dataset and showed that the average detection time reduced by 15.91% over the existing traditional SIFT-based algorithm. Moreover, they showed that the proposed algorithm decreases the detection time and enhances accuracy in some cases. Bi and Pun [42] proposed a fast copy-move forgery detection algorithm using Local bidirectional coherency error to refine the feature correspondences and detection of the copy-move forgery region. They used Precision rate and Recall rate to evaluate the accuracy and showed that the proposed method can keep good performance under different forgery scenarios. Also, this algorithm optimized robustness and minimized the computation complexity. Hejazi *et al*. [43] proposed an improved SIFT features-based method for copy-move forgery detection. This method works on the basis of density-based clustering and Guaranteed Outlier Removal algorithm. It effectively reduces the false positive rate and improves time and space complexity. In addition, it successfully promotes the accuracy and efficiency. Li and Zhou [44] proposed a fast and effective copy-move forgery detection algorithm based on hierarchical feature point matching. They generated a sufficient number of keypoints and then developed a novel hierarchical matching strategy to solve the keypoint matching problems even if the copy-move forgery only involves smooth or small regions. Finally, a novel iterative homographic estimation and a copy-move localization technique have been suggested, without involving any clustering and segmentation procedures. Experimental results indicate good performance of proposed method, in terms of both efficiency and accuracy. Also, evaluation of the proposed method indicates a higher True Positive Rate (TPR) and a lower False Positive Rate (FPR) simultaneously in most of the cases, compared with both the existing dense-field and keypoint-based approaches. Mahmood *et al*. [45] proposed a robust technique based on adopted SWT (stationary wavelet transform). They reduced the dimension of the feature vectors by applying discrete cosine transform (DCT). Experimental results revealed that the proposed technique has higher accuracy. Al-Qershi and Khoo [46] compared four matching techniques in terms of accuracy and robustness against different image processing operations. For comparison, they used Zernike moments, with the four features and four matching techniques based on lexicographical sorting, lexicographical sorting and grouping, kd-tree and locality sensitive hashing. The experimental results showed that matching method has a significant impact on the accuracy of copy-move forgery detection. Mayer and Stamm [47] proposed a new approach to forgery detection based on detecting localized LCA (lateral chromatic aberration) inconsistencies. They proposed a statistical model that captures the inconsistency between global and local estimates of LCA. The Experimental results indicated that the proposed method reduces estimation time and improves detection rate. Pun and Chung [48] proposed a two-stage localization for copy-move forgery detection. In the first stage or rough localization stage, they have employed Simple Linear Iterative Clustering (SLIC) for image segmentation into superpixels and used the Weber Local Descriptor (WLD) for local feature calculation and extraction from each superpixel. In the precise localization stage, they employed the Discrete Analytic Fourier–Mellin Transform (DAFMT) algorithm to extract features from the circular block. Finally, they used Euclidean distance to filter out the weak features. This approach overcomes the defects of both the keypoint-based methods and block-based methods. The Experimental results indicated that this method outperforms other existing methods.

3 Proposed Algorithm

The main purpose of the proposed method is to reduce the calculation time and the cost of the algorithm while increasing the accuracy of forgery detection through the formation of a similarity matrix between the keypoints using the Spearman relationship and the clustering of the keypoints with high similarity. Fig. 1 represents the proposed algorithm diagram.

3.1 Pre-Processing

In this operation, the red, green, and blue channels are merged, and a grayscale image is created. This step is taken to reduce computation time and improve performance in the next step.

3.2 Extraction of the KeyPoints and their Features

The keypoints are directed circular regions of the image, which are defined in a geometric form with four parameters; the coordinates x and y of the center of the keypoint, the keypoint scale (the radius of the region), and its direction (the angle that describes the radian). These points are selected in the high entropy regions of the image. At this stage of the algorithm, the keypoints and their features were extracted using the SIFT algorithm. SIFT is a machine-vision algorithm for detecting and describing local features in an image. This

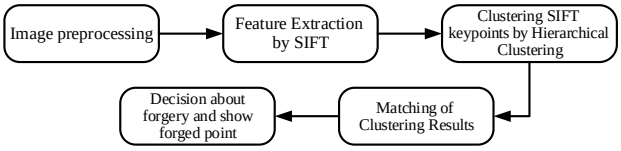

Fig. 1 Diagram of the proposed algorithm.

algorithm has been registered at the University of British Columbia, Canada, and has been published by David Lowe in 1999 [19]. A general analysis of several descriptors in [50] suggests that the SIFT feature is an appropriate solution due to its high efficiency and low computational cost. This method is divided into the following four stages: 1) making scale space and detecting extremum; 2) locating keypoints; 3) allocating canonical orientation; and 4) producing a keypoint descriptor. In fact, by introducing the image I as the input, the SIFT features are identified using a representation of the scale-space on different scales that are implemented as a pyramid of the image. To build a scale space, the original image is gradually smoothed in several steps. SIFT receives these images and changes them into half of the original image in four octaves step-by-step. The pyramid surfaces are obtained using Gaussian smoothing and image-resolution sampling, while the desired points are selected as local extrema (Min/Max) in space scales. These keypoints, which are denoted as X_i in the following, are extracted using the Laplace–Gaussian computational approximation, which is called difference of Gaussians (DOG). DOG of the image D is obtained by (1).

$$\begin{aligned} L(x,y,\sigma) &= G(x,y,\sigma)\times I(x,y) \\ G &= \frac{1}{2\pi\sigma^2} e^{\frac{-(x^2+y^2)}{2\sigma^2}} \\ D(x,y,\sigma) &= \left(G(x,y,k\sigma) - G(x,y,\sigma)\right)\times I(x,y) \\ &= L(x,y,k\sigma) - L(x,y,\sigma) \end{aligned} \quad (1)$$

The scale-space image is regarded as $L(x, y, \sigma)$, generated by the convolution process between function and image. $L(x, y, k\sigma)$ is the convolution of the original image $I(x, y)$ with the Gaussian blur $G(x, y, k\sigma)$ at scale $k\sigma$. To ensure invariance to rotation, the algorithm assigns a canonical orientation o to each keypoint. To obtain this orientation, a gradient orientation histogram is calculated in the neighboring of each keypoint. For the image sample of $L(x, y, \sigma)$, in particular, on the scale of σ (the scale at which the keypoint was detected), the gradient magnitude $m(x, y)$ and orientation $\theta(x, y)$ were calculated using (2) and (3), which are the differences of the pixels.

$$\begin{aligned} m(x,y) &= \Big(L(x=1,y) - L(x-1,y)\Big)^2 \\ &\quad + \Big(L(x,y+1) - L(x,y-1)\Big)^2\Big)^{1/2} \end{aligned} \quad (2)$$

$$\theta(x,y) = tan^{-1}\left(\frac{L(x,y+1) - L(x,y-1)}{L(x+1,y) - L(x-1,y)}\right) \quad (3)$$

Then an orientation histogram is create that, it consists of 36 sections with each section covering almost 10 degrees. The weight of each sample in the neighboring of the window is calculated by its gradient magnitude and is added to the histogram. The peaks in this histogram are proportional to the dominant orientations. When these keypoints are identified and a canonical orientation is assigned to them, SIFT descriptors are calculated in their locations in both the original image and the scale space. Each feature descriptor contains a 128-element histogram $\boldsymbol{f}$ derived from a 16×16-pixel region around the desired keypoint. This region is selected by the coordinates (x, y) of the center of the keypoint, and its canonical direction is chosen as the main axis. The contribution of each pixel is obtained by collecting a gradient magnitude of the image $m(x, y)$ and direction $\theta(x, y)$ in the scale space; in addition, the histogram is calculated as the local statistic of the slope directions (which contains eight sections) in 4×4 sub-sections.

In summary, by introducing the image I, this procedure ends with a list of N keypoints, each of which is fully described by the following statement: $X_i = \{x, y, \sigma, o, f\}$, where (x, y) are the coordinates in the image; σ is the keypoint scale (related to the level of the image pyramid used in the calculation of the descriptor), o is the canonical orientation (in order to invariance against rotation), and $\boldsymbol{f}$ is the feature vector of the final descriptor SIFT.

3.3 Finding Similar KeyPoints

Finding and matching similar keypoints are performed on the SIFT feature vectors. The previous studies have used either lexicographic sorting of the feature vectors [14, 51] or the multiple randomized kd-tree [29, 52]; however, the former method has a high computational cost and the latter is unable to find several similar points. In the present study, a different strategy has been used to solve this problem, eliminating the previous drawbacks.

The input to this phase is, indeed, the output matrix in the previous phase, which consists of 64 to 128 numbers for each single-vector keypoint. Comparison of the features of each keypoint with a numerous numbers requires much time and cost. Moreover, one-by-one comparison of the numbers increases the error rate. Therefore, the proposed algorithm takes advantage of the equations for calculating the similarity between vectors, the outcome of which is only one number. This can improve the speed and accuracy of the algorithm. In this research Spearman distance used to calculate the similarity level according to (4).

$$Similarity_{st} = 1 - \frac{(r_s - \bar{r}_s)(r_t - \bar{r}_t)'}{\sqrt{(r_s - \bar{r}_s)(r_s - \bar{r}_s)'}\sqrt{(r_t - \bar{r}_t)(r_t - \bar{r}_t)'}} \quad (4)$$

where

$$\bar{r}_s = \frac{1}{n}\sum_j r_{sj} = \frac{(n+1)}{2} \quad \text{and} \quad \bar{r}_t = \frac{1}{n}\sum_j r_{tj} = \frac{(n+1)}{2}$$

s is the keypoint of the origin, t is the destination keypoint, r_{sj} is the rank of x_{sj} taken from $x_{1j}, x_{2j}, \ldots, x_{mj}$, calculated by the tiedrank algorithm, r_s and r_t are the coordinate-wise rank vectors of x_s and x_t, i.e., $r_s = (r_{s1}, r_{s2}, \ldots, r_{sm})$.

According, to this equation, in order to reduce the computation time and to compare the keypoints, a matrix of similarity between the keypoints was formed using their features to calculate the similarity level.

Having formed the matrix, each entry was a number representing the degree of similarity between the origin and the destination points. After this step and in order to reduce the comparisons time between the keypoints, the rows were arranged in descending order based on the similarity level; finally, in order to measure the similarity and the likelihood of the presence of the keypoints in the list of similar points, the following equation was used, and a threshold was considered for the response. If the response is lower than the threshold, the pair of points is located in the list of similar keypoints.

$$Rate = \frac{C_i}{C_{i+1}} \quad \textbf{if} \quad Rate < Threshold \quad \textbf{then} \quad Add \ \ Keypionts \ \ to \ \ list \tag{5}$$

This will prevent excessive comparisons, and non-similar points will not be compared. Moreover, the computational cost is significantly reduced due to the decreased size of the matrix in the previous step.

3.4 Filtering the KeyPoints

To reduce the likelihood of the presence of incorrect keypoints, Euclidean distance was used. A filtering approach is based on the neighboring pixels that are too similar to each other, and this may lead to errors in forgery detection. To prevent this problem, they are filtered for the next step by calculating the Euclidean distance between them and placing a threshold.

3.5 Clustering and Forgery Detection

In some of the images, there may be areas with very similar texture, which cause errors in detecting the existence of forgeries. This probability can be reduced using clustering. In this paper, Agglomerative Hierarchical Clustering (AHC) [53] has been used to cluster the forged areas; it is applied to similar keypoints. Hierarchical clustering can be represented as a hierarchy of clusters in a tree structure. Hierarchical clustering involves the following steps:

1. Assigning each keypoint to a cluster,
2. Calculation of the reciprocal spatial distance between all the clusters,
3. Finding the pair of clusters close to each other,
4. Merging them into a single cluster via Ward's linkage method.

This computation continues until a certain limit is reached. There are several linkage methods, each of which calculates the distance between the clusters. In particular, Ward's linkage method has been used in certain previous studies such as Amerini *et al.*'s approach [54].

The given two clusters P and Q in Ward's method, respectively, include n_p and n_Q objects (where X_{pi} and X_{Qi} represent the i-th and j-th objects in the clusters P and Q, respectively). Ward proposes a clustering process that seeks to form clusters ($P_1, P_2, \ldots, P_{n-1}, P_n$) in a way to minimize the loss of a link in each grouping; as a result, the quantity of the loss is determined in a form that can be easily interpreted. At each step of the analysis, the union of every possible cluster pair is considered and the two clusters, whose fusion results in minimum increase in information loss, are combined. Information loss is defined by Ward in terms of an Error Sum-of-Squares criterion (ESS).

In the Ward link, increase or decrease in the ESS after merging the two clusters into one cluster is calculated as follows:

$$\Delta_{dist}(P,Q) = ESS(PQ) - \left[ESS(P) + ESS(Q)\right] \tag{6}$$

where

$$\mathrm{ESS(P)} = \sum_{i=1}^{np} \left| X_{P_i} - \bar{X}_P \right|^2 \quad \text{and} \quad \bar{X}_P = \frac{1}{n_P} \sum_{i=1}^{n_P} X_{P_i} \tag{7}$$

where, $\bar{X}_p$ is a centroid and PQ represents a hybrid cluster. At the end of the clustering procedure, the clusters that do not contain a significant number of matched keypoints (more than 3) are eliminated. If more than one cluster is found with the necessary conditions, the image will be considered as a forged image.

A Particular tree structure is generated as a result of this linkage method. Then the inconsistency coefficient (IC) parameter is compared with the threshold T_h in order to stop cluster aggregation. So, with a higher value of this coefficient, the points with less similarity are agglomerated together in a manner in which clustering stops when it exceeds the threshold T_h. The IC focuses mainly on the distance between the clusters and does not allow the agglomeration of too far clusters at the hierarchy level. It is clear that the proper choice of T_h directly affects forgery detection efficiency.

4 Experimental Results

In this section, the proposed method is evaluated with two datasets. The MICC-F220 dataset [1] contains 220 images including 110 manipulated and 110 original images in different resolutions between 722×480 and 800×600 pixels. The manipulated images in the dataset are generated by selecting the circle- and square-shaped regions randomly in different places and sizes, performing copy-move operations, and symmetric/asymmetric scale change and rotation in the

image. At first, the proposed technique is examined in order to identify the most appropriate settings for the cut-off threshold T_h introduced on the base of Ward's linkage method. The given values are set for all remaining experiments and comparisons. All the 220 images have been chosen to perform a training to find the best threshold T_h for ward's linkage method.

Detection accuracy and efficiency was measured in terms of Precision, Recall, F1, True Positive Rate (TPR) and False Positive Rate (FPR) based on (7)-(11), respectively.

$$Precision = \frac{TPR}{TPR + FPR} \times 100 \tag{8}$$

$$Recall = \frac{TPR}{TPR + FN} \tag{9}$$

$$F1 = \frac{2 \times Percision \times Recall}{Percision + Recall} \tag{10}$$

while

$$TPR = \frac{Num\,of\ \ images\,detected\,as\,forged\,being\,forged}{Num\,of\ \ forged\,images} \tag{11}$$

$$FPR = \frac{Num\,of\ \ images\,detected\,as\,foreged\,being\,orginal}{Num\,of\ \ orginal\,images} \tag{12}$$

TPR is the fraction of the correctly detected forged images and FPR is the fraction of the original images that are not properly detected. In addition, FN is the number of the forged images detected as original. The recall is the rate of detection that determines the percentage of correctly detected forgeries to the sum of the number of correctly detected forgeries and the number of forged images that are not detected. Precision represents the probability of how much of the detected forgery is real. Furthermore, F1 is another measure of performance, which combines Precision and Recall. Table 1 shows the precision of the proposed method on this dataset. Figs. 2 and 3 illustrate examples of the tests performed on the images.

Moreover, Table 2 presents a comparison between the various algorithms such SIFT, SURF, FAST, MSER and HARRIS [55] in the case they have used the proposed method to find the similarity together with Centroid and Ward clustering. The algorithm with higher TPR and lower FPR and implementation time is regarded as the best one.

Table 3 shows the results on MICC-F220 dataset obtained by different copy-move forgery detection methods, including keypoint-clustering-based [44, 54, 56], keypoint-segmentation based [57, 58], block-based [14, 59] and our proposed approaches. The table shows that the running times of the proposed method are in the upper group compared to the popular methods.

We can see that, due to decreased search space and search of keypoints with higher similarity, the computation time, FPR and F1 criteria are much better in the proposed method compared to other similar techniques. Also, the proposed method after the keypoint-clustering-based techniques [44, 53] has the most TPR.

Table 1 The precision of the proposed method on MICC-F220 data.

Precision	Recall	F1
99.565	97.80	98.67

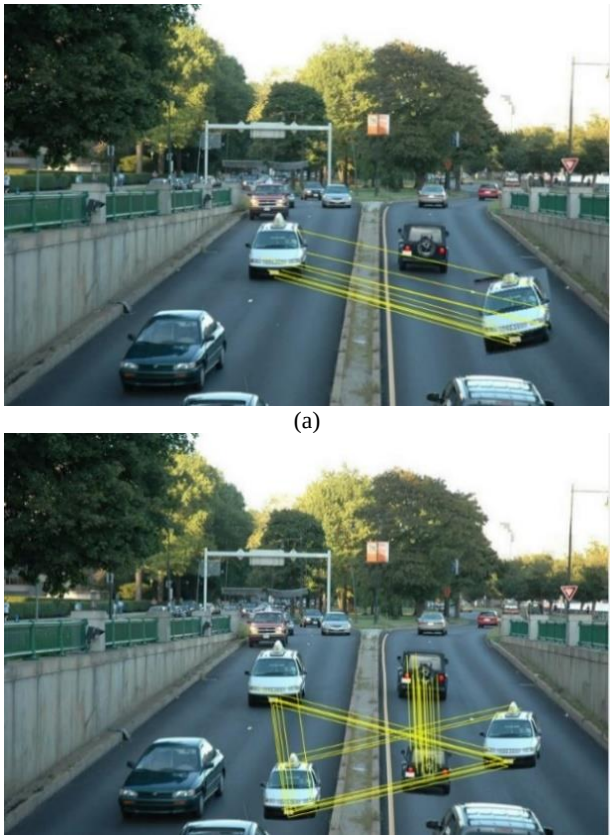

Fig. 2 The top side; copy-move forgery along with rotation and the scale change, and lower side; detection of several similar points.

Fig. 3 Detection of multiple identical copies of a fish in an image.

In the following section, second dataset has been used in which the forged areas have been distorted by various changes [11, 60]. This dataset contains 48 different images. In the dataset, the copied regions are from the categories of living, nature, man-made and mixed. In this case, the forged images have been generated using each of the images in the dataset and the copied areas are distorted by manipulations such as geometric distortions including scale and rotation changes.

So, the dataset has 1826 images in total. In this study, the color images were converted to grayscale images. So that the color does not affect the selection of the forged areas.

1. Down Sampling: the scale of all the images in the dataset is reduced from 90 percent to 10 percent by a step of 20 percent and a new dataset is prepared; in this case, 5×48=240 images must be tested.
2. Scaling: the scale of the copied areas is changed by varying the scales between 91 percent and 109 percent, with a 2 percent step, and a new dataset is prepared; in this case, 10×48=480 images must be tested.
3. Rotation: a new dataset is prepared by rotating the copied regions with varying degrees between 2° and 10° in a 2° Step 2, in which 5×48=240 should be tested.

Table 4 shows the results on IMD dataset obtained by different copy-move forgery detection methods, and our proposed approaches.

Figs. 4-6 show the results of forgery detection in various manipulations. Areas in red color are the results

Table 2 Comparison results under proposed method on MICC-F220 dataset.

	Cluster Enabled	Clustering Method	Similarity Method	Threshold	TPR [%]	FPR	Time
SIFT	Yes	Centroid	Spearman	0.35	90.00	1.545	226
	Yes	Ward	Spearman	0.35	93.64	1.818	240
	No		Spearman	0.35	99.09	4.909	183
SURF	Yes	Centroid	Spearman	0.65	73.64	1.545	80
	Yes	Ward	Spearman	0.65	82.73	2.455	106
	No		Spearman	0.65	97.27	8.091	100
FAST	Yes	Centroid	Spearman	0.56	49.00	1.189	114
	Yes	Ward	Spearman	0.56	53.43	1.274	120
	No		Spearman	0.56	92.73	8.00	95
MSER	Yes	Centroid	Spearman	0.7	53.64	5.45	90
	Yes	Ward	Spearman	0.7	65.45	1.455	92
	No		Spearman	0.7	100	7.545	69
HARRIS	Yes	Centroid	Spearman	0.6	60.91	3.182	111
	Yes	Ward	Spearman	0.6	71.45	4.545	117
	No		Spearman	0.6	98.18	9.455	84

Table 3 The results on MICC-F220 dataset by different copy-move forgery detection methods.

	TPR	FPR	F1	Time (image level)
Amerini *et al*. [54]	98.18	9.09	94.74	3.5
Li and Zhou [44]	100	1.82	99.10	3.0
Bravo-Solorio and Nandi [14]	19.09	6.36	30.43	17.4
Li *et al*. [57]	70.91	17.27	75.36	111.6
Cozzolino *et al*. [59]	84.55	17.27	83.78	5.3
Zandi *et al*. [58]	78.18	48.18	69.08	16.6
Silva *et al*. [56]	45.45	41.82	48.54	4.1
Proposed method	93.64	1.818	98.67	1.5

Table 4 Comparison results on IMD dataset by different copy-move forgery detection methods.

	Precision	Recall	F1
SIFT [49]	88.37	79.17	83.52
SURF[61-63]	91.49	89.58	90.53
Bravo-Solorio and Nandi [14]	8.27	100	93.20
Wang *et al*. [64]	92.31	100	96.00
Pun and Chung [48]	97.9	97.9	97.9
Pun *et al*. [7]	96	100	97.96
Amerini *et al*. [54]	88.4	79.2	83.5
Proposed method	99.565	97.80	98.67

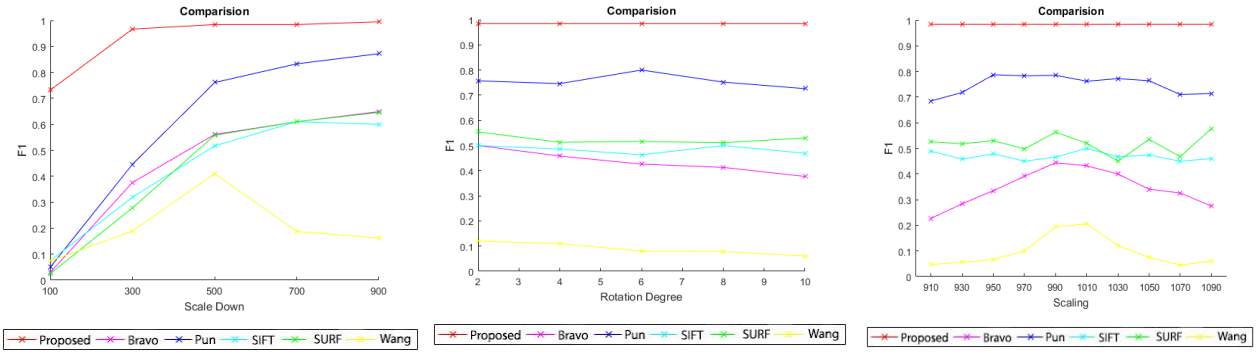

Fig. 4 Illustrating F1 in scale down, scaling, and rotation.

of the proposed algorithm, which have been compared with the methods based on keypoints, such as SIFT [49], SURF [61, 62], Pun [7], Bravo and Nandi [14], and the circle blocking-based method by Wang *et al*. [64].

In Figs. 4-6, the axis *x* represents the scale factor for scaling, scaling down, and the rotation degree for rotation. Comparing the above graphs, it is easy to conclude that the proposed method has higher accuracy and capability of detection in comparison with other methods.

Also, two samples of the forged images and their forgery detection by the proposed algorithm are shown in Figs. 7 and 8. As the figures show, due to decreased

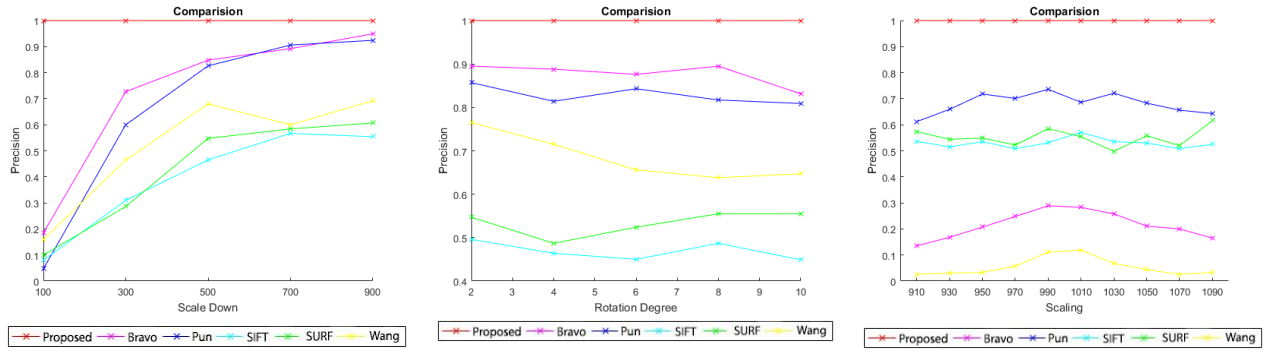

Fig. 5 Illustrating precision in scale down, scaling, and rotation.

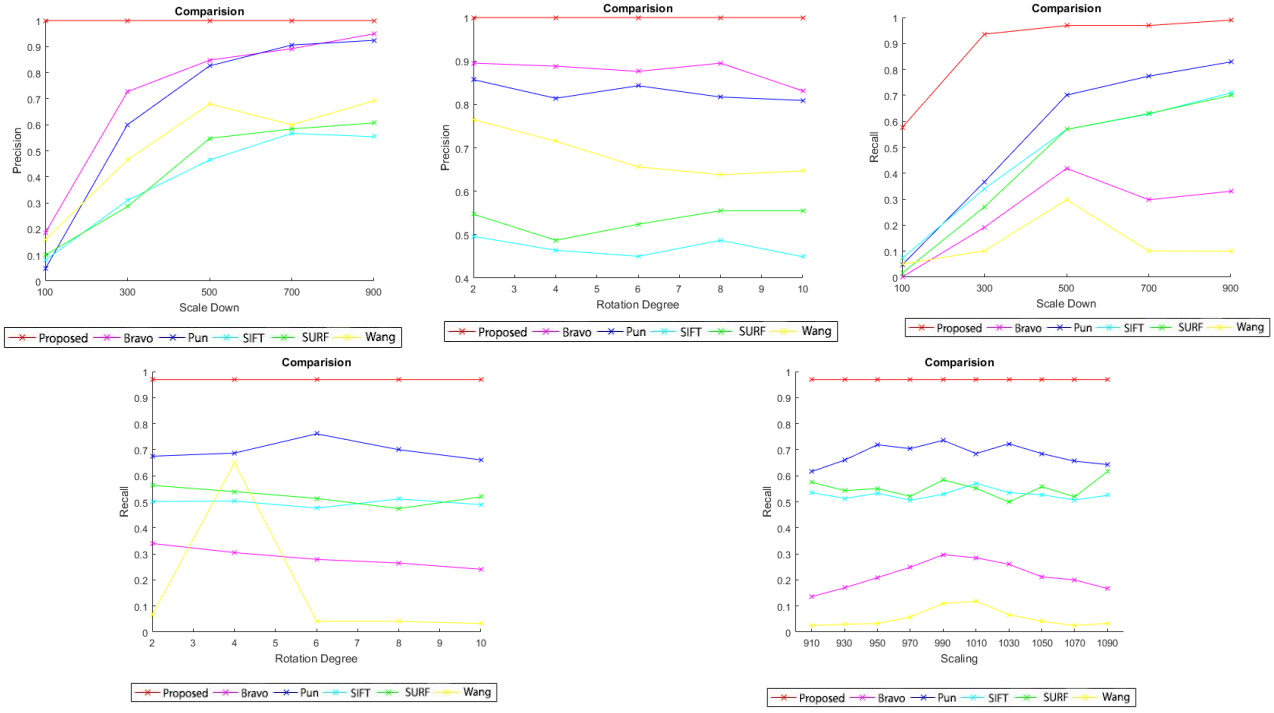

Fig. 6 Illustrating F1 in scale down, scaling, and rotation.

(a) (b) (c)

Fig. 7 Samples from the original and forged images; a) original image, b) b) forged image, and c) forgery detection.
* In image (b), the building is hidden using the copy-move of the trees

(a) (b) (c)

Fig. 8 Samples of the original and forged images; a) original image, b) b) forged image, and c) forgery detection.
* In image (b), a boat rider is hidden by copy-move forgery of the surrounding areas.

search space and search of points with higher similarity, the considered criteria are much better in the proposed method compared to other similar techniques.

5 Conclusion

In this paper, we presented a new method for detecting copy-move forgery. In comparison with other methods, our proposed algorithm has higher speed and accuracy in detecting types of forgery, including rotation, scale change, deformation, and luminance. In this method, owing to the reduction in the number of comparisons in the stage of detecting similar areas, and through the use of Spearman relationship, the speed has been dramatically increased; in addition, in the forgery-detection phase, due to the detection of several similar areas and the use of clustering algorithm, the accuracy of the algorithm has been improved. However, a significant issue concerning the accuracy of this algorithm involves calculating the correct threshold value to achieve correct detection and the least error. In the future, we intend to work on the smart and optimal calculation of threshold, and the use of SURF and FAST algorithms to identify the keypoints.

References

[1] M. Barni and F. Bartolini, *Watermarking systems engineering: Enabling digital assets security and other applications*. CRC Press, 2004.

[2] I. J. Cox, M. L. Miller, J. A. Bloom, and C. Honsinger, *Digital watermarking*. Vol. 53, San Francisco: Morgan Kaufmann, 2002.

[3] Z. W. Zhang, L. F. Wu, H. G. Lai, H. B. Li, and C. H. Zheng, "Double reversible watermarking algorithm for image tamper detection," *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 7, No. 3, pp. 530–542, 2016.

[4] F. C. Chang and H. C. Huang, "Reversible data hiding with difference prediction and content characteristics," *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 7, No. 3, pp. 599–609, 2016.

[5] D. Chauhan, D. Kasat, S. Jain, and V. Thakare, "Survey on keypoint based copy-move forgery detection methods on image," *Elsevier Procedia Computer Science 85*, pp. 206–212, 2016.

[6] K. Asghar, Z. Habib, and M. Hussain, "Copy-move and splicing image forgery detection and localization techniques: a review," *Australian Journal of Forensic Sciences*, Vol. 49, No. 3, pp. 281–307, 2017.

[7] C. M. Pun, X. C. Yuan, and X. L. Bi, "Image forgery detection using adaptive over segmentation and feature point matching," *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 8, pp. 1705–1716, 2015.

[8] N. Kanagavalli, and L. Latha, "A Survey of copy-move image forgery detection techniques," in *International Conference on Inventive Systems and Control (ICISC)*, pp. 1–6, 2017.

[9] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," *Department. Computer Science, Dartmouth College*, Tech. Rep. TR2004-515, 1-11, 2004.

[10] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1053–1056, 2009.

[11] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 6, pp. 1841–1854, 2012.

[12] B. Soni, P. K. Das, and D. M. Thounaojam, "CMFD: A detailed review of block based and key feature based techniques in image copy-move forgery detection," *IET Image Processing*, Vol. 12, No. 2, pp. 167–178, 2017.

[13] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in *Proceedings of the 18th IEEE International Conference on Pattern Recognition*,Vol. 4, pp. 746–749, 2006.

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

[15] 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 *IEEE International Conference on Multimedia and Expo*, pp. 1750–1753, 2007.

[16] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic Science International*, Vol. 171, No. 2–3, pp. 180–189, 2007.

[17] R. Dixit, R. Naskar, and S. Mishra, "Blur-invariant copy-move forgery detection technique with improved detection accuracy utilising SWT-SVD," *IET Image Processing*, Vol. 11, No. 5, pp. 301–309, 2017.

[18] R. Dixit and R. Naskar, "Review, analysis and parameterisation of techniques for copy–move forgery detection in digital images," *IET Image Processing*, Vol. 11, No. 9, pp. 746–759, 2017.

[19] B. Dybala, B. Jennings, and D. Letscher, "Detecting filtered cloning in digital images," in *Proceedings of the 9th ACM Workshop on Multimedia & Security*, pp. 43–50, 2007.

[20] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in *Proceedings of Digital Forensic Research Workshop*, 2003.

[21] X. Lin, S. L. Wang, W. J. Huang, and J. Y. Lai, "An Experimental study on block DCT coefficient analysis for image splicing detection," in *IEEE First International Conference on Data Science in Cyberspace (DSC)*, pp. 69–73, 2016.

[22] S. Bayram, H. T. Sencar, and N. Memon, "A survey of copy-move forgery detection techniques," in *IEEE Western New York Image Processing Workshop*, pp. 538–542, 2008.

[23] S. J. Ryu, M. J. Lee, and H. K. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in *International Workshop on Information Hiding*, pp. 51–65, Springer, Berlin, Heidelberg, 2010.

[24] H. J. Lin, C. W. Wang, and Y. T. Kao, "Fast copy-move forgery detection," *WSEAS Transactions on Signal Processing*, Vol. 5, No. 5 pp. 188–197, 2009.

[25] V. Christlein, C. Riess, and F. Angelopoulou, "A study on features for the detection of copy-move forgeries," in *Proceeding. of Information Security Solutions Europe*, Berlin, Germany, pp. 105–116, 2010.

[26] X. Shuai, C. Zhang, and P. Hao, "Fingerprint indexing based on composite set of reduced SIFT features," in *IEEE 19th International Conference on Pattern Recognition*, pp. 1–4, 2008.

[27] H. Su, D. Crookes, A. Bouridane, and M. Gueham, "Local image features for shoeprint image retrieval," in *British Machine Vision Conference*, 2007.

[28] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "Geometric tampering estimation by means of a SIFT-based forensic analysis," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1702–1705, 2010.

[29] X. Pan, and S. Lyu, "Detecting image region duplication using SIFT features," in *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1706–1709, 2010.

[30] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in *IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, Vol. 2, pp. 272–276, 2008.

[31] K. Kiruthika, S. D. Mahalakshmi, and K. Vijayalakshmi, "Detecting multiple copies of copy-move forgery based on SURF," *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 3, No. 3, pp. 2276–2281, 2014.

[32] R. Nithiya and S. Veluchamy, "Keypoint descriptor based copy and move image forgery detection system," in *IEEE Second International Conference on Science Technology Engineering and Management (ICONSTEM)*, pp. 577–581, 2016.

[33] P. R. Rukar and P. S. Patil, "Copy move image forgery detection using SIFT," *Oriental Journal of Computer Science and Technology*, Vol. 9, No. 3, pp. 235–245, 2016.

[34] K. Hayat and T. Qazi, "Forgery detection in digital images via discrete wavelet and discrete cosine transforms," *Computers & Electrical Engineering*, Vol. 62, pp. 448–458, 2017.

[35] C. C. Chen, L. Y. Chen, and Y. j. Lin, "Block sampled matching with region growing for detecting copy-move forgery duplicated regions," *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 8, No. 1, pp. 86–96, 2017.

[36] S. Sadeghi, H. A. Jalab, K. Wong, D. Uliyan, and S. Dadkhah, "Keypoint based authentication and localization of copy-move forgery in digital image," *Malaysian Journal of Computer Science*, Vol. 30, No. 2, pp. 117–133, 2017.

[37] L. Alamro and N. Yusoff, "Copy-move forgery detection using integrated DWT and SURF," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, Vol. 9, No. 1–2, pp. 67–71, 2017.

[38] A. Hilal, T. Hamzeh, and S. Chantaf, "Copy-move forgery detection using principal component analysis and discrete cosine transform," in *IEEE Sensors Networks Smart and Emerging Technologies (SENSET)*, pp. 1–4, 2017.

[39] M. R. Resmi and S. Vishnukumar, "A novel segmentation based copy-move forgery detection in digital images," in *International Conference on Networks & Advances in Computational Technologies (NetACT)*, pp. 346–350, 2017.

[40] M. K. S. Varma, N. K. K. Rao, K. K. Raju, and G. P. S. Varma, "Pixel-based classification using support vector machine classifier," in *IEEE 6th International Conference on Advanced Computing (IACC)*, pp. 51-55, 2016.

[41] H. A. Alberry, A. A. Hegazy, and G. I. Salama, "A fast SIFT based method for copy move forgery detection," *Future Computing and Informatics Journal*, Vol. 3, No, 2, pp. 159–165, 2018.

[42] X. Bi and C. M. Pun, "Fast copy-move forgery detection using local bidirectional coherency error refinement," *Pattern Recognition*, Vol. 81, pp. 161–175, 2018.

[43] A. Hegazi, A. Taha, A. M M. Selim, "An improved copy-move forgery detection based on density-based clustering and guaranteed outlier removal," *Journal of King Saud University-Computer and Information Sciences*, 2019.

[44] Y. Li and J. Zhou, "Fast and effective image copy-move forgery detection via hierarchical feature point matching," *IEEE Transactions on Information Forensics and Security*, Vol. 14, No. 5, pp. 1307–1322, 2018.

[45] T. Mahmood, Z. Mehmood, M. Shah, and T. Saba, "A robust technique for copy-move forgery detection and localization in digital images via stationary wavelet and discrete cosine transform," *Journal of Visual Communication and Image Representation*, Vol.53, pp. 202–214, 2018.

[46] O. M. Al-Qershi and B. E. Khoo, "Comparison of matching methods for copy-move image forgery detection," in *9th International Conference on Robotic, Vision, Signal Processing and Power Applications*, Springer, Singapore, pp. 209–218, 2017.

[47] O. Mayer and M. C. Stamm, "Accurate and efficient image forgery detection using lateral chromatic aberration," *IEEE Transactions on Information Forensics and Security*, Vol. 13, No. 7, pp. 1762–1777, 2018.

[48] C. M. Pun and J. L. Chung, "A two-stage localization for copy-move forgery detection," *Information Sciences*, Vol. 463, pp. 33–55, 2018.

[49] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, Vol. 60, No. 2, pp. 91–110, 2004.

[50] K. Mikolajczyk and C. Schmid, "A performance evaluation of local descriptors," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 27, No. 10, pp. 1615–1630, 2005.

[51] M. Bashar, K. Noda, N. Ohnishi, and K. Mori, "Exploring duplicated regions in natural images," *IEEE Transactions on Image Processing*, 2010.

[52] X. Pan and S. Lyu, "Region duplication detection using image feature matching," *IEEE Transactions on Information Forensics and Security*, Vol, 55, No. 4, pp. 857–867, 2010.

[53] J. Friedman, T. Hastie, and R. Tibshirani, *The elements of statistical learning*. Vol. 1, No. 10, New York: Springer Series in Statistics, pp. 337–387, 2001.

[54] 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 Transactions on Information Forensics and Security*, Vol. 6, No. 3, pp. 1099–1110, 2011.

[55] U. Sinha, "Harris Corner Detector," 2016. [Online]. Available: http://aishack.in/tutorials/harris-corner-detector/.

[56] E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes," *Journal of Visual Communication and Image Representation*, Vol. 29, pp. 16–32, 2015.

[57] J. Li, X. Li, B. Yang, and X. Sun, " Segmentation-based image copy-move forgery detection scheme," *IEEE Transaction on Information Forensics and Security*, Vol. 10, No. 3, pp. 507–518, 2015.

[58] M. Zandi, A. Mahmoudi-Aznaveh, and A. Talebpour, "Iterative copy-move forgery detection based on a new interest point detector," *IEEE Transaction on Information Forensics and Security*, Vol. 11, No. 11, pp. 2499–2512, 2016.

[59] D. Cozzolino, G. Poggi, and L. Verdoliva, "Efficient dense-field copy-move forgery detection," *IEEE Transaction on Information Forensics and Security*, Vol. 10, No. 11, pp. 2284–2297, 2015.

[60] "Image manipulation dataset," *Department of Computer Science 5 of FAU*, [Online]. Available: http://www5.cs.fau.de/research/data/image-manipulation/.

[61] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-up robust features (SURF)," *Computer Vision and Image Understanding*, Vol. 110, No. 3, pp. 346–359, 2008.

[62] 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, No. 4, p. 199, 2011.

[63] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in *International Conference on Multimedia Information Networking and Security*, pp. 889–892, 2010.

[64] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in *IEEE International Conference on Multimedia Information Networking and Security*, Vol. 1, pp. 25–29, 2009.

A. Fattahi was born in Yazd on 1990. He received the M.Sc. degree in Islamic Azad University, Iran, in 2017, in Computer Software Engineering. His research interests are in image processing, robotics and intelligent systems, data base management, linux server management.

S. Emadi was born in Yazd on 1973. She received the B.Sc. and M.Sc. degrees both in Islamic Azad University, Iran, in 1995 and 1997, both in Computer Software Engineering. She is an Assistant Professor and Director of Computer Postgraduate with the Department of Computer Engineering, Yazd Branch of Islamic Azad University. His current research interests include services computing software, web service composition, service driven architecture, agile methodologies, software fault tolerance, software testing, design pattern, image processing and performance evaluation.