CrossMark

2-Levels of clustering strategy to detect and locate copy-move forgery in digital images

Mohamed Abdel-Basset[1] · **Gunasekaran Manogaran**[2] ·
Ahmed E. Fakhry[3] · **Ibrahim El-Henawy**[4]

Abstract Understanding is considered a key purpose of image forensic science in order to find out if a digital image is authenticated or not. It can be a sensitive task in case images are used as necessary proof as an impact judgment. it's known that There are several different manipulating attacks but, this copy move is considered as one of the most common and immediate one, in which a region is copied twice in order to give different information about the same scene, which can be considered as an issue of information integrity. The detection of this kind of manipulating has been recently handled using methods based on SIFT. SIFT characteristics are represented in the detection of image features and determining matched points. A clustering is a key step which always following SIFT matching in-order to classify similar matched points to clusters. The ability of the image forensic tool is represented in the assessment of the conversion that is applied between the two duplicated images of one region and located them correctly. Detecting copy-move forgery is not a new approach but using a new clustering approach which has been purposed by using the 2-level clustering strategy

✉ Mohamed Abdel-Basset
    analyst_mohamed@zu.edu.eg

    Gunasekaran Manogaran
    gunvit@gmail.com

    Ahmed E. Fakhry
    a.e.fakhry@gmail.comand

    Ibrahim El-Henawy
    ielhenawy@zu.edu.eg

[1] Faculty of Computers and Informatics, Department of Operations Research, Zagazig University, Zagazig, Egypt

[2] VIT University, Vellore, India

[3] Faculty of Information Systems and Computer Science, October 6 University, Cairo, Egypt

[4] Faculty of Computers and Informatics, Computer Science Department, Zagazig University, Zagazig, Egypt

Springer

based on spatial and transformation domains and any previous information about the investigated image or the number of clusters need to be created is not necessary. Results from different data have been set, proving that the proposed method is able to individuate the altered areas, with high reliability and dealing with multiple cloning.

Keywords Copy-move forgery · Digital image forensics · Manipulating detection · Copy-move localization

1 Introduction

Digital images are spread and used widely all over the world, but the bad quality effects can have a negative influence on these images. There are many ways of improving these images, like improving brightness, contrast, or even changing a colored image to gray. All the previous editing and ways of improving couldn't be considered as being manipulating. Unfortunately, software technologies are growing at a rate that allows the manipulation, alteration and even the creation of realistic synthetic images that far surpasses defensive measures. Crimes are spread everywhere and in many criminal cases, digital images play the role of evidence.

By considering digital content as a digital clue it is shown that a Multi-media forensics is considered as a supporter for making a decision or being a crime evidence [13, 29, 35] Multimedia forensics concerns developing technological tools which allow determining digital manipulating if exists without a necessity of knowing any previous information (watermarks) [3, 11] inside the image. The word forensics refers to "passive" in which the assessment formulation on a digital media depends on the digital asset itself, which allows us to find out the answers for many questions like "Is image content is manipulated?" [14, 33] "which acquisition device has been adopted?" [9, 38]. This paper answers the question related to the authenticity of the image content is given but this authenticity becomes uncertain because of the spread of digital image and ease of processing.

Figure 1 a photo on Facebook of a crowd of supporters of Prime Minister Najib Tun Razak is considered as a fake one because it is very obvious that crowd has been duplicated to appear larger. Figure 2 another photo from a newspaper that was tempered by duplicate people crowed to make a volume of people.

Modifying a digital image considered as crucial evidence to change a judgment at the court to change the meaning of what is shown in it. Furthermore, it is interesting to establish

Fig. 1 A fake photo

Fig. 2 A fake photo

something that is manipulated before in order to understand what will happen if there are any covered object or person, if a part of the image is cloned (copy-move attack), if any part is copied from another image (copy-paste attack).

In particular, a copy movie attack is going to be an area of concentration, in which a person who attacks and creates fake image by reproducing a certain area of an image on another area for the same image or another one, he is usually in necessity of applying a geometric transformation i.e. (scaling, translation, rotation…).

The proposed strategy that presented here is able to detect this kind of manipulation and localize these duplicated areas. Such strategy is based on Scale Invariant Features Transform (SIFT) [28]. It is well-known robust technique that is able to detect key points (features) and features matching that are belonged to cloned areas. These matched features are located under the umbrella of a 2-level clustering strategy in order to insure that points are used later to assist the geometric transformation of the cloned regions belonging to specified clusters representing the embedded regions in the given image.

Level A mission is to deal with the spatial domain offering a number of different clusters separated from each other. Then, level B mission is to combine these clusters to its related objects. The localization of the duplicated area depends on the clusters obtained in the last phase. This is completely done by using Structural Similarity Index (SSIM) between the original image and the duplicated one that is obtained from the estimated geometric transformation occurred in the manipulating attack [30]. We concentrated our study on using a better clustering algorithm (2-level clustering) and an algorithm for segmentation (SSIM) to enhance our results.

2 Literature review

Cloning is considered as one of the most commonly used techniques in digital image forgery. It is a process of copying and pasting portions of an image to another image scene. Detection of the cloning technique is very difficult if it's done in a proper, professional way by using the technique of retouching. Moreover, in case the copied parts are from a group of images with same features, some features as noise and color will be similarly comparable to rest of the images making it more difficult in detecting incompatibilities using statistical measures in different regions of the image [5, 15]. Furthermore, it is computationally infeasible to search all possible image locations and sizes if the cloned regions can be of any shape and location as an exhaustive search as pointed out in [17]. Many techniques are going under the umbrella of

manipulating, which can be classified into two main categories: **visual feature-based** and **block-based** methods.

2.1 Block-based methods

Classifying the image according to the overlapping blocks, showing the difference between the image in the original scene and the pasted one which is done by a block–based method. Representation of the blocks of the image through a low dimensional representation can be proved by applying the second process of feature extraction. In addition, different block-based representations are previously proposed in the literature, such as Discrete Wavelet Transform (DWT) [20, 25], Discrete Cosine Transform (DCT) [22] and Principal Component Analysis (PCA) [18, 32] for both tasks of copy-move detection [18, 22, 25, 26] and image splicing [21].

Recently, in the study of Bashar et al. [4], authors have proposed a duplication detection approach based on DWT and kernel principal component analysis (KPCA) techniques, moreover authors mentioned in [27] it's a necessity to use the radix sort for classifying the feature vectors for the divided sub-blocks, instead of classifying lexicographic, in which will improve the computational complexity of these methods, as However, all these methods suppose that the copied region is not gone through any post-processing such as rotation, scaling and JPEG compression.

Duplication detection approach is the method [7] which a Fourier Mellin Transform method is applied to each block. Forgery is performed in case there is more than one block connected and the distance between each pair of a block is the same. Forgery is often created by resizing, rotating and stretching portions of an image. Like creating a composition of two objects, one object resized to cope with the relative heights. This process requires re-sampling of the original image introducing specific periodic correlations between neighboring pixels.

Correlations due to re-sampling can be used to detect image changes [34] but can't handle specific manipulations. Consequently, it is better to use copy-move forgery detection technique as it is considered as a robust handling different transformation, such as rotation and scaling and some other manipulations including Gaussian noise, gamma correction, and JPEG compression.

In [6, 7, 19] two methods are used to detect small variations in rotation and scaling. The authors in [27, 36] discuss rotation transformations in which [36] suggest using Zernike moments in order to identify rotation copying in copy move manipulations while in [27] JPEG compression and Gauss noise manipulations are analyzed to understand how it works to detect the copy-move detection.

In [8] it is obvious that is a used method is being represented in order to detect duplication and transformation of regions through the usage of block description invariant to the reflection and rotation such as the log-polar block representation has summed along its angle axis. To this end, this general approach is presented in [10], in which the selected technique is used for better detecting rotation and scaling variations in the copied regions, instead of the wide usage of shift vectors. This phase called Same Affine Transformation Selection (SATS) and it is collocated after the feature extraction and block matching phases. As proved, they show that any set of rotation-invariant features like [8, 36, 40] can benefit from the inclusion of this processing step in the pipeline.
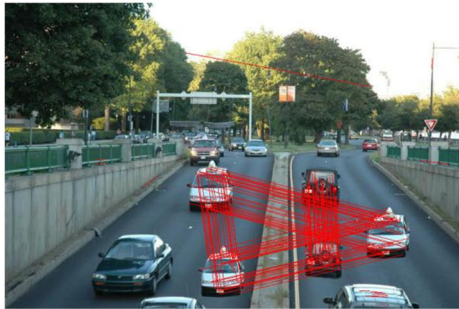
The selected strategy can be considered as a modified version of the scenario proposed in [2] for detecting copy-move forgeries and localizing these forgeries more efficiently, is given in Fig. 3, the detailed steps of the applied scenario are given in procedure no. 1.
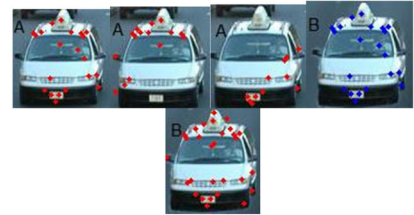
Test (Tampered) Image
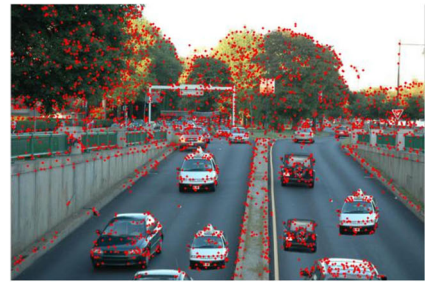
a Extract SIFT Features

b Match SIFT Features

c Excluding noise and keeping important features
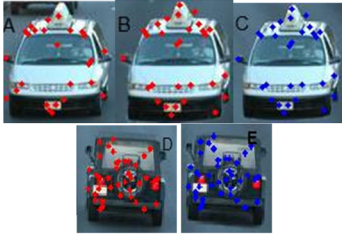(Clustering Phase A)

Fig. 3 Proposed method scenario

2.2 Visual feature-based method

It's proved that the usage of block-based methods is not sufficient enough for the wide usage, as it usually provides a fake and false significance of positives alarms for investigating images, for their nature of invariance compared to geometrical and affine transformations. And other manipulations like blurring and brightness changes. This insufficient usage raises the necessity of providing more robust methods that can be used to solve these issues, Feature-based methods try to address this problem by choosing to match key point-features and using the visual features found in the image instead of blocks.
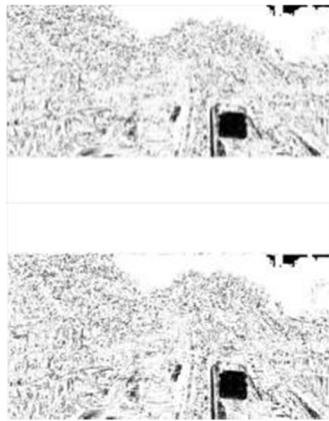
Many existed techniques are fell under this category as Speed Up Robust Features (SURF) and SIFT, which are widely applicable in image retrieval, object recognition, robotic mapping, and navigation, 3D modeling, and reconstruction. As proposed, discussing the problem of copy-move manipulating based on SIFT [41] however; the work which has been proposed [41] is not sufficient enough in case of multiple copy-move forgeries are exited.

The proved method in [1] provides a robust matching procedure that has been used in SIFT matching and then the clustering technique is performed on the coordinates of the key points that are found. On the contrary, the work has been proposed in [1] provides a good

d   Combining related clusters (Clustering phase B)

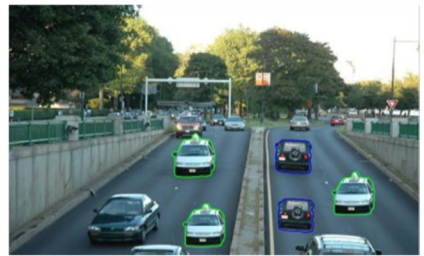**e**   Duplicated regions localization (on car E&D)

f   SSIM result on car SSIM result (on car E& D)

g   Segmentation result (on car E&D)

h   Segmentation (final result)

I   Investigation Result

Fig. 3 (continued)

performance about a copy-move forgery detection but it still suffers from lacking the ability to locate the duplicated regions.

In [23] a key step in localizing the duplicated region is proposed in order to enhance the usage of MPEG-7 features in order to detect and locate copy-move forgeries, by following a similar framework according to [1], but in many cases, the results of clustering and localization are not accurate and sufficient enough.

In [2] j-linkage method is used to detect and locate a copy-move forgery, which provides a better and more accurate results than those in [1, 23], this method provides a good sampling strategy and explores the idea of performing clustering on the matched pairs in the transformation of domain instead of the spatial domain using an adaptation of the original j-linkage algorithm for clustering and a block-wise correlation measure Zero mean Normalized Cross Correlation (ZNCC) to locate original and duplicated regions.

In this paper, methods are used in order increase the efficiency of detecting manipulated regions and accurately localizing these regions by performing some modifications on the scenario proposed in [2].

3 The proposed method

Our proposed strategy which can be considered as a modified version of the scenario proposed in [2] for detecting copy-move forgeries and localizing these forgeries more efficiently, is given in Fig. 2, the detailed steps of the applied scenario is given in procedure1.

3.1 SIFT features extraction

By using SIFT algorithm to extract stable and robust features against many forms of transformations such as rotation, scaling and my other affine transformations which is proposed in [1, 41]. This algorithm can be summed up into four main steps: i) detect scale-space extreme; ii) locate key points; iii) assign one or more orientations for every key point; iv) generate key point descriptors. Any image scale space can be represented as a pyramid of scale levels.

These levels can be obtained using sub-sampling of the image resolution and Gaussian smoothing, to find important key points using Laplacian of Gaussian (LoG) [1] is the best operation to perform the task, but unfortunately it has a very high computational cost, so an approximation of this operation is done using Different of Gaussian (DoG). Locating key points is performed by locating maxima/minima in DoG images, and then determine accurately these locations by finding the sub-pixel maxima/minima. Assignment of one or more canonical orientation (o) to each keypoint is performed using a gradient orientation histogram of each key point neighborhood.

Having an image to investigate I, let S: ={s1,…..,sn} considered as the list of n important key points detected in our image, where $s_i = \{x_i, d_i\}$ is a vector that stores every key point coordinates $x_i = (x, y)$, and d_i is the feature descriptor of the local neighborhood around that key point (i.e. 128 histograms of gradient orientations elements).

3.2 SIFT feature matching

SIFT features is a provided matching procedure to determine matched key points using g2NN strategy which is working in the following manner; having a set (S) of descriptors of size (n)

each of size (m), where (m) is the number of elements of each vector (128 for SIFT). And a set(X) of key points that are different from one show large Euclidean distances among them and vice versa.

The concept of the 2NN Test is a way to measure the ratio between the distance of the 2nd nearest neighbor and the candidate match (supposed to be low if a match lower than a chosen threshold T equals to 0.6 as suggested for that algorithm) and high if two different features, the g2NN works by iterating the 2NN test between $d_i/d_i + 1$ until this ratio is greater than T, where $T = 0.6$ [1]. Assume that k represents the value of procedure termination, then each key point in correspondence to a distance in $\{d_1,. .., d_k\}$ where $1 \leq k < n$ is considered as a match for the inspected key point. Finally, the matched points can be obtained by iterating over key points in set X. Matched key points only are kept, and no longer need for isolated ones in the following steps.

To calculate the step more efficiently, MATLAB is used to find the ratio of angles (inverse cosine of dot products of unit vectors) which are considered as a close approximation to the ratio of Euclidean distances for small angles. It's only about keep tracking of the matches in which the ratio of vector angles from the nearest to second nearest neighbor is less than distance Ratio (in our experiments we choose 0.6).

3.3 Clustering

Detecting the cloned areas is achieved by using the most important steps which are the clustering and also in the next step which is localizing these areas. In [2] clustering algorithms has been proved in author's experiments that deal only with the coordinates of the key points in spatial domain and not the matching constraint between points. It is not good enough to perform the task, hierarchical agglomerative clustering (HAC) procedure is the most famous procedure that have been used as it is proposed in [1].

But due to its drawbacks which can be summarized as follows: i) it is very difficult to identify single patches that have key points with non-uniform spatial distribution, ii) there is no way to separate duplicated regions In case they are very near to each other. In our proposed clustering algorithm we are going to apply two phases of clustering one is performed in spatial domain taking in consideration the matching constraint between points and then the output of this phase is entered to the next phase which is performed in transformation domain see Fig. 3.

3.3.1 Phase A: clustering in spatial domain

In this phase, an isolating strategy of unwanted matches (noise matches) is the main purpose and keeping track of the main matches that can be considered as the main clusters representing the duplicated regions. Using a value 0.6 as a threshold value for T gives out all possible matches, but also increases the number of the unwanted matches even if it has been examined to decrease the value of T the unwanted matches still exist see Fig. 4a, b. So, in the next procedure an idea of isolating these matches is suggested. A threshold value $T = 0.55$ is used in the g2NN test which is better than using 0.6, this helps in decreasing the unwanted matched points while keeping enough number of possible matches that represent duplicated regions Fig. 4a, b.

Calculating local density function of key-points It is observed that matched pairs specified within duplicated regions are denser than other unwanted matched points. In [12] the

Original image

a Using T=0.55for g2NN

b Using T=0.6 for g2NN

Fig. 4 Clustering in spatial domain

authors have produced an idea of a clustering technique that provides good results in the area of based spatial clustering of applications with noise using Density-based spatial clustering of applications with noise (DBSCAN), "the distribution of points belonging to a cluster should be denser than that of the outside".

step1: by calculating the density of the data space around each point that can be considered as the sum of the influence function of all data points surrounding this point. The influence function of point **X** on point **Y** can be represented by the impact of point **X** on point **Y** as the Euclidean distance between them:

$$\mathrm{INF}(x, y) = \sqrt{\sum_{i=1}^{d} (x_i - y_i)^2} \qquad (1)$$

(in this experiment d = N-1, where N Is the total number of key points). As the distance between the two points decreases, the impact of **X** on **Y** increases and vice versa.

step2: Calculate the local density function for point **X** as the summation of (influence functions within the k-nearest neighbors) distances among the point **X** and the k-nearest neighbors and keep track of these distances. The local density function of point **X** with respect to other k-points is given by:

$$\text{LOC-DEN}(X, y_1, y_2, \ldots . y_k) \sum_{i=1}^{k} \text{INF}(X, yi) \tag{2}$$

(in our experiments k = 10).

> **step3:** Sort all the points(×1,×2,…..xn) in ascending order according to their **LOC-DEN function**

Isolate unwanted matches A number of clusters are created by representing matched regions see Fig. 3. The needed target is to only keep the matched pairs representing the three statues in the image. The used procedure is explained in the following steps:
All of the above steps are repeated until all matched pairs are examined.

3.3.2 Phase B: clustering in transformation domain

The clusters that are produced from the previous phase are then reassembled to give the final clustering result by representing the duplicated regions [37]. In that proposed strategy a method is going to be used in order to find the best model that fits2D homograph with the highest appropriate inlier points using Random sample consensus (RANSAC).

This method works on two sets of homogeneous-points (representing the original and duplicated regions X1 and X2 respectively). The two sets X1& X2are supposed to be 2*N, where N is the number of the provided points these points are then padded with homogeneous scale factor of 1and also a distance threshold (**t**) (set to 0.005 in our experiment) is provided representing the distance between the model and data point which is used to decide whether a point is an inlier or not.

Finally, the appropriate H can be detected with the satisfied indices of inlier points. Where H is 3×3 homography matrix representing the transformation applied X2 = H * X1. And inliers which are an array of indices of (some or all) of the elements of X1, X2 that are found as the best model. It starts its work by doing a normalizing step on each set of points so, the origin is sqrt(2) at centroid and mean distance from origin. Both sets are stacked together (6*N) to be ready to go under RANSAC.

RANSAC is a resampling technique which generates candidate solutions by using the minimum number of observations (data points) required to estimate the underlying model parameters. As pointed out by Fischler and Bolles [16]. RANSAC works iteratively on N iterations ($N = 100$ in our experiments) & max data trials (M = 5) to select anon-degenerate data set of X1 & X2.Also a desired probability ($P = 0.99$) of choosing at least one sample free from outliers.

It begins by selecting random non repeated points, then compute the homography using the Normalized Direct Linear Transformation (NDLT) affine homography algorithm as proposed by Hartley and Zisserman in [39], given a set of correspondences (×1,×2,…….. x(k + 1)) and (×1',×2',………x'(k + 1)), the algorithm minimizes the following objective function:

$$\sum_{i=1}^{k+1} \left\| \mathbf{x}_i' - \mathbf{H}\mathbf{x}_i \right\|^2. \tag{3}$$

Storing the best no of inliers with the best model found so far, calculating the probability of inliers found (Pin = the number of inliers found/no of points) & the probability of outliers

START

step1: a new matched pair is selected **m** = (X; X') from the set M, in which X and X' are defined by their coordinates (x,y) & (x',y') respectively

step2: suppose we have two sets **O(original)** and **D(double)** of w nearest neighbors to the key point coordinates of X and X', respectively (w=12 in our experiments).

step3: select another **V** matched pairs from **M**= {(X,X')1, (X,X')2,...... (X,X')q} such that X ∈ O and X' ∈ D and V=3 (the minimum no points representing a region).

if not exist, store the matched pair (**m** selected previously) as an isolated match in the form of a (**1*4**) matrix and return to step1

Otherwise, go to **step4**

From **step4** by checking how closely **(m)** is related to **(V)** selected pairs

step4: examine how closely **selected** **m=(X,X')** related to matched **V={(X1,X1'),(X2,X2'),(X3,X3')}**

test1:
- Calculate the distance between every two matched points included in **(m) & (V)**
- Calculate the percent variation in distance which is given by:
    DiffPercent = (higher value - lower value) / lower value x 100 **(3)**
- A comparing threshold (**F2= 0.045** In our experiments) is used for checking
   If (DiffPercent>F2)
   - test1Result=false
- Store the matched pair (**m** selected previously) as an isolated match in the form of a (**1*4**) matrix and return to step1
   Otherwise
- go to test2

test2:
- Evaluate **r1, r2, r3** representing the position of **X** in **X1, X2 & X3** lists.
- Evaluate **rr1, rr2, rr3** representing the position of **X1, X2 & X3** in **X** list.
- Evaluate **s1, s2, s3** representing the position of **X'** in **X1', X2' & X3'** lists.
- Evaluate **ss1, ss2, ss3** representing the position of **X1', X2' & X3' in X'** list.
- Evaluate **t1** representing the position of **X** in **X'** list.
- Evaluate **t2** representing the position of **X'** in **X** list. A comparing threshold (**F= 5** In our experiments) is used for checking
   If [min(r1,r2,r3)>F || min(rr1,rr2,rr3)>F || min(s1,s2,s3)>F || min(ss1,ss2,ss3)>F || t1<= min(ss1,ss2,ss3) || t2<= min(rr1,rr2,rr3)]
      - store the matched pair (**m** selected previously) as an isolated match and return to step1.
   If [t2>=max(rr1,rr2,rr3) && t1>=max(ss1,ss2,ss3)]
   test2Result=true
      If test1Result==true && test2Result==true
      - store **m** with **V** in the form of a matrix of size (**n*4**) where **n** is the number of records representing **Xs,X's** of the duplicated regions. In the next iterations **n** is extended if there exists common matches
      Otherwise
      - store the matched pair (**m** selected previously) as an isolated match in the form of a (**1*4**) matrix and return to step1.

END

found (Pout = 1-Pin^4) & updating Update the estimate of N, the number of trials to ensure we pick (N = log(1-p)/log(Pout)).

In particular, transformations are used to detect the geometric distortions between the copied and original regions like scaling, rotation, and shearing. In matrix form this kind of transformation comes as:

$$
\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & t_x \\ a_{21} & a_{22} & t_y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = \mathbf{H} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \tag{4}
$$

3.4 Duplicated regions transformation estimation

All clusters now represent the matching regions Fig. 3 (e,d). The estimation of the transformation for every two matched regions, re-calling RANSAC again with (N = 1000& M = 100). Since all the points related to the original region (**RO**) having equivalent points related to its duplicated region (**RD**) through the same transformation (**T**) (expressed in matrix form as **H**):

$$
RD = H*RO, RO = H\text{-}1*RD \tag{5}
$$

After estimating **H** (If **H**is non-empty matrix, then the image is suffering of copy-move forgery) **H**is then applied on the entire image, obtaining two overlapping images where the first region **RO** will overlap the second region **RD,** by the same way applying the inverse transformation **H-1**, the region **RD** will overlap the region **RO**. This operation is continued until all duplicated regions are examined.

3.5 Duplicated regions localization

In this phase every two wrapped images are tackled, (**W1, W2**) obtained in the previous step with the original image (**O**) in SSIM, producing (**I1 & I2**). SSIM is used to measure the similarity between any two images. A Detailed description is given in [39]. Before start working O, W1, W2 should be changed to gray double images. Pre-defined parameters should be considered in the tackled experiments, these parameters are set with the following values: a Gaussian window is defined with (**size = 5 with a blurring factor = 1.2**), dynamic range (**L = 255**), constant K is set to a very small value (**K = 0.00001**). Some of these parameters are re-customized to achieve the required goal.

$$
\mathbf{I1 = SSIM\,(O, W1), \quad I2 = SSIM(O, W2)C = \left(K^*L\right) \wedge 2} \tag{6}
$$

$$
\text{SSIM(x, y)} = \frac{2\mu_x\mu_y + C_1\left(2\sigma_{xy} + C_2\right)}{\left(\mu_x^2 + \mu_y^2 + C_1\right)\left(\sigma_x^2 + \sigma_y^2 + C_2\right)}. \tag{7}
$$

Where C1& C2 = C (in our experiments).I1& I2are considered as SSIM maps.

Q = complement (I1^ 0.67) **B** = complement (I2^ 0.67) (To decrease unwanted details and to prepare it for segmentation).

3.6 Segmentation of objects in SSIM maps

In this, separating the black car from the image is tackled. Segmentation algorithms is one of the most famous method that can be used in our case, region growing segmentation algorithm uses a seed **point(x,y)** which has been chosen randomly and spontaneously as a starting point that works on **Q&B** images that are produced from the previous step, according to a given maximum intensity threshold (**v = 0.27** in our experiments). It's obvious that the region continues to grow iteratively by comparing all unallocated neighboring pixels to the region. The difference between the region's mean and a pixel's intensity value can be considered as a similarity measure. The pixel with the smallest difference measured this way is allocated to the respective region. The process terminated if the intensity difference between new pixel and region mean become larger than (**v**). The region is selected with intensity values (equal to 1). Finally, gaps filled by mathematical morphological operations in the binary image.

4 Results and discussion

The proposed methodology has been evaluated according to two main points of view (**detection capability**) and also (**accurate localization**) compared to the two methods provided in [1, 2], on a novel realistic multiple cloning dataset called MICC-F8 and secondly, on more larger dataset named as MICC-F2000 in addition to MICC-F220 to test for our clustering strategy, another dataset of Personal Columbia downsized pictures of 800 authentic images is involved to ensure detection capability.

In our experiments we use MATLAB for implementation on a machine with Intel(R) Core(TM)2 Duo CPU-P7450@2.13 GHz, With 4GB of RAM, the whole procedure takes about 20 to70 seconds depending on some factors like image size, the number of key points and the number of matches to be examined.

4.1 Datasets

Four famous datasets have been examined in these experiments MICC-F2000, MICC-F220, MICC-F8 and a dataset of Personal Columbia downsized pictures of 800 authentic images. MICC-F2000 are composed of images with disparate contents coming from the Columbia photography image repository [31] and from a personal collection, is composed of 2000 photos with 2048*1536 pixels where 1300 are original and the others have tampered.

The tampered picture generated by applying many attacks using rotation, translation, and scaling. The duplicated patches (corresponding to an average size of 1.12% of the whole image) are rectangular and they are not accurately segmented or spatially well separated from the original areas. MICC-F220 consists of 220 images where 110 are original and 110 are manipulated. The image resolution varies from 722×480 to 800×600 pixels and the size of the forged patch covers, on the average, 1.2% of the whole image. MICC-F8 consists of 8 tampered images with realistic multiple cloning, which are originally found in MICC-F2000.

4.2 Evaluation criteria

Detection Capability is measured in terms of the True Positive Rate (**TPR**) and False Positive Rate (**FPR**), where TPR is the fraction of tampered images correctly identified as such, while

FPR is the fraction of original images that are not correctly identified:

$$TPR = \frac{\#\ images\ detected\ as\ forged\ being\ forged}{\#\ forged\ images} \tag{8}$$

$$FPR = \frac{\#\ images\ detected\ as\ forged\ being\ original}{\#\ original\ images} \tag{9}$$

And also patch localization can be computed as the percentage of erroneously matched pixels **FP** (false positives) and erroneously missed pixels **FN** (false negatives). Formally, let **R1** be the copied region, **Ri** $(i > 1)$ be the ith duplicated region and **B** representing the unchanged background. So **FP** and **FN** can be defined as:

$$FP = \frac{|matches\ in\ B|}{|B|} \tag{10}$$

$$FN = \frac{|missed\ matches\ in\ UiRi|}{|UiRi|} \tag{11}$$

Where low FP& FN implies high accuracy localization.

4.3 Results on MICC-F2000, MICC-F220, MICC-F8 datasets

The method which is proposed in [2] detects if an image forged by finding one affine transformation at least, and it fits N number of points of an image area and other N points of another image area. It also demonstrated that the high value of N (i.e N > =7) means a higher TPR and a lower FPR. In this tackled method the value of N should be high because of applying clustering in the spatial domain ensures having a bigger value for N for the next steps for calculating the affine transformation in most of the cases see (Fig. 3d,e), but our proposed method doesn't affected by the value of N thus makes it much better. Table 1 shows a comparison of different sample set sampling strategies that are important for providing better clusters which affect the forgery detection accuracy between the proposed method and the one which proposed in [2].

Table 2 shows a comparison in the TPR and FPR values for MICC-F2000 using proposed method, the j-linkage method in [2] and the proposed by Amerini et al. in [1] which has two main drawbacks; 1) if two or more cluster points are near each other then they can form wrong clusters, another drawback that if a cluster points are scattered away from its centroid then they can be combined to another cluster, thus not accurate results.

Table 1 Different sample set sampling strategies comparisons

	Proposed Method	Using j-linkage in [2] $N=9$
TPR(%)	83.63	81.60
FPR(%)	5.75	7.27
FP	0.45	0.31
FN	13.23	6.59

Table 2 Comparison in the TPR and FPR values for MICC-F2000

	Data sets	Proposed method	j-linkage in [2]	Amerini et al. in [1]
TPR(%)	MICC-F2000	95.63	94.86	93.42
FPR(%)		8.75	9.15	11.61

Table 3 Results for MICC-F220 dataset

	Data sets	Proposed method	Kaur et al. in [24]	
			SURF	PCA-SIFT
TPR(%)	MICC-F220	97.87	–	–
FPR(%)		7.63	10	7.27

Table 3 shows the results of TPR and FPR values using the proposed method and the proposed by Kaur et al. in [24] for MICC-F220 which uses two famous methods SURF and PCA-SIFT, but it was proved that SIFT can provide more accurate key points than both. Table 4 shows the results of TPR and FPR values using the proposed method for MICC-F8 dataset.

Some examples of results are proposed in Fig. 5 (obtained from MICC-F8) dataset achieved by the proposed method the localization accuracy has been evaluated visually. The proposed method is able to accurately segment the duplicated regions, or even the image contains multiple copy-move regions.

5 Conclusions and future works

This research presents a new strategy based on SIFT features is tackled to detect and locate accurately copy-move forgeries that have been presented, the two levels of clusters are examined in which one level in the spatial domain isolates the unwanted matches and keeps the most important matches that represent the main clusters, the second level works in the transformation domain by combining related clusters (belonging to same regions). This procedure can also deal in the presence of multiple copy-move forgeries. The capability of detection measured in terms of True Positive Rate (TPR) and False Positive Rate (FPR) and as the percentage of erroneously matched pixels False Positives (FP) and erroneously missed pixels False Negatives (FN).

The overall efficiency has to be improved in terms of time-consuming. A way to detect is necessary to be found. If an object is covered with a copied flat patch, SIFT algorithm still not able to detect this kind of forgery.

Table 4 Results for MICC-F8 dataset

	Data sets	Proposed method
TPR(%)	MICC-F8	98.79
FPR(%)		5.23
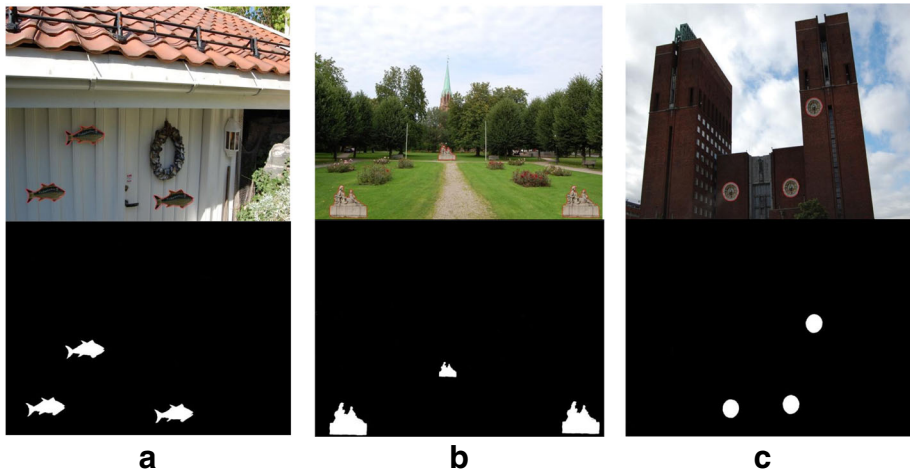
Fig. 5 Results achieved for MICC-F8

As a future work, we can implement other algorithms with the same scenario in particular clustering algorithm because it is the most important stage in the process and it definitely will be affected by the final result. Since the presence of blurring or Gaussian noise in image could have a negative impact on the quality, then we are going to work with two different scenarios, the first one is to enhance the SIFT algorithm to be able to work much better under these conditions, the second one is to develop an algorithm to recover the image that suffers from blurring or Gaussian noise.

References

1. Amerini I, Ballan L, Caldelli R, DelBimbo A, Serra G (2011) ASIFT based forensic method for copy move attack detection and transformation recovery. IEEE Trans Inf Forensics Secur 6(3):1099–1110
2. Amerini I, Ballan L, Caldelli R, DelBimbo A, Serra G (2014) Copy-move forgery detection and localization by means of robust clustering with J-Linkage
3. Barni M, Bartolini F (2004) "Watermarking systems engineering enabling" Digital assets security and other applications. Marcel Dekker
4. Bashar M, Noda K, Ohnishi N, Mori K (2018) Exploring duplicated regions in natural images. IEEE Trans Image Process
5. Bayram S, Avcibas I, Sankur B, Memon N (2005) Image manipulation detection with binary similarity measures. In: Proc. of EUSIPCO, Antalya, Turkey
6. Bayram S, Sencar HT, Memon N (2008) A survey of copy-move forgery detection techniques. In: Proc. of IEEE Western New York Image Processing Workshop
7. Bayram S, TahaSencar H, Memon N (2009) An efficient and robust method for detecting copy-move forgery. In: Proc. of IEEE ICASSP, Washington, DC, USA
8. Bravo Solorio S, Nandi AK (2009) Passive method for detecting duplicated regions affected by reflection, rotation and scaling. In: Proc. of EUSIPCO, Glasgow, Scotland

9. Chen M, Fridrich J, Goljan M, Lukas J (2008) Determining image origin and integrity using sensor noise. IEEE Trans Inf Forensics Secur 3(1):74–90
10. Christlein V, Riess C, Angelopoulou E (2010) On rotation invariance in copy-move forgery detection. In: Proc. of IEEE WIFS, Seattle, WA, USA
11. Cox IJ, Miller ML, Bloom JA (2002) Digital watermarking. Morgan Kaufmann, San Francisco
12. Fahim A, Saake G, Salem A, Torkey F, Ramadan M (2009) Improved DBSCAN for spatial databases with noise and different densities. GESJ 3(20):53–60
13. Farid H (2009) Photo fakery and forensics. Adv Comput 77:1–55
14. Farid H (2009) A survey of image forgery detection. IEEE Signal Process Mag 2(26):16–25
15. Farid H, Lyu S (2003) Higher-order wavelet statistics and their application to digital forensics. In: Proc. of IEEE CVPR Workshop on Statistical Analysis in Computer Vision, Madison, WI, USA
16. Fischlerand MA, Bolles RC Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. Commun ACM 24(6):381–395
17. Fridrich J, Soukal D, Lukás J (2003) Detection of copy-move forgery in digital images. In: Proc. of DFRWS
18. Fridrich J, Soukal D , Lukás J (2003) Detection of copy-move forgery in digital images. In: Proc. of DFRWS, Cleveland, OH, USA
19. Fridrich J, Soukal D, Lukás J (2003) Detection of copy-move forgery in digital images. In: Proc. of DFRWS
20. He Z, Sun W, Lu W, Lu H (2011) Digital image splicing detection based on approximate run length. Pattern Recogn Lett 32(12):1591–1597
21. He Z, Lu W, Sun W, Huang J (2012) Digital image splicing detection based on markov features in DCT and DWT domain. Pattern Recogn 45(12):4292–4299
22. Huang Y, Lu W, Sun W, Long D (2011) Improved DCT based detection of copy-move forgery in images. Forensic Sci Int 206(1–3):178–184
23. Kakar P, Sudha N (2012) Exposing post-processed copy-paste forgeries through transform invariant features. IEEE Trans Inf Forensics Secur 7(3):1018–1028
24. Kaur H, Saxena J, Singh S (2015) Simulative Comparison of Copy- Move Forgery Detection Methods for Digital Images. International Journal of Electronics, Electrical and Computational System IJEECS, ISSN 2348-117X Volume 4, Special Issue
25. Li G, Wu Q, Tu D, Sun SJ (2007) A sorted neighborhood approach for detecting duplicated region in image forgeries based on DWT and SVD. In: Proc. of IEEE ICME, Beijing, China
26. Lin Z, He J, Tang X, Tang CK (2009) Fast automatic and fine grained tampered JPEG image detection via DCT conceit analysis. Pattern Recogn 42(11):2492–2501
27. Lin HJ, Wang CW, Kao YT (2009) Fast copy-move forgery detection. WSEAS Trans Sig Proc 5(5):188–197
28. Lowe DG (2004) Distinctive image features from scale invariant keypoints. Int J Comput Vis 60(2):91–110
29. Lyu S, Farid H (2005) How realistic is photorealistic? IEEE Trans Signal Process 53(2):845–850
30. Mohamed Mursi MF, Salama MM, Habeb MH (2017) An improved SIFT-PCA-based copy-move image forgery detection method. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE) 6(3)
31. Ng T-T, Chang S-F, Hsu J, Pepeljugoski M (2004) Columbia photo-graphic images and photorealistic computer graphics dataset. ADVENT, Columbia University, Tech. Rep
32. Popescu A, Farid H (2004) Exposing digital forgeries by detecting duplicated image regions. Dartmouth College, Computer Science Tech. Rep. TR2004–515
33. Popescu A, Farid H (2005) Statistical tools for digital forensics. In: Proc. of Int. Workshop on Information Hiding, Toronto, Canada
34. Popescu AC, Farid H (2005) Exposing digital forgeries by detecting traces of resampling. IEEE Trans Signal Process 53(2):758–767
35. Redi JA, Taktak W, Dugelay JL (2011) Digital image for ensics: a booklet for beginners. Multimed Tools Appl 51(1):133–162
36. Ryu S, Lee MJ, Lee HK (2010) Detection of copy – rotate – move forgery using zernike moments. In: Proc. of International Workshop on Information Hiding, Calgary, Canada
37. Singh RD, Aggarwal N (2017) Detection and localization of copy-paste forgeries in digital videos. Forensic Sci Int 281:75–91
38. Swaminathan A, Wu M, Liu K (2008) Digital image forensics via intrinsic fingerprints. IEEE Trans Inf Forensics Secur 3(1):101–117
39. Wang Z, Bovik AC, Sheikhand HR, Simoncelli EP (2004) Image quality assessment: From error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
40. Wang J, Liu G, Li H, Dai Y, Wang Z (2009) Detection of image region duplication forgery using model with circle block. In: Proc. of MINES, Washington, DC, USA
41. Yanga F, Lia J, Lua W, Wengb J (2017) Copy-move forgery detection based on hybrid features. Eng Appl Artif Intell 59:73–83

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Prof. Dr. Mohamed Abdel-Basset Received his B.Sc., M.Sc and the Ph.D in operations research from Faculty of Computers and Informatics, Zagazig University, Egypt. He is a head of department of operations research and decision support, Faculty of Computers and Informatics, Zagazig University. His current research interests are Optimization, Operations Research, Data Mining, Computational Intelligence, Applied Statistics, Decision support systems, Robust Optimization, Engineering Optimization, Multi-objective Optimization, Swarm Intelligence, Evolutionary Algorithms, and Artificial Neural Networks. He is working on the application of multi-objective and robust meta-heuristic optimization techniques. He is also an/a Editor/reviewer in different international journals and conferences. He has published more than 100 articles in international journals and conference proceedings.

Prof Dr. Gunasekaran Manogaran is received his PhD from the Vellore Institute of Technology University, India. He received his Bachelor of Engineering and Master of Technology from Anna University and Vellore Institute of Technology University respectively. He has worked as a Research Assistant for a project on spatial data mining funded by Indian Council of Medical Research, Government of India. His current research interests include data mining, big data analytics and soft computing. He is the author/co-author of papers in conferences, book chapters and journals. He got an award for young investigator from India and Southeast Asia by Bill and Melinda Gates Foundation. He is a member of International Society for Infectious Diseases and Machine

Intelligence Research labs.

Dr. Ahmed E. Fakhry Received his B.Sc. degree and master degree from Cairo University, faculty of computers and informatics, Egypt. His area of interest includes is computation intelligence, Optimization, Swarm Intelligence, Evolutionary Algorithms, and Artificial Neural Networks.

Prof. Dr. Ibrahim El-henawy , he is a head of Department of computer science, Faculty of Computers and Informatics, Zagazig University, Egypt. His area of interest includes software engineering, computational intelligence, optimization techniques, bio-informatics, and embedded systems. He has authored more than 250 publications in different journals and conference of national and international repute. His current research work includes machine learning, optimization, image processing and advances in mobile computing and communications. He is also an/a Editor/reviewer in different international journals and conferences.