Multimedia Tools and Applications
https://doi.org/10.1007/s11042-019-08044-8

A passive forensic scheme for copy-move forgery based on superpixel segmentation and K-means clustering

Yong Liu[1] · Hongxia Wang[2] · Yi Chen[3] · Hanzhou Wu[1] · Huan Wang[4]

Received: 22 September 2018 / Revised: 5 July 2019 / Accepted: 26 July 2019
Published online: 01 September 2019

Abstract
Copy-move forgery is a commonly used operation for digital image. Most of the existing copy-move schemes designed to region duplication are block-based and keypoint-based. In general, block-based methods fail to handle geometric transformations. Though keypoint-based methods can handle geometric transformations, they have a poor detection effect on the smooth region. This has motivated us to propose an efficient copy-move forgery detection method, which is based on superpixel segmentation and cluster analysis to improve the detection accuracy due to some specified attacks in this paper. In the proposed method, K-means clustering technology is used to divide the superpixel of the image into complex regions and smooth regions. The clustering rule is based on the mean and standard deviation of the pixels, and the ratio of the feature points in the superpixel block, this clustering method can distinguish complex regions (non-smooth regions) and smooth regions. In complex regions, Scale-Invariant Feature Transform (SIFT) features are used to detect tampering. In smooth regions, the sector mask feature and RGB color feature are proposed to detect tampering. Filtering out error matching is applied to these two kinds of regions for the copy-move detection. Experimental results have shown that the proposed method can detect the tampering of complex regions and smooth regions and it indeed has the advantage in the detection accuracy compared with some related works when the test images are processed by blurring, adding noise, JPEG compression and rotation.

Keywords Copy-move forgery detection · Image segmentation · Cluster analysis · Harris points · Sector mean · RGB color feature

1 Introduction

With the rapid development of science and technology and powerful image software widely used, it is easy to use some software to tamper digital images. Meanwhile, it is difficult to distinguish whether the image is tampering or not by the naked eye. Moreover, the tampered

✉ Yong Liu
liuyongresearch@163.com

Extended author information available on the last page of the article

image can cause great harm in forensic investigation [23], internet of things forensics [18], smartphone forensics [9] and so on. Therefore, we are in urgent need of an effective forgery detection method to determine whether digital images are tampered [6]. In general, image authentication technology can be classified as active forensics and passive forensics in the existing studies [16]. Active authentication technology adopts digital watermarking technologies [25] to embed some watermarks into digital images to protect copyrights or integrity of digital products. The receivers can extract the hidden watermark information to judge whether the digital images have been tampered. However, watermarks need to be generated by some special methods, and they need to be embedded into the digital image in advance. In the contrary, passive authentication is the process of detecting whether a digital image is tampered without any additional information except for itself [34]. Compared with active authentication, passive authentication is more practical, and it has become a very valuable research hotspot.

In many forgery techniques, copy-move forgery is a common tampering method for digital images. In copy-move forgery, one can copy some regions from an image and past the copied regions into other regions in the same image with the motivation of hiding undesired objects or emphasizing objects. Due to the duplicated regions come from a same digital image, they have many of the same features, such as the color palettes, noises and dynamic ranges, they are compatible with the remainder of the image [12], so it is difficult for human eyes to distinguish the forgery from the original.

In copy-move forgery detection algorithms, it is common to find possible similar regions. Some match areas may be mismatches, it is necessary to remove the mismatches through filtering processing. In this process, geometric inconsistency is usually used. There are texture-rich regions and smooth regions in the image. Owing to the fact that the smooth regions are extremely similar, some copy-move forgery detection methods neglect these regions to achieve a better detection performance. These methods may not be able to detect the smooth copied regions. Although numerous copy-move forgery detection methods have been proposed, processing the test image with smooth regions is still a challenge.

This paper proposes a new and effective solution to deal with smooth regions. Firstly, the method uses simple linear iterative clustering (SLIC) superpixel segmentation and K-means clustering technology to divide the image into complex regions and smooth regions. Clustering is based on the mean and standard deviation of pixels and the ratio of feature points to the total pixels of the block. Secondly, feature matching and filtering error matching are performed in the complex region and smooth region respectively, and SIFT feature points are used to match in the complex region. In the smooth region, the matching feature is constructed by extracting the dense Harris points, which is a sector feature including RGB three channel color characteristics. Experimental results show that the proposed method not only can detect copy-move forgery in complex regions but also can detect the forgery in smooth regions, and it is robust to blur, noise, JPEG compression, and rotation attacks.

The main contributions of our proposed approach can be summarized as follows. (1) Image segmentation and k-means clustering are used to divide the image into complex regions and smooth regions, which is helpful to detect smooth regions more accurately. The proposed method not only can detect copy-move forgery in complex regions but also can detect the forgery in smooth regions. (2) We obtain enough key points by using lower extraction thresholds in smooth regions. (3) A sector feature vector with rotation invariance for tampering detection in smooth regions is constructed by combining RGB color feature information.

The rest of this paper is organized as follows. In Section 2, the previously proposed copy-move forgery detection methods are reviewed briefly. In Section 3, the proposed method is

described in detail. The experimental results are provided in Section 4. Finally, we conclude this paper in Section 5.

2 Related works

In recent years, many scholars have put forward many copy-move forgery detection methods, these methods can be mainly classified into two categories: block-based methods and keypoint-based methods.

2.1 Block-based methods

Many of early copy-move forgery detection schemes are block-based methods. Fridrich et al. [8] first proposed a block matching detection method based on Discrete Cosine Transform (DCT), this method divides the test image into 8×8 overlapping blocks and extracts Discrete Cosine Transform (DCT) features from the overlapping blocks. The features of all blocks are sorted lexicographically and similar block feature vectors are identified to judge forgery. This method can detect the copy-move forgery, but it has high computational complexity. Thereafter, some efficient block-based algorithms were proposed in [14, 20, 21, 28]. Popescu et al. [20] proposed the Principle Component Analysis (PCA) to reduce the feature dimension. In [14], Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) are combined to generate feature vectors, which are then matched to detect duplicate region. Wang et al. [28] proposed a passive authentication scheme for copy-move forgery based on DCT and the package clustering algorithm, the Discrete Cosine Transform (DCT) was used to extract features, the package clustering algorithm is applied to replace the general lexicographic order technologies to improve the detection precision. However, it is difficult to resist rotation tampering for this scheme. In Wang [26] and Ryu [22], Hu Moments (HU) and rotation invariant Zernike Moments (ZERNIKE) are respectively used to judge forgery. In [21], a suspicious image is taken and features are extracted through the Block Discrete Cosine Transform (BDCT) and enhanced threshold method. For copy-move detection, Zernike Moment-polar is used to improve the detection precision and locate the duplicated regions in image.

All the algorithms mentioned above apply a feature extraction process to each overlapping block. Block-based methods are typically robust to blur, add noise, JPEG compression, but most of them lack of robustness against rotation attacks, they also have a high complexity and take a long time to run when the image size is large.

2.2 Keypoint-based methods

Keypoint-based methods do not take advantage of block-based feature representation. These algorithms identify high entropy regions (keypoints) in the test image and extract feature vectors only at the key points extracted, they reduce the number of feature vectors, and keypoint-based methods cost less time. Huang et al. [10] proposed a method to detect tamper regions based on Scale-Invariant Feature Transform (SIFT) key points. In [35], matching feature is SIFT feature, and then the global context descriptor based on overlapping regions is extracted to test the matching pair. Amerini et al. [2] used SIFT keypoints to detect the tamper regions. They put forward the generalized 2NN test (g2NN) for feature matching, then

stratified clustering and Random Sampling Consistency (RANSAC) were used to filter outliers. In [13], a hybrid method was proposed by Kumar, the key points in the image are detected by Speed-Up Robust Features (SURF), and the corresponding features of these key points are represented by the Binary Robust Invariant Scalable Keypoints (BRISK) feature. Zandi et al. [31] proposed an iterative copy-move forgery detection based on a new interest point detector, the new interest point detector is used to extract the keypoints. In addition, a new filtering algorithm is employed, which can effectively prune the falsely matched regions, so it has high detection accuracy.

Although keypoint-based methods have strong robustness to geometric transformation and low cost, they may not be able to handle smooth regions. In [5], the key points were extracted by detecting Harris feature points, and then the feature vectors were matched by step sector statistics. This method does not get enough key points in the smooth region, which leads to its poor tamper detection effect in the smooth regions. In [15], the proposed scheme first segments the test image into semantically independent patches, SIFT keypoints were matched between patches and Expectation Maximization algorithm (EM) was used to filter false alarm patches Although the scheme can reduce the affine estimation error, it failed to detect the forgery in smooth regions of the image. In [27], the matching feature is the average DC coefficient and AC DCT coefficient of each Harris point. As a result of DCT coefficients do not have rotation invariance, this method is less robust to rotation. In [17], it first uses simple linear iterative clustering (SLIC) superpixel segmentation and pixel clustering technique to partition the image content into complex regions and smooth regions. The result of pixel clustering is not good for some images, the color feature of the image was not considered when it detects the smooth regions, it may lead to some tampered images cannot be detected.

In summary, some block-based methods are less robust to rotation. Comparatively speaking, some keypoint-based methods are robust to rotation, but they cannot get enough key points in the smooth region, which leads to its poor tamper detection effect in the smooth regions.

In the next section, we propose an algorithm whose goal is to deal with complex regions and smooth regions. The experimental results of the keypoint-based methods show that SIFT has good detection results in complex regions, so SIFT keypoints are used to detect the complex copied parts in complex regions. Although the SIFT keypoints cover the whole image, the amount of keypoints under investigation is dropped dramatically in smooth regions. As a result, it is necessary to find more keypoints for detection. To adjust the density of keypoints is another advantage of the proposed method. When enough key points are obtained, we can easily create features for detection in smooth regions.

3 The proposed scheme

In the proposed scheme, the flowchart of the proposed method is given in Fig. 1. In Fig. 1, a test image is first adaptively divided into non-overlapped region by using SLIC superpixel segmentation. For the obtained superpixel blocks, they can be classified into two categories according to the mean and standard deviation of the pixels and the ratio of the SIFT feature points in the superpixel block. The two types of regions can be defined as smooth regions and complex (i.e., non-smooth) regions. In complex regions, we use SIFT (Scale-invariant feature transform) features for feature matching and adopt RANSAC algorithm to filter out error matching. In smooth regions, we change the comparison threshold of the Harris to extract

more Harris feature points and then construct a feature with rotation invariance around each Harris feature point. We can construct the feature of a smooth region that contains sector mask feature and RGB color feature. Both sector mask feature and RGB color feature have rotation invariance, and then feature matching and error matching are performed. Finally, the final detection results can be achieved. The detail of the proposed detection scheme is illustrated in the following three subsections.

In order to better illustrate the implementation process of the proposed algorithm, the detailed implementation method of the algorithm is given in Algorithm 1.

Algorithm 1 The proposed copy-move forgery detection algorithm

Input: A suspicious image I

Output: A map that includes the detecting results.

A. Image Segmentation and K-means Cluster Analysis

Step1. Applying SLIC algorithm to segment the image I, dividing the image into N independent non-overlapping regions, denoted as B_i, where $1 \leqslant i \leqslant N$;

Step2. Extracting SIFT keypoints of the whole image;

Step3. For each B_i

Step4. Calculating the pixel mean value and standard deviation of superpixel block, and the ratio of the feature points in the superpixel block, denoted as M_{ej}, S_{dj}, R_{aj};

Step5. End For

Step6. Applying K-means clustering algorithm to divide the image I into complex and smooth regions;

B. Feature point extraction and feature matching in complex and smooth regions

Step7. In complex regions, extracting SIFT keypoints and getting the feature vector;

Step8. In smooth regions, extracting enough Harris keypoints by choosing the threshold as $t_{th}=10^{-5}$;

Step9. For each Harris point

Step10. Extracting the sector mask feature vector and RGB color feature vector;

Step11. End For

Step12. Calculating the Euclidean Distances of SIFT keypoints and Harris keypoints in complex regions and smooth regions respectively;

Step13. Applying g2NN algorithm to match keypoints in complex regions and smooth regions respectively;

C. Filtering outliers

Step14. Applying RANSAC algorithm to filter outliers and remove false alarms in complex regions and smooth regions respectively. If the matched keypoints are in the same segmentation block, remove the pair of keypoints;

Step15. Outputting the map that includes the detecting results.

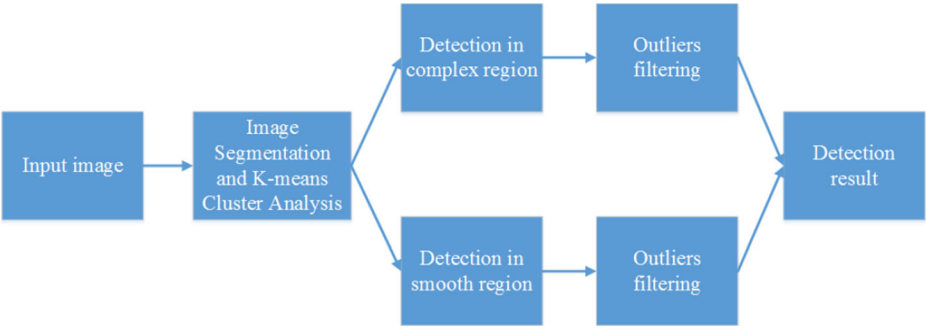


Fig. 1 Flowchart of the proposed method

3.1 Image segmentation and K-means cluster analysis

3.1.1 Image segmentation

In order to better deal with the source area and paste area of the image, the image is segmented with superpixel. The concept of a superpixel is an irregular pixel block consisting of adjacent pixels with similar textures, colors, and brightness, which greatly reduces the complexity of image post-processing. There are many segmentation methods in image segmentation algorithms, such as a segmentation method via fusing Normalized Cut (NCut) eigenvector maps [32], the simple linear iterative clustering (SLIC) algorithm [1]. Here we segment the test image into many independent non-overlapping regions by using the simple linear iterative clustering (SLIC) algorithm [1]. The superpixel generated by the algorithm are as compact and neat as the cells, and the neighborhood features are easy to express. It can not only divide color images, but also divide gray images. It is a kind of segmentation with high comprehensive evaluation on computing speed, target contour and image element shape.

In practice, different images have different texture features and sizes. The initial segmentation parameters of superpixel has a great influence on the segmentation results. Usually, when the texture of the image is relatively simple, the parameters of the superpixel segmentation can be set relatively small, so the size of the superpixel block is larger, which can reduce the time used by the algorithm to process the smooth region. On the contrary, when the texture of the image is rich, the initial segmentation parameters are set to a larger number. Dividing small pixels into superpixel helps to process images accurately. Through a lot of experiments, we set the initial parameter of superpixel segmentation in SLIC algorithm to 200, and the number of iterations can be set to 10. Figure 2 is an example of SLIC superpixel segmentation. In Fig. 2, the tree is a rich region of texture in the image. The tree on the left is copied and pasted on the right. After image segmentation, the copy area and paste area are divided into some non-overlapping superpixel segments fast, and these smaller superpixel can replace a large number of pixels to represent the image features and facilitate the subsequent image retrieval.

3.1.2 K-means cluster analysis

In the K-means clustering analysis of image, we can cluster according to image pixels or image key points. Keypoint clustering method can be applied to image recognition, model the background on video sequences [3], real-time moving object detection by PTZ cameras [4]

Fig. 2 Example of image SLIC superpixel segmentation: **a** The forgery image, **b** The result after SLIC superpixel segmentation

and so on. After the test image segmentation, SIFT feature points in the image are first extracted, and then the image is divided into complex region and smooth region by K-means clustering analysis. The K-means clustering is used for the clustering of segmentation regions. There are two kinds of clusters. The clustering rule is based on the mean value and standard deviation of image fragment pixels and the ratio of the feature points in the superpixel block. An example of the detected SIFT corner points is shown in Fig. 3. Figure 3 shows that many SIFT feature points are concentrated in the rich texture area of images, SIFT feature points account for the proportion of the total pixels of the superpixel block can reflect the degree of image texture change. The mean and standard deviation of superpixel can reflect the change of image pixels.

The mean and standard deviation of the image segments pixels and the ratio of the feature points can be labeled as Me_j,Sd_j,Ra_j, they are defined as:

$$Me_j = \frac{\sum_{i=1}^{n_j} x_i}{n}, i = 1, 2, \cdots, n_j, j = 1, 2, \cdots, N \tag{1}$$

Fig. 3 The detected SIFT corner points: **a** The test image, **b** The result of extracting Harris points

$$Sd_j = \sqrt{\left[\left(x_1 - Me_j\right)^2 + \left(x_2 - Me_j\right)^2 + \cdots + \left(x_i - Me_j\right)^2\right]/n} \tag{2}$$

$$Ra_j = \frac{SF_j}{PI_j} \tag{3}$$

where N is the number of the superpixel block, n is the number of pixels in the superpixel segmentation block, SF_j is the number of SIFT feature points in the image segments, PI_j is the total number of pixels in the image segments. Then the basis of cluster can be obtained, i.e. $X = (Me_j, Sd_j, Ra_j)$.

Due to the basis of cluster have different dimension, we should normalize them to use maximum and minimum normalization, X' is the result of normalization, the formula of maximum and minimum normalization is as follows:

$$X' = \frac{X - X_{MAX}}{X_{MAX} - X_{MIN}} \tag{4}$$

After normalization, K-means clustering is used to cluster the regions, the result of K-mean cluster is shown in Fig. 4d. Figure 4 is the contrastive results of different cluster. In Fig. 4b, c and d show that image segmentation blocks are divided into two categories, the black part represents complex region and the other part represents smooth region. As is shown in Figure (d), the proposed cluster result is more conformed to the contour and texture features of the image compare with the other two results, because the pixel cluster only considered the mean and standard deviation clustering of pixels at pixel level, the pixel cluster is not enough to distinguish some regions with the same standard deviation. The superpixel clustering method based on SIFT feature points only considered the degree of image texture change, some pixel level features were ignored. In our method, the proposed cluster method considers the changes of SIFT feature points and image pixels, the clustering rule is based on the mean and standard deviation of the image segments pixels, and the ratio of the feature points in the superpixel block. SIFT feature points account for the proportion of the total pixels of the superpixel block can reflect the degree of image texture change, and the mean and standard deviation of superpixel can reflect the change of image pixels, so the proposed cluster method has a better effect in distinguishing texture-rich regions and smooth regions.

3.2 Detection in complex region

In the process of image feature detection, there are many detection methods, such as SIFT feature detection, saliency detection based on integrated features [11], 2-D cartoon character detection based on scalable-shape context [33] and so on. In addition, a novel Skeleton Modulated Topological Visual Perception Map (SMTPM) integrated with visual attention and visual masking mechanism [24] can also be used for feature detection and image processing. Compared with smooth regions, complex regions are rich in texture, SIFT feature is used to detect possible tampering areas. For given the SIFT keypoints, the SIFT keypoints are denoted as $p = \{p_1, p_2, \ldots, p_n\}$, the similarity values between it and other keypoints are calculated and form a similarity vector, the similarity value is based on Euclidean distance. The Euclidean distances are sorted from small to large, they are denoted as $(s_1, s_2, \ldots, s_{n-1})$, where n is the number of keypoints, then the g2NN algorithm is used to find matching points. The

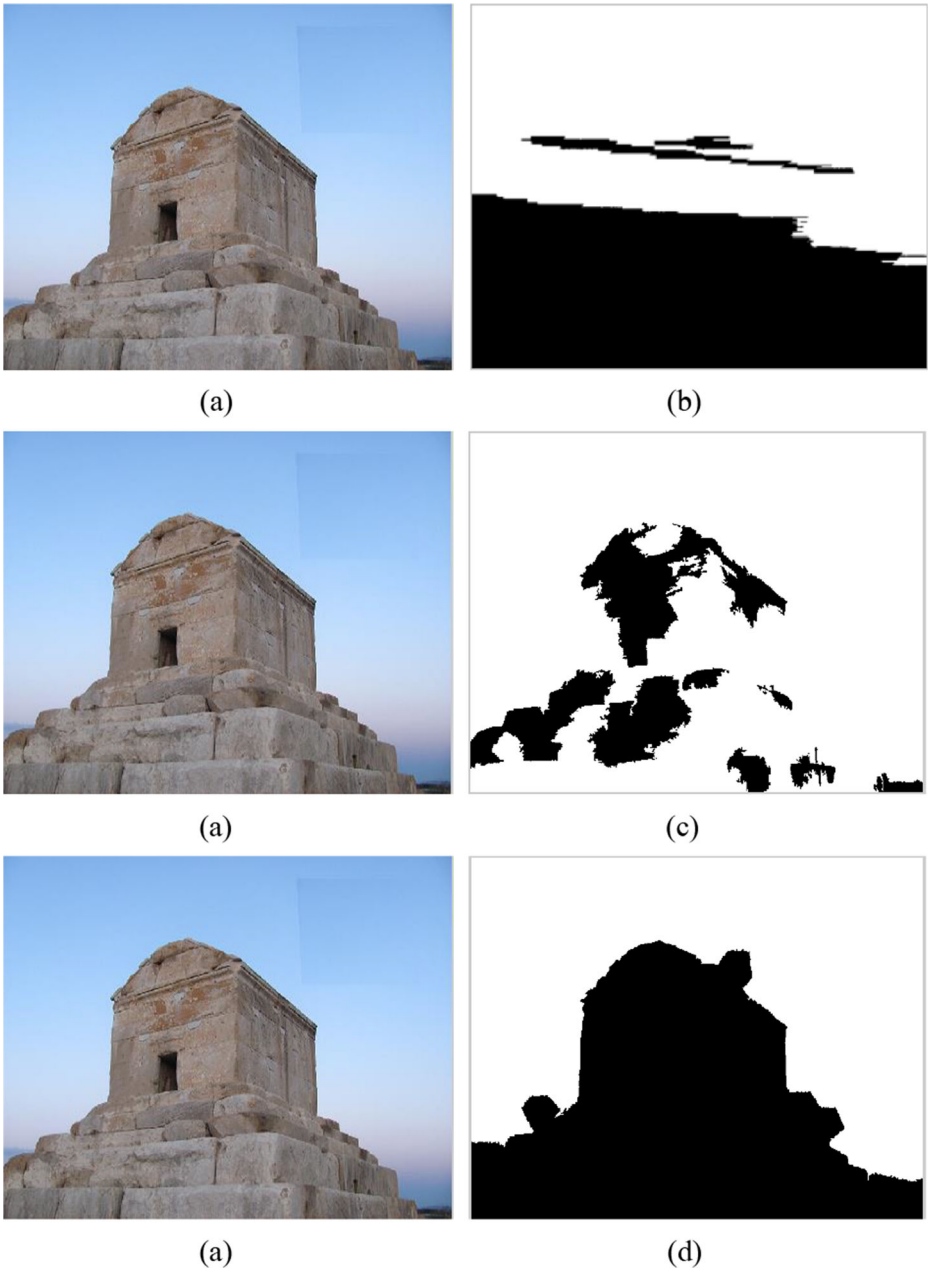


Fig. 4 The contrastive results of different cluster: **a** The test image. **b** The superpixel clustering result based on pixel mean and standard deviation. **c** The superpixel clustering result based on SIFT feature points. **d** The result of K-mean cluster in proposed method

formula (5) of the g2NN algorithm is shown in formula (5), T is the appropriate threshold (in this experiment, $T = 0.52$, $T \in (0,1)$). If the obtained Euclidean distance satisfies the in equation (5), we consider that the feature point $p_i$matches the feature point whose distance is (s_1, s_2, …,

s_k).To avoid matching from adjacent feature points, each two matched SIFT points should not be located in the same partition region.

$$\begin{cases} \frac{s_k}{s_{k+1}} < T \\ \frac{s_{k+1}}{s_{k+2}} > T \end{cases} \tag{5}$$

After feature matching is completed in complex region, we employ RANSAC algorithm to filter outliers and remove false alarms. Figure 5a and b illustrate the comparison of the matching keypoints before and after filtering, respectively.

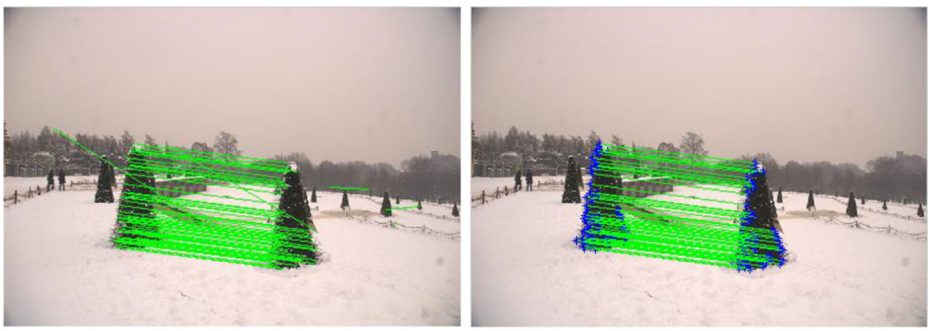
3.3 Detection in smooth region

In smooth regions, we use Harris corners as key-points to detect the possible tampered regions in smooth region. Harris corner detection is based on the second moment auto correlation matrix. The traditional Harris extraction method can extract more feature points in rich texture regions, and less feature points can be extracted in smooth regions. In order to make better tamper detection in the smooth region, we extract dense Harris feature points in these regions so that enough features can be extracted on the smooth region. In fact, sector mean and RGB color features are used to detect smooth regions. The detailed detection process is as follows:

Step1: Extracting dense Harris feature points.

After the detection of complex regions, the smooth region is detected. The feature points extracted here are Harris feature points, and the Harris operator has rotation invariance. It has been widely applied to the matching detection of various images. The key points obtained by the traditional Harris operator are mostly concentrated in the complex region and obtained in the smooth region. In order to get enough feature points in the smooth region, we use lower threshold of the extracted keypoints to extract dense feature points. The method can get enough Harris feature points in the smooth region, which facilitates the tamper detection in the smooth region.

The traditional Harris feature point is to calculate the response function of the corner point through the formula (6), in which k is an empirical constant, the range of the value of k is



(a) (b)

Fig. 5 Detection results before and after using RANSAC algorithm: **a** The matching key-points before using RANSAC algorithm, **b** The matching key-points after using RANSAC algorithm

[0.04,0.06], and the Harris angle obtained with different k values will have different effects.

$$R(x,y) = \det(M(x,y)) - k*tr^2(M(x,y)) \tag{6}$$

In order to avoid the value of k to choosing and reduce the randomness of k, here we choose the improved response function in Ref. [19]. The response function is used to detect corner points, and its corner response function formula is shown in formula (7).

$$R(x,y) = \det(M(x,y))/(trance(M(x,y)) + \varepsilon) \tag{7}$$

where $R(x,y)$ is the response value of the Harris corner, which ε is an arbitrarily small positive number. The Harris corner point larger than the specified threshold is recognized as the local maximum of the Harris measurement response, i.e.,

$$(x_c,y_c) = \{(x_c,y_c)|R(x_c,y_c) > R(x_i,y_i), \forall(x_i,y_i) \in W(x_c,y_c), R(x_c,y_c) > t_{th}\} \tag{8}$$

where (x_c,y_c) is the set of all corner points, $R(x,y)$ is the Harris measure response calculated at point (x,y), $W(x_c,y_c)$ is setting centered around the point (x_c,y_c), and t_{th} is a specified threshold. Obviously, the number of detected Harris corner points depends on the comparison threshold t_{th}.

By changing the threshold of the Harris extraction value, we can get a different number of Harris key points. Figure 6 is the detection results of Harris corner points under different

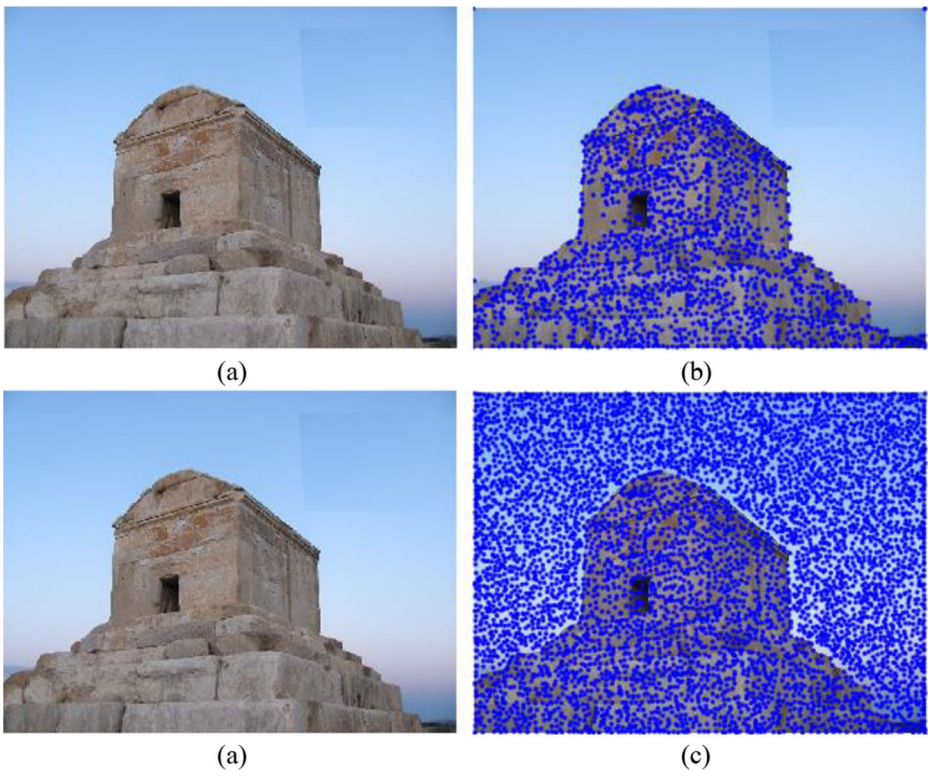


Fig. 6 The detection results of Harris corner points under different comparison threshold: **a** The test image. **b** The detection result of Harris corner with the threshold $t_{th} = 10^{-2}$ **c** The detection result of Harris corner with the threshold $t_{th} = 10^{-5}$

comparison thresholds. When the threshold is large, many key points are extracted in the texture rich area, and few feature points are extracted in the smooth area. As shown in Fig. 6b, when the threshold is small, many dense and uniform feature points can be extracted in the smooth region. In order to better reflect the change of the number of Harris key points with the threshold value t_{th}, Fig. 7 is the average of the number of Harris points which are extracted from all images in the image dataset SBU-CM16 [30] under different comparison thresholds. As the threshold value decreases, more Harris corner points can be extracted. When the threshold value decreases to a certain value ($t_{th} = 10^{-5}$), the number of corner points no longer increases, and the growth rate of keypoints is 0. Therefore, $t_{th} = 10^{-5}$ is an appropriate threshold to extract sufficient keypoints in smooth regions.

Step2: Feature description and the construction of feature vector.

The small circle area around Harris corner is described by the image region description method based on sector statistics. For each Harris point, it will be represented by a small circle area [17]. The Harris corner point is used as the center of the circle, then the sector is derived from the circle of Harris corner points, the created sector mask is shown in Fig. 8. After the circle is divided into 36 equal parts, 36 sectors are obtained and labeled as $S_1, S_2, \ldots, S_{36}$. The angle of the sector is 10°, and the radius is 16, these parameters are determined through lots of experiments.

After getting the created sector masks, the sector masks $S_k (k = 1,2,\ldots,36)$ are used to constitute the sector mask feature by computing the mean of the pixels within each sector mask S_k, e.g., $M_{S_1} = mean(S_1)$. Finally, a vector of 36 dimensions can be obtained, i.e.$(M_{S_1}, M_{S2}, \cdots, M_{S_{36}})$.

No matter how many degrees the circle image region has been rotated, the sectors have the same location relationship in the circle image region, so the sector with the largest mean can be set as the first direction mark of the circle image region, then the remaining sectors are rearranged in a preset direction [17]. Thus, the sector mask is arranged according to the content of the circle image region, which is barely affected by rotation. In this way, the image region description method based on sector mask features can be rotation-robust. In order to better detect the smooth region, here we calculate the mean and standard deviation of the new sector in R, G, B three channel between the maximum sector mean and the minimum sector mean. The new sector is shown as shown in Fig. 9.

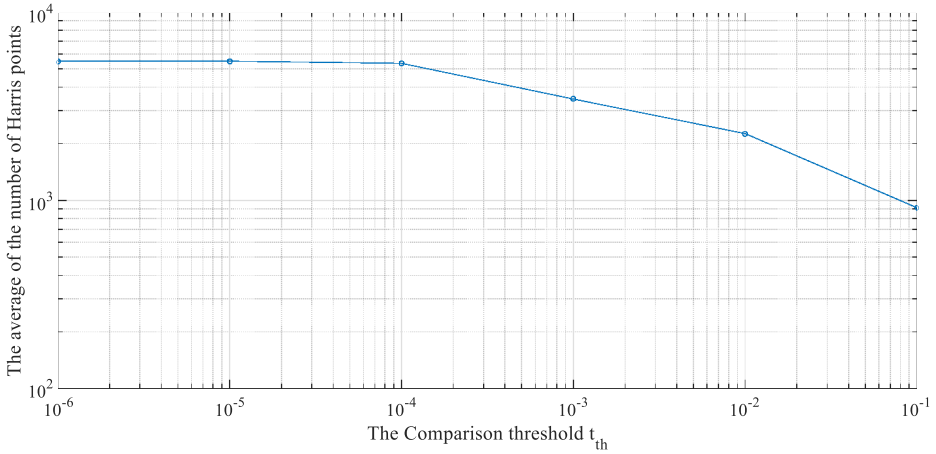


Fig. 7 The contrastive results of Harris detection under different response functions

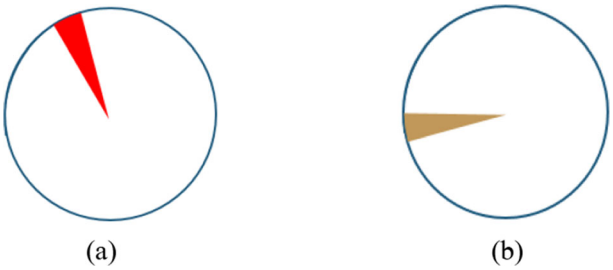


Fig. 8 The sector masks: **a** The sector mask in direction of 110°, **b** The sector mask in direction of 190°

In Fig. 9a, the red area and the brown area are the largest and the smallest regions respectively, the blue area is a new large sector area as shown in Fig. 9b. Then we get the mean and standard deviation of the new sector in R, G, B three channel, they can be labeled asM_R, M_G, M_B, S_R, S_G, S_B, If the element with the largest mean in the aforementioned 36 dimensional feature vector is M_{S_i}, a vector of 42 dimensions is obtained, the elements in the vector can be rearranged as

$$\left(M_{S_i}, M_{S_{i+1}}, \cdots, M_{S_{36}}, M_{S_1}, M_{S_2}, \cdots, M_{S_{i-1}}, M_R, M_G, M_B, S_R, S_G, S_B\right)$$

Step3: Matching features and removing error matching.

After the Harris corner points are obtained, the small circle region around each Harris point is represented with a feature vector using the image region description method based on sector statistics described [17]. We set the Harris corner points as $P = \{P_1, P_2, \ldots, P_n\}$, the corresponding vector is labeled as $X = \{x_1, x_2, \ldots, x_n\}$. Then, the detected Harris points can be matched based on their representation feature vectors using the g2NN algorithm [2].

We can get the matching points by using g2NN algorithm in complex region and smooth region respectively. We calculate the Euclidean distances between $x_i (i = 1, 2, \ldots, n)$ and the others. Then we sort the resulting distances in ascending order and label them as $D = \{d_1, d_2, \ldots, d_{n-1}\}$. If the resulting distances can satisfy the formula:

$$\begin{cases} \dfrac{d_k}{d_{k+1}} < T \\ \dfrac{d_{k+1}}{d_{k+2}} > T \end{cases} \tag{9}$$

Fig. 9 The new sector masks: **a** Two sectors of the maximum mean and the minimum mean, **b** The new sector between the maximum mean sector and the minimum mean sector

where T is the appropriate threshold (in default, $T = 0.5$), we think that the Harris point x_i matches with these points that the corresponding distance is $\{d_1, d_2, \ldots, d_k\}$. In order to avoid searching the nearest neighbors of a Harris point from its adjacent region, the distance between two matched Harris points should be larger than a certain distance such as $2R$ (R is the radius of the sector region). In the meanwhile, every two matched Harris points should not be in the same segmented block.

All matching Harris points are shown as circles with a radius of 16 and connected to them with a line. Therefore, the duplicate areas can be displayed through these circles and relational lines. However, the number of matched pairs will vary between different images. When two or more matching pairs exist to cluster to show a certain kind of affine transformation, the region they cover can be considered as the duplicate areas [17]. An error match can occur when there are only a pair of matching pairs or several matching pairs but are distributed randomly, Since these dense Harris points are almost uniformly distributed in the image, there is a high probability that nearby Harris points will be matched when there is only a pair of matching pairs or several matching pairs but are distributed randomly, so the scattered matching pairs may be the wrong matching pairs. In order to further remove mismatches, we use RANSAC algorithm [7] to filter outliers and remove false match points.

4 Experimental results

In this section, we present the detection results of the proposed scheme, the proposed scheme are carried out on the platform with Intel Core 2.40 GHZ and MATLAB 2014b. All the test images used in the experiment were in the dataset named SBU-CM16 [30] which contains 16 original images and 240 forged images, each tampered image in this dataset has one forged part. Tampered images created by coping one part and pasting it on another part in the same image, and then different attack is performed on the copied region or on the whole image. In this dataset, tampering occurs not only in the textured region but also in the smooth region, it will be beneficial to the algorithm performance of a more comprehensive detection.

This image databases contains a considerable amount of images which smooth areas has been tampered. Table 1 shows the attack parameters for the image databases SBU-CM16 [30].

4.1 Evaluation metrics

To evaluate the performance of our scheme, we employ recall, precision and F1 measurements as metrics which are often used in the field of image copy-move forgery detection, they are defined as:

$$\mathrm{Re}call = \frac{T_P}{T_P + F_N} \tag{10}$$

Table 1 Setting of the attacks

Attack	Parameters
Blurring	Filter radius: 0.5, 1.5, 2.5
Noise	Zero mean, Variance: 0.001, 0.002, 0.003
JPEG compression	Quality: 70, 80, 90, 100
Rotation	Angle: 10, 30, 50, 70, 90

$$\text{Precision} = \frac{T_P}{T_P + F_P} \tag{11}$$

$$F1 = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{12}$$

where T_P is the number of correctly detected forged images, F_N is the number of forged images that have been falsely missed, F_P is the number of original images that have been erroneously detected as the forged, they are as the following:

$$T_P = \frac{\text{No.of forged images detected as forged}}{\text{No.of forged images}} \tag{13}$$

$$F_P = \frac{\text{No.of original images detected as forged}}{\text{No.of original images}} \tag{14}$$

$$F_N = \frac{\text{No.of forged images has been falsely missed}}{\text{No.of original images}} \tag{15}$$

As seen, Recall denotes the probability that a forged image is detected, while Precision indicates the probability that a detected forgery is truly a forgery, *F1* is a trade-off between Precision and Recall, in general a higher *F1* indicates the algorithm has superior performance. The higher the T_P and the lower the F_P, the better the detection performance.

4.2 Selection of the number of initial segmentation blocks

The number of initial superpixel image segments will have some influence on the algorithm, it will lead to a different clustering result as shown in Fig. 10. In Fig. 10, the result of the number of initial image segments is 200 has better result of K-means cluster compared with the other two results, and it is more consistent with the texture and contour features of the image.

Table 2 is the different detection results of the proposed method under different number of image segments. As shown in Table 2, we can see that the proposed scheme has a higher True Positive Rate and a lower False Positive Rate when the number of initial image segments is 200, the parameter N_0 is the initial number. In the proposed method, the number of initial image segments which we choose is 200.

4.3 Robustness

The purpose of robustness tests is to investigate the performance of the proposed method with blurring, adding noises, JPEG compression and Rotation, respectively. Each tampered image contains one irregular and meaningful duplicated regions.

In the experiment of our method, Figs. 11, 12, 13 and 14 is the detection results of the copied region in the texture-rich region, and Figs. 15, 16, 17 and 18 is the detection results of the copied region in the smooth region. In these experimental diagrams, green is the label of correctly detected regions and white color specifies the duplicated portions. As shown in Figs. 11, 12, 13, 14, 15, 16, 17 and 18, the proposed method can detect tampering in complex

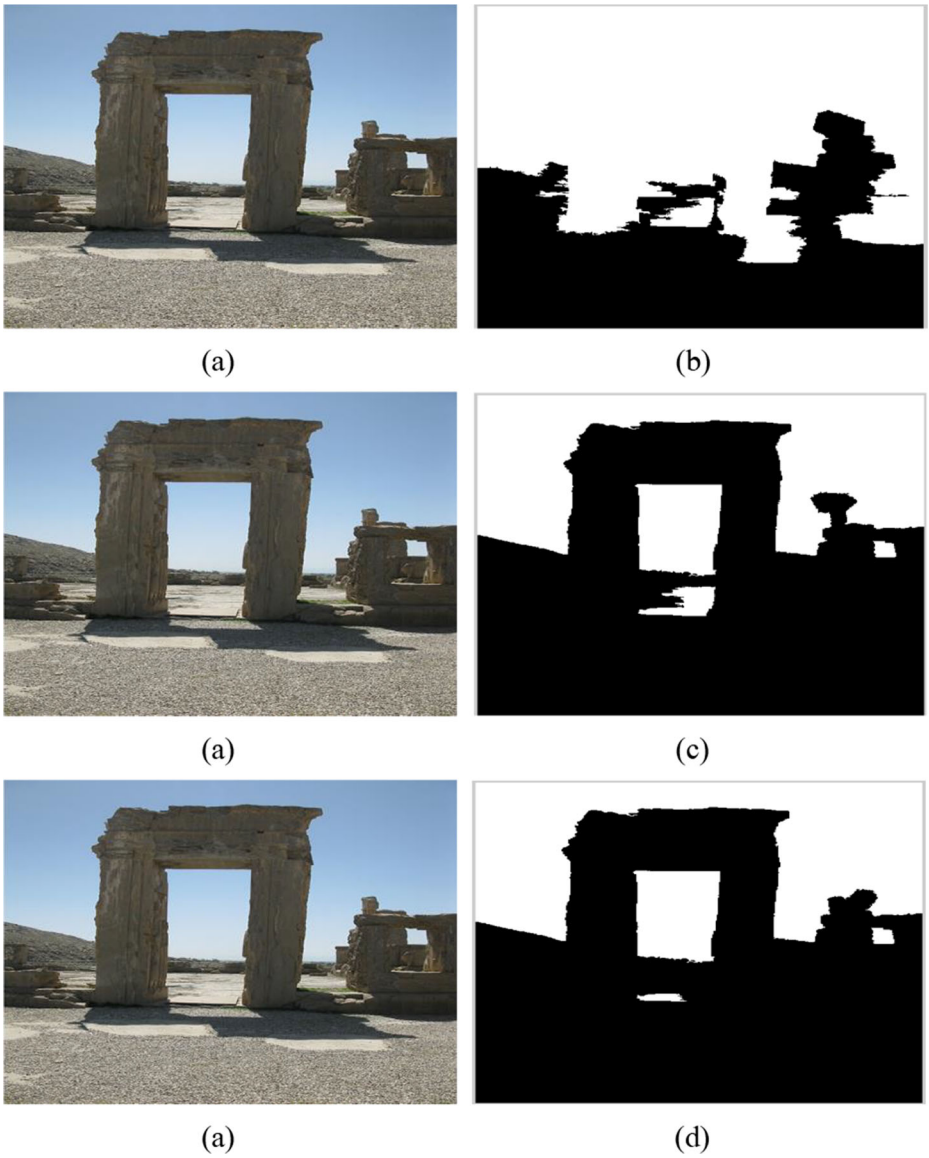


Fig. 10 The clustering results of the proposed method under different number of image segments. **a** The test image, **b**, **c**, **d** The result of K-mean cluster when the number of initial superpixel block is 180,200,210 respectively

Table 2 The result of the proposed method under different number of image segments

N_0	180	200	210
T_P	85.83%	87.08%	86.25%
F_P	18.75%	12.50%	12.50%

Fig. 11 The detection results after the attack of blurring (Filter radius:0.5)

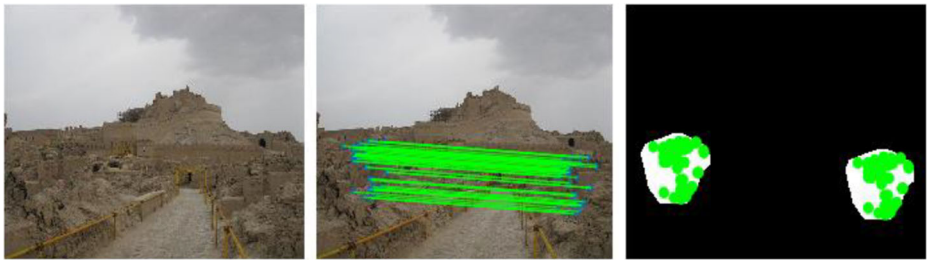


Fig. 12 The detection results after the attack of adding noise (Variance = 0.001)

and smooth regions, it also robust for the manipulation such as blurring, adding noise, JPEG compression, and rotation. SIFT feature have a good detection result for texture rich regions in complex regions, and the feature of sector configuration can also detect smooth regions. Few SIFT keypoints are extracted in smooth regions, so it is difficult to detect smooth areas. When detecting the tampering of smooth regions, sufficient keypoints can help us to find suspicious areas, evenly dense keypoints can be conducive to the detection of smooth regions, the sector mask feature and RGB color feature have rotation invariance, and RGB color feature also has further increased the degree of discrimination.

4.4 Performances comparison

The robustness of the proposed scheme is evaluated for various post-processing operations such as blur, adding noise, JPEG compression and rotation. In order to make a more comprehensive comparison, we evaluated the robustness of this method by using the SBU-CM16 image database and compared it with the algorithms in Ref. [5, 15, 27].

Fig. 13 The detection results after the attack of JPEG compression (Quality factor = 80)

Fig. 14 The detection results after the attack of rotation (Rotation angle = 50)

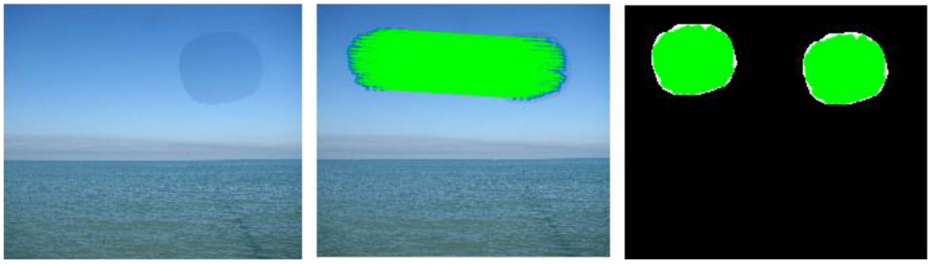


Fig. 15 The detection results after the attack of blurring (Filter radius = 0.5)

Figure 19 exhibits the correct detection rate of different tamper attack in contrastive experiment result on the SBU-CM16 dataset. The proposed method is more noticeable in this experiment, and it has a higher true positive rate when it compared with the algorithm of Ref. [5, 15, 27]. Since the SBU-CM16 dataset contains a considerable amount of smooth area, SIFT features or Harris features cannot have a good detection effect on smooth region, at the same time matching of smooth region have a great number of falsely matched pairs. In Ref. [5], there are few feature points extracted in the smooth region, and the detection effect on the smooth region is poor. In Ref. [15], it first segments the test image into semantically independent patches, SIFT keypoints were matched between patches and Expectation Maximization algorithm (EM) was used to filter false alarm patches, most of the extracted SIFT feature points are concentrated in texture-rich areas or complex regions, SIFT features have a good detection result for texture rich regions in complex regions. In smooth regions, the suspicious regions can be investigated more precisely by selecting more keypoints, but few SIFT feature points can be extracted in the smooth region. In Ref. [27], DCT coefficient is used as the feature vector, which is unable to resist rotation attack. Our method takes account of complex

Fig. 16 The detection results after the attack of adding noise (Variance = 0.001)

Fig. 17 The detection results after the attack of JPEG compression (Quality factor = 80)

regions and smooth regions, SIFT features are used to detect complex regions, evenly dense Harris keypoints are used to avoid the problem of extracting few feature points in smooth regions, sector mean and RGB color features are used to detect smooth regions. Note that RGB color feature has further increased the detection degree of discrimination in smooth regions.

We also use true positive rate and false positive rate to compare our proposed method with the algorithm of Ref. [5, 15, 27]. The detection result is given in Table 3. As shown in Table 3, the proposed method has a higher correct detection rate and a lower False Positive Rate when compared with the Ref. [5, 15, 27].

5 Conclusion

This paper presents a passive forensics scheme for copy-move forgery based on superpixel segmentation and K-means Clustering. The proposed scheme adopts the SLIC superpixel segmentation and K-means clustering divide the image into complex region and smooth region. The clustering rule is based on the mean and standard deviation of the pixels, and the ratio of the feature points in the superpixel block, this clustering method accords with the contour and texture features of the image, and it has a good effect on dividing the image into rich texture regions and smooth regions. In complex regions, we use SIFT features for feature matching. In order to improve the effect of smooth region detection, we consider the pixel characteristics of the RGB three channel in the smooth region, we use dense Harris point and sector mask feature to match. The experimental results show that the proposed scheme has an advantage in the detection accuracy compared with some related works, and is able to overcome the problem of lack of key-points by using the extraction of dense Harris feature points. In

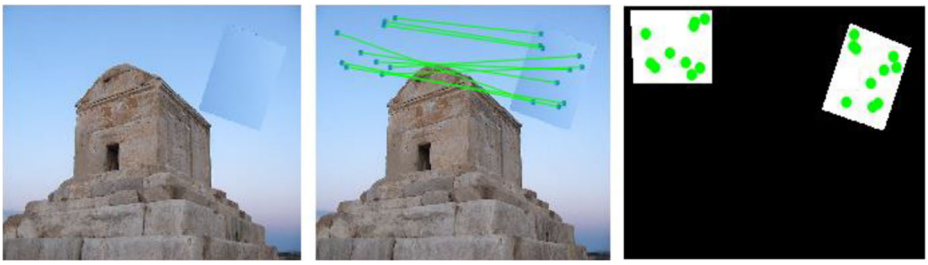


Fig. 18 The detection results after the attack of rotation (Rotation angle =70)

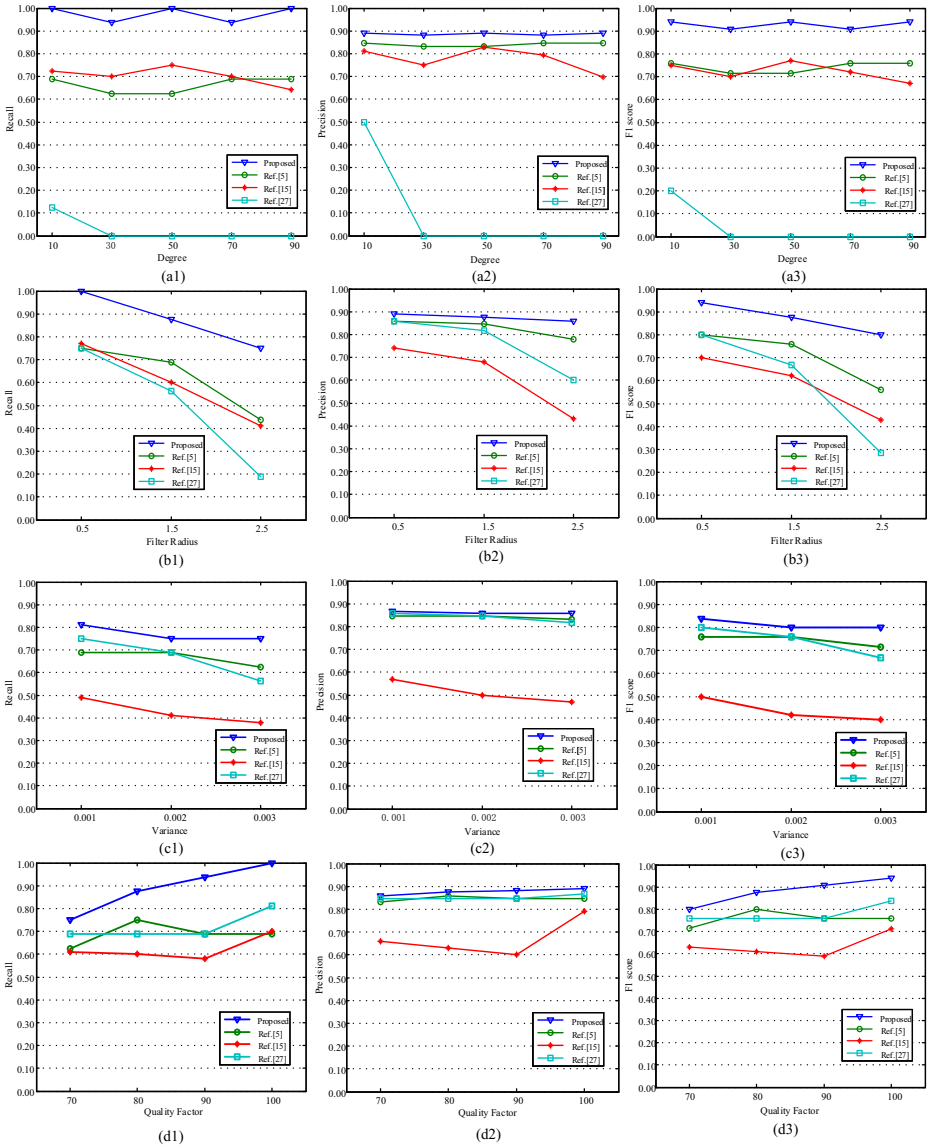


Fig. 19 The contrastive experimental results on SBU-CM16 dataset. (a1) Rotation, Recall. (a2) Rotation, Precision. (a3) Rotation, F1 score. (b1) Blur, Recall. (b2) Blur, Precision. (b3) Blur, F1 score. (c1) Noise, Recall. (c2) Noise, Precision. (c3) Noise, F1 score. (d1) JPEG compression, Recall. (d2) JPEG compression, Precision. (d3) JPEG compression, F1 score

Table 3 Detection results of comparison experiment

Measures	Chen et al. [5]	Li et al. [15]	Wang et al. [27]	Proposed
T_P	69.58%	60.42%	44.17%	89.16%
F_P	18.75%	18.75%	12.50%	12.50%

the future, we will select the appropriate parameters to improve accuracy, and some new technologies will be considered, such as image fusion, color segmentation [29] and deep learning, etc.

Acknowledgments This work was supported by the Fundamental Research Funds for the Central Universities under the grant No. YJ201881 and Doctoral Innovation Fund Program of Southwest Jiaotong University.

References

1. Achanta R, Shaji A, Smith K, Lucchi A, Fua P, Susstrunk S (2012) SLIC superpixels compared to state-of-the-art superpixel methods. IEEE Trans Pattern Anal Mach Intell 34(11):2274–2281
2. Amerini I, Ballan L, Caldelli R, Bimbo AD, Serra G (2011) A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Transactions on Information Forensics and Security 6(3):1099–1110
3. Avola D, Bernardi M, Cinque L, Foresti GL, Massaroni C (2017) Adaptive bootstrapping management by keypoint clustering for background initialization. Pattern Recogn Lett 100:110–116
4. Avola D, Bernardi M, Cinque L, Foresti GL, Massaroni C (2018) Combining keypoint clustering and neural background subtraction for real-time moving object detection by PTZ cameras. In: Proceedings of international conference on pattern recognition applications and methods, pp 638–645
5. Chen L, Lu W, Ni J, Sun W, Huang J (2013) Region duplication detection based on Harris corner points and step sector statistics. J Vis Commun Image Represent 24(3):244–254
6. Christlein V, Riess C, Jordan J, Riess C, Angelopoulou E (2012) An evaluation of popular copy-move forgery detection approaches. IEEE Transactions on Information Forensics and Security 7(6):1841–1854
7. Fischler MA, Bolles RC (1981) Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. Commun ACM 24(6):381–395
8. Fridrich J, Soukalm D, Lukas J (2003) Detection of copy-move forgery in digital images. In: Proceedings of digital forensic research workshop, Cleveland, pp 19–23
9. Hamdi D, Iqbal F, Baker T, Shah B (2016) Multimedia file signature analysis for smartphone forensics. In: IEEE international conference international conference on developments in Esystems engineering, pp 130–137
10. Huang H, Guo W, Zhang Y (2009) Detection of copy-move forgery in digital images using SIFT algorithm. In: The workshop on computational intelligence and industrial application, vol 2, pp 272–276
11. Jing H, He X, Han Q, Abd El-Latif AA, Niu X (2014) Saliency detection based on integrated features. Neurocomputing 129:114–121
12. Kang L, Cheng XP, Li K (2010) Copy-move forgery detection in digital image. In: Image and signal processing (CISP), vol 5, pp 2419–2421
13. Kumar S, Desai JV, Mukherjee S (2016) A fast Keypoint based hybrid method for copy move forgery detection. Ijcds Journal 4(2):91–99
14. Li G, Wu Q, Tu D, Sun S (2007) 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
15. Li J, Li X, Yang B, Sun X (2015) Segmentation-based image copy-move forgery detection scheme. IEEE Transactions on Information Forensics and Security 10(3):507–518
16. Lian S, Kanellopoulos D (2009) Recent advances in multimedia information system security. Informatica 33:3–24
17. Liu Y, Wang HX, Wu HZ, Chen Y (2017) An efficient copy-move detection algorithm based on Superpixel segmentation and Harris key-points. In: International conference on cloud computing and security, pp 61–73
18. Macdermott A, Baker T, Shi Q, Shah B (2018) Iot forensics: challenges for the Ioa era. In: IFIP international conference on new technologies, mobility and security, pp 1–5
19. Mao YM, Lan MH, Wang YQ, Feng QS (2009) An improved corner detection method based on Harris. Computer technology and development 19(5):130–133
20. Popescu AC, Farid H (2004) Exposing digital forgeries by detecting duplicated image regions. In: Comput.sci.dartmouth College Private Ivy League Res.univ, p 646
21. Prakash CS, Kumar A, Maheshkar S, Maheshkar V (2018) An integrated method of copy-move and splicing for image forgery detection. Multimed Tools Appl 77(20):26939–26963
22. Ryu S, Lee M, Lee H (2010) Detection of copy-rotate-move forgery using Zernike moments. Lect Notes Comput Sci 6387:51–65

23. Sharif SA, Ali MA, Reqabi NA, Iqbal F, Baker T (2016) Magec: an image searching tool for detecting forged images in forensic investigation. In: IFIP international conference on new technologies, mobility and security, pp 1–6
24. Shi Z, Yu L, Abd El-Latif AA, Niu X (2012) Skeleton modulated topological perception map for rapid viewpoint selection. IEICE Trans Inf Syst E95D(10):2585–2588
25. Tong X, Liu Y, Zhang M, Chen Y (2013) A novel chaos-based fragile watermarking for image tampering detection and self-recovery. Signal Process Image Commun 28:301–308
26. Wang JW, Liu GJ, Zhang Z, Dai YW, Wang ZQ (2009) Fast and robust forensics for image region-duplication forgery. Acta Automat Sin 35(12):1488–1495
27. Wang X, He G, Tang C, Han Y, Wang S (2016) Keypoints-based image passive forensics method for copy-move attacks. Int J Pattern Recognit Artif Intell 30(3):304–308
28. Wang H, Wang H, Sun X, Qian Q (2017) A passive authentication scheme for copy-move forgery based on package clustering algorithm. Multimed Tools Appl 76(10):12627–12644
29. Wu HZ, Shi YQ, Wang HX, Zhou LN (2017) Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification. IEEE Transactions on Circuits and Systems for Video Technology 27(8):1620–1631
30. Zandi M, Mahmoudi-Aznaveh A, Mansouri A (2014) Adaptive matching for copy-move forgery detection. In: The workshop on information forensics and security, pp 119–124
31. Zandi M, Mahmoudi-Aznaveh A, Talebpour A (2016) Iterative copy-move forgery detection based on a new interest point detector. IEEE Transactions on Information Forensics and Security 11(11):2499–2512
32. Zhang T, Abd El-Latif AA, Wang N, Li Q, Niu X (2012) A new image segmentation method via fusing NCut eigenvectors maps. In: International conference on digital image processing, vol 8334
33. Zhang T, Han Q, Abd El-Latif AA, Bai X, Niu X (2013) 2-D cartoon character detection based on scalable-shape context and Hough voting. Inf Technol J 12(12):2342–2349
34. Zhou L, Wang D, Guo Y, Zhang J (2007) Blur detection of digital forgery using mathematical morphology. In: Proceedings of the 1st KES International symposium on agent and multi-agent systems. Technologies and applications. Springer-verlag, Wroclaw
35. Zhou Z, Wang Y, Wu QMJ, Yang CN, Sun X (2017) Effective and efficient global context verification for image copy detection. IEEE Transactions on Information Forensics and Security 12(1):48–63

Yong Liu received the B.S degree from Hubei University of Automotive Technology, Shiyan, China, in 2015.He received his M. S. degree from School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China, in 2018. He is currently pursuing the Ph.D. degree with School of Communication and Information Engineering, Shanghai University, Shanghai,China.His research interests include multimedia forensics and image processing.

Hongxia Wang received the B.S. degree from Hebei Normal University, Shijiazhuang, in 1996, and the M.S. and Ph.D. degrees from University of Electronic Science and Technology of China, Chengdu, in 1999 and 2002, respectively. She pursued postdoctoral research work in Shanghai Jiao Tong University from 2002 to 2004. Since September 2013, she has been a visiting scholar at Computer Science Department of Northern Kentucky University in USA. Currently, she is a professor with College of Cybersecurity, Sichuan University, Chengdu. Her research interests include multimedia information security, digital forensics, information hiding and digital watermarking. She has published 100 peer research papers and wined 10 authorized patents.

Yi Chen received the B.S. degree from Southwest Jiaotong University (SWJTU) in 2015. He is currently pursuing the Ph.D. degree with School of Information Science and Technology of SWJTU. His research interests include data embedding, steganography, steganalysis, digital forensics and machine learning.

Hanzhou Wu received his B.S. and Ph.D. from Southwest Jiaotong University, Chengdu, China, in June 2011 and June 2017. From October 2014 to October 2016, he was a visitor in New Jersey Institute of Technology, New Jersey, United States. He was a researcher in Institute of Automation, Chinese Academy of Sciences from July 2017 to March 2019. Starting from April 2019, he is an Assistant Professor in Shanghai University, Shanghai, China. His research interests include information hiding, graph theory, and game theory. He has published around 20 papers in peer journals and conferences, such as IEEE TDSC, IEEE TCSVT, IEEE SPL, IEEE WIFS, ACM IH&MMSec, and IS&T Electronic Imaging– MWSF. He also serves a reviewer for more than 10 peer journals such as IEEE TIFS, IEEE TCSVT, IEEE IoT Journal, and IEEE Communications Letters. He once received 2 Silver Medals and 1 Bronze Medal as a student contestant in ACM International Collegiate Programming Contest (Asia Regional) and Invitational Contest. He was selected to participate in Yahoo! Hack Beijing 2013 onsite contest based on his technical merit.

Huan Wang received the B. S. and the M. S. degree from Xihua University, Chengdu, China, in 2009 and 2013, respectively. She received the Ph.D. degree from School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China, in 2018. Her current research interest focuses on digital image forensics.

Affiliations

Yong Liu[1] · Hongxia Wang[2] · Yi Chen[3] · Hanzhou Wu[1] · Huan Wang[4]

Hongxia Wang
hxwang@scu.edu.cn

Yi Chen
yichen.research@gmail.com

Hanzhou Wu
wuhanzhou_2007@126.com

Huan Wang
ideahuan@163.com

[1] School of Communication and Information Engineering, Shanghai University, Shanghai 200444, China

[2] College of Cybersecurity, Sichuan University, Chengdu 610065, China

[3] School of Information Science and Technology, Southwest Jiaotong University, Chengdu 611756, People's Republic of China

[4] Guizhou University of Finance and Economics, Guiyang, Guizhou 550025, People's Republic of China