Ye et al. J Wireless Com Network (2022) 2022:30
https://doi.org/10.1186/s13638-022-02112-8

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

A two-stage detection method of copy-move forgery based on parallel feature fusion

Wujian Ye[1], Qingyuan Zeng[1], Yihang Peng[1], Yijun Liu[1*] and Chin-Chen Chang[2]

*Correspondence: 371785144@qq.com; yjliu2002@163.com
[1] School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, Guangdong, China
Full list of author information is available at the end of the article

Abstract

The copy-move forgery refers to the copying and pasting of a region of the original image into the target region of the same image, which represents a typical tampering method with the characteristics of easy tampering and high-quality tampering. The existing single feature-based methods of forgery detection have certain shortcomings, such as high false alarm rate, low robustness, and low detection accuracy. To address these shortcomings, this paper proposes an improved two-stage detection method based on parallel feature fusion and an adaptive threshold generation algorithm. Firstly, the SLIC super-pixels segmentation algorithm is used for image preprocessing, and a similar region extraction algorithm without threshold is employed to obtain the suspected tampering regions with high similarity. Secondly, the parallel fusion feature is obtained based on the SIFT and HU features to express the characteristics of local regions. Then, the corresponding threshold value is generated based on the histogram of oriented gradient (HOG) to describe the texture characteristics of the obtained regions, which acts as a criterion to judge whether a region has been forged or not. The experimental results show that the proposed method outperforms the existing methods, achieving the accuracy of 99.01% and 98.5% on the MICC-F220 and MICC-F2000 datasets respectively. In addition, the proposed method has stronger robustness performance on COMOFOD dataset than the comparison methods.

Keywords: Copy-move forgery, Two-stage forgery detection, Super-pixel segmentation, Parallel feature fusion, Adaptive threshold

1 Introduction

As an effective carrier of common information in the information age, a digital image has been widely used in many fields, including scientific research, media, and judicial expertise. The popularity of image editing software has reduced the cost of image content modifying but has led to the dissemination of a large number of tampering images containing false information on the Internet. In general, copy-paste modifies the local information of an image's region through the covering operation, and its specific operation is to select a region in the original image to copy and paste it into another local

regions in the same image, which represents a typical tampering method. The tamper region is homologous to the original region in the image, and thus difficult to be detected [1].

The existing forgery detection methods [2] mainly use the similarity between tampering regions as a detection criterion, and the detection process includes four steps, namely, preprocessing, feature extraction, feature matching, and post-processing, among which, feature extraction and feature matching play a key role. Since the existing methods use a fixed threshold in the detection process, their generalization ability is not strong enough. In addition, most of them rely on a single feature easily disturbed by the natural high-similarity region, which leads to the high false alarm rate. Aiming at mentioned problems, it is of high significance to improve the performance of the forgery detection methods by increasing their feature expression ability and realizing adaptive threshold automation with feature fusion.

In this paper, an improved two-stage [3] detection method of copy-move forgery based on parallel feature fusion is proposed. Firstly, the SILC super-pixel segmentation algorithm is applied to preprocess an image, and then a local region extraction algorithm without threshold is used to obtain a suspected tampering local region with high similarity. To improve the feature expression ability, a new parallel feature combining the SIFT feature and Hu moment feature is used to describe the extracted local regions with high similarity. Finally, the thresholds are generated adaptively according to the histogram of oriented gradient (HOG) features of the suspected tampering regions, which are then used to determine the attributes of local regions and to improve the generalization of the proposed method. The experimental results show that the proposed method can achieve high accuracy of 99.01% and 98.5% on the MICC-F2000 and MICC-F220 datasets respectively, and also shows strong robustness on the COMOFOD dataset.

The rest of this paper is organized as follows. Section 2 describes the current related works of copy-paste forgery detection technology. Section 3 introduces an improved two-stage forgery detection method based on parallel feature fusion. Section 4 presents the verification and analysis results of the proposed scheme from various aspects. Finally, Sect. 5 concludes the paper and gives future work directions.

2 Related works

The existing forgery detection methods are carried out based on the similarity between copy region and paste region, which can be roughly divided into three categories of image partition-based, feature point-based and deep learning-based methods [4].

The image partition-based methods are to segment and sample an image to obtain a local region first, then extract the features of the local region for matching, and finally to obtain the similar local region for identification. The commonly used features include the Discrete Cosine Transform (DCT) coefficients [5–7], RGB fusion information [8], Discrete Wavelet Transformation (DWT) [9], Zernike Moment [10, 11], Analytical Fourier-Mellin Transform (AFMT) [12], Hu invariant moment, Polar Cosine Transform (PCT) [13], PCET-SVD [14], CMF-iteMS [15], and Stabilized Wavelet Transform (SWT) [16]. The listed features mainly acquire the descriptor of an image's local region in the color domain or transform domain. Although these features have many advantages, they also have certain shortcomings. For instance,

the DCT and RGB features have low computational complexity, but their robustness is not strong. The Hu feature is composed of seven invariant moments, which can describe the object shape well, achieving certain robustness and low computational complexity. Zernike Monment, PCT and AFMT need to map an image to a higher order, which has higher computational complexity but achieves slightly stronger robustness than the RGB and other features.

The feature points-based methods extract the key points in the high entropy region of an image and construct the descriptor to complete the region matching. Their commonly used features include the SIFT [17–21], SURF [22, 23], ASIFT [24], ORB [25] and LBP [26]. The feature points are distributed where the gray level of an image changes dramatically, and their robustness mainly depends on the formation of a feature descriptor. Among the mentioned features, the SIFT detects key points in the scale space, and forms feature descriptors by using the main direction mechanism, which provides strong robustness and effective resistance to attacks, such as illumination, rotation and scale change. For example, Tahaoglu et al. [27] proposed a new forgery detection and localization method, which does not rely on forgery region features, but obtains SIFT key points based on RGB and LAB color space. However, its eigenvector has 128 dimensions and is of high complexity.

The deep-learning-based methods do not require manually extract features but learn the internal characteristics of a forged image through the training mechanism to complete the forgery detection. Wu et al. [28] designed a deep matching and validation modelbased on a simple convolutional neural network (CNN) for recognition. And they further presented an end-to-end detection model based on a two-branch structure, namely Busternet, including operation detection branch (Mani-Det Branch) and similarity detection branch (Simi-DET Branch) [29]. Jaiswal and Srivastava [30] proposed an encoder-decoder CNN model based on multi-scale input and multi-level convolution layer, which can divide pixels into forged and unforged pixels by the final sigmod activation function. Liu et al. [31] proposed a novel convolutional kernel network (CKN) based on an improved CNN structure that can greatly reduce the training time cost.

Recently, a number of multi-features-based methods have been proposed for improved detection performance. Sunitha et al. [32] presented a keypoint-based method for efficient detecting copy-move forgery with a hybrid feature. Peng et al. [33] proposed a progressive hybrid feature-based method, which uses no threshold in the steps of obtaining similar local regions. Khan et al. [34] develop a detection method by combining the features of block and feature points, but this method has a relatively high false alarm rate. Pun et al. [35, 36] combine the SURF feature and DAMFT features, but their method has a high time complexity and still uses a fixed threshold when judging a region's attributes.

In summary, the image partition-based methods generally adopt a global search strategy, which can achieve high accuracy but with a high false alarm rate, because the used features like SIFT can be easily disturbed by natural similarity. The deep-learning-based methods can automatically extract features, but their robustness needs to be improved due to the uncertainty of the deep feature generation and needs of large amounts of training data. In order to achieve low false alarm rate and high robustness, we explore how to combine different features and attend to propose an improved method with adaptive thresholds in this paper.

3 Proposed method

In [33], the authors used uniform non-overlapping segmentation in the image preprocessing stage, but this approach did not consider the correlation between pixels, easily resulting in losing the correlation between local regions in the image. The number of regions acquired by the Hu and SIFT features is inconsistent in terms of progressive hybrid features. In addition, a fixed threshold value is still used in the final determination of regional attributes. To solve these problems, this paper proposes an adaptive two-stage forgery detection method based on super-pixel segmentation and parallel feature fusion. The proposed method is shown in Fig. 1, where it can be seen that it includes two stages, coarse-grained detection and fine-grained detection.

In the first stage, the simple linear iterative cluster (SLIC) algorithm is used to preprocess an image to obtain the set of irregular local regions with semantic information, and the SIFT feature is used to characterize these regions and establish the correlation distribution map. Then, the candidate tampering regions are obtained according to the correlation distribution map.

In the second stage, the candidate tampering regions are combined with some similar local regions first, and then, a parallel fusion feature is extracted to express the characteristics of local regions. Next, the thresholds are adaptively generated according to the HOG feature of matched local regions, which is used to decide whether a local region has been tampered.

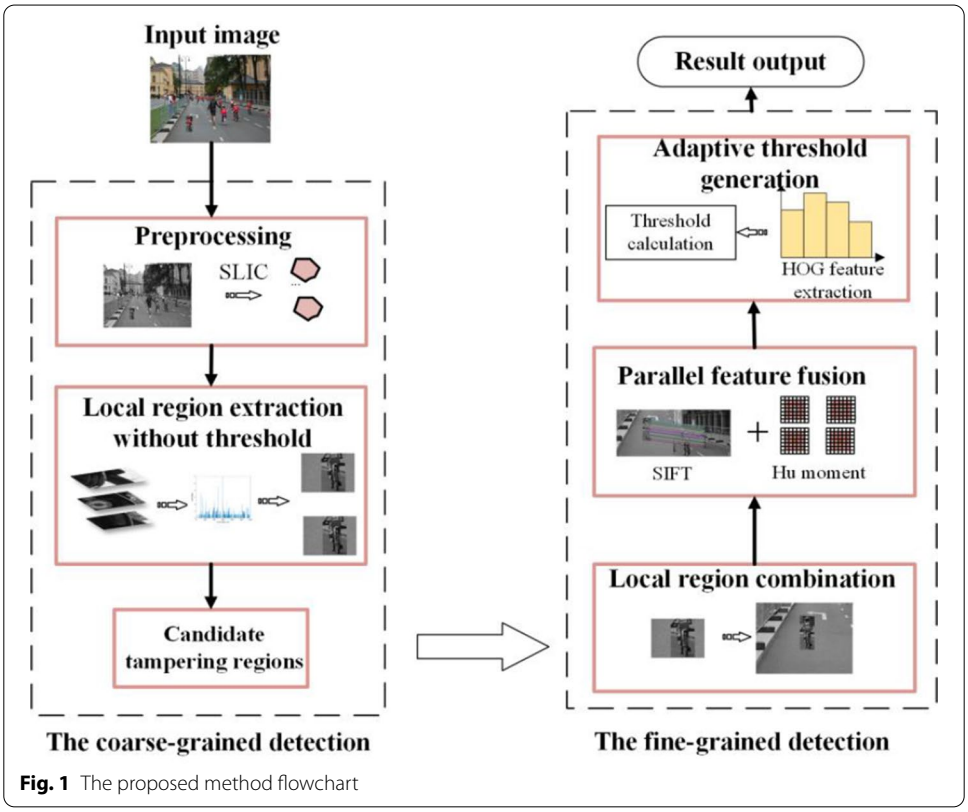

Fig. 1 The proposed method flowchart

3.1 Preprocessing step

In the preprocessing step, a color image is mapped to the gray space first and then segmented by the SLIC algorithm is to obtain the local regions. The SLIC algorithm clusters pixels to generate irregularly shaped super-pixels by using an iterative strategy, which is ideal in running speed, compactness and contours preservation. The main process is to transform RGB color images into 5-dimensional feature vectors in CIELAB color space and XY coordinates, and then construct distance metrics for 5-dimensional feature vectors, and perform local clustering of image pixels. The distance metric of the super-pixels D' is calculated by Eq. (1).

$$D' = \sqrt{(d_c/N_c)^2 + (d_s/N_s)^2} \tag{1}$$

where d_c and d_s represent the color distance and the spatial distance respectively; N_s is the maximum spatial distance within the class, which is applicable to each cluster; N_c is the maximum color distance. The pseudocode of the SLIC is given in Algorithm 1.

Algorithm 1: SLIC super-pixel segmentation

Input: Gray-scale image (gray_image)
Output: super-pixel segmentation image
Initialization
1) Init_Cluster_Center (gray_image)→(C_k) // Initialize cluster centers C_k
2) Reselect_Clusters (C_k)→(M_C_k) // Reselect new cluster centers M_C_k to the lowest gradient // position in a 3×3 neighborhood
Repeat
3) Assignment $(M\_C_k) \rightarrow (d_c, d_s)$ // Set allocation parameter and get d_c and d_s
4) Distance_metric $(d_c, d_s) \rightarrow (D')$ // Compute the distance of super-pixels
5) Update_Clusters$((D') \rightarrow (E)$ // Update new cluster centers and compute residual error E
Until $E \leq threshold$
6) **return (slic_image)** // return the result of super-pixel segmentation

The comparison of the segmentation effects of the non-overlapping segmentation and the SLIC segmentation on a gray-scale image is presented in Fig. 2. Traditional segmentation simply divides regions without considering the correlation between pixels. In addition, the local region extraction algorithm with no-threshold in the next step operates based on the correlation between local regions. Therefore, when a tampering region

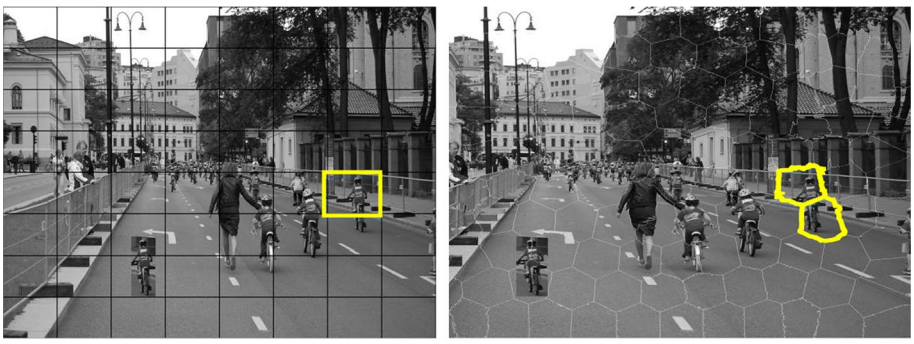

Fig. 2 Comparison of the segmentation effects of two different segmentation schemes. **a** Uniformly non-overlapping segmentation, **b** SLIC segmentation

is divided into several different local regions, the correlation between them will be weakened, leading to a failure of the local region extraction algorithm to mine accurately the local information of an image containing the tampering region. Conversely, the SLIC segmentation clusters correlated pixels into a super-pixel block of an irregular shape, which has the visual integrity of an object and can retain tampering region information as much as possible.

3.2 Similar local region extraction without threshold

The process of similar local region extraction is to find the pairs of matching regions with a high similarity according to the degree of feature point matching between regions, and denote them as the candidate tampering regions. The specific process is shown in Fig. 3.

Firstly, each local region is described by the SIFT feature. And the two-nearest neighbor algorithm is used to match the SIFT feature points of local regions. When the Euclidean distance of two feature points is less than the minimum distance and the second smallest (default value is 10), the feature matching is considered successful.

Secondly, we use the RANSAC algorithm to further remove false matching points from the above matching points. Specifically, a corresponding homography matrix containing geometric information such as rotation and scaling of the tampered region is estimated for each matching point using an iterative mechanism. Then, the correlation confidence of the two matching points is calculated based on the upper homography matrices. If the correlation confidence is lower than a fixed threshold (the default value is set as 0.995 in this paper), the two matching points are mismatched.

Next, according to the matching results of feature points, the correlation distribution map between local regions is established, as shown in Fig. 4. This map represents the correlation between two local regions, and the larger its value is, the stronger the correlation between two regions will be. Thus, a pair of two matching regions with the greatest correlation can be a tampering region. Therefore, the local regions that correspond to the peak and sub-peak of correlation are selected as the candidate tampering regions.

The candidate tampering regions obtained by coarse-grained detection is a set of local regions with high correlation, which includes both the real tampering regions and the natural original regions with high similarity. Therefore, it is necessary to accurately determine the candidate tampering super-pixels in the next stage of fine-grain detection.

3.3 Local region combination

To obtain larger receptive fields and to generate more complete candidate tampering regions, the acquired target local regions are needed to be combined. The specific process is shown in Fig. 5, where it can be seen that the target super-pixel is set as a center and the neighborhood super-pixels and the target super-pixel are combined;

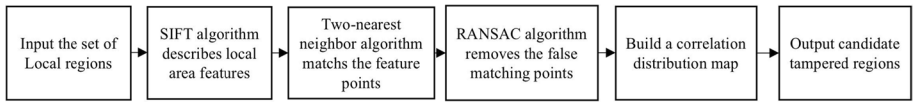

Fig. 3 The block diagram of the similar local region extraction process

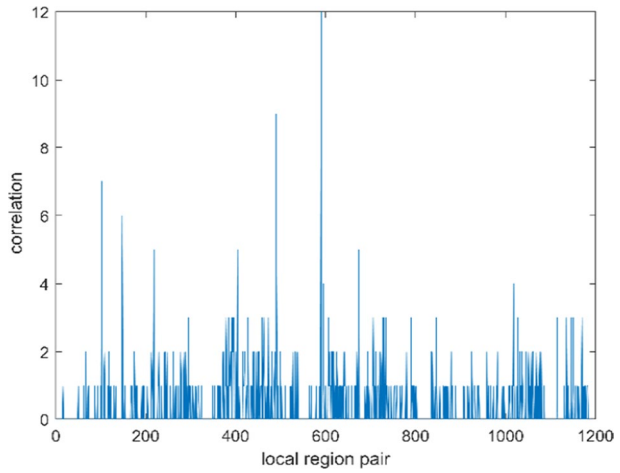

Fig. 4 Correlation distribution map

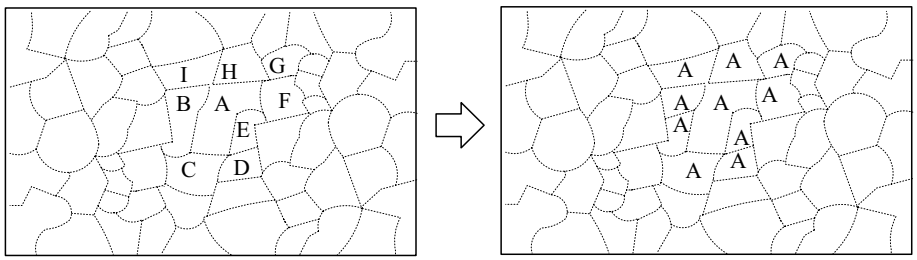

Fig. 5 Illustration of the region combination process

namely, the pixel labels of the neighborhood super-pixels are modified into that of the target super-pixel.

In the process of region combination, if the distance between two super-pixels is too close, local aliasing can be easily caused. Thus, it is necessary to consider a relative position between two suspected tampering regions. First, each super-pixel is labeled and the distance between the super-pixels is calculated by Eq. (2), where d represents a relative positions of two local regions, abs() represents the absolute value function, and c_i represents the location coding of a local region i.

$$d = \text{abs}(c_1 - c_2) \tag{2}$$

According to the relative position between two local regions, there are two possible cases.

(1) A region in the matched pair is at the image edge.
(2) No region in the matched pair is at the image edge.

In case (1), due to the influence of the edge effect, it is impossible to use eight-neighborhood for the local region on the image edge, so the four-neighborhood association is adopted. In case (2), the n-neighborhood is adopted, and the value of n

depends on the relative position d, which is calculated by Eq. (3), where L represents the sampling size. When two local regions are distant, the eight-neighborhood combination mode can be chosen, otherwise, the six-neighborhood combination mode can be chosen.

$$n = \begin{cases} 6, & d = 1, L, L+1, L-1, L+2, L-2, 2L+1, 2L-1, 2L+2, 2L-2 \\ 8, & \text{else} \end{cases} \tag{3}$$

3.4 Parallel feature fusion

To eliminate the interference introduced by natural highly correlated regions, Peng et al. [33] proposed a forgery detection method based on progressive fusion features. In this method, first, the SIFT feature of each local region is extracted and matched, and then the Hu moment feature is extracted from the neighborhood of each pair of matched feature points, which are required to be secondly matched. Finally, the attribute of the local region is judged according to the rules. The fusion feature with a progressive structure can effectively combine the SIFT feature with the Hu feature to enhance the detection robustness and to avoid the interference of a similar natural region caused by illumination invariance, however, this approach has certain problems. First, the scheme needs quadratic matching of feature points, which is highly time-consuming to calculate. Secondly, the expression ability of the progressive fusion features is not strong enough to make full use of the SIFT or Hu features, thus leading to a relatively high false alarm rate.

Moreover, the Hu moment feature is calculated for the neighborhood pixels of the SIFT-based matched key points, so its scope is limited to the matched feature points, which makes it difficult to describe the local region accurately, leading to the phenomenon of "missing matching" in the feature point matching algorithm. As shown in Fig. 6, some of the discrete feature points are not judged as matching points.

To solve the above problems, a new parallel fusion feature is proposed to describe a local region with suspected tampering. The block diagram of the fusion process is shown in Fig. 7. First, a set of SIFT feature points is obtained from the candidate local regions, and then the SIFT and HU features are calculated and combined simultaneously in the neighborhood of the feature points, and the final descriptor corresponding to the pair of matched regions is constructed after normalization.

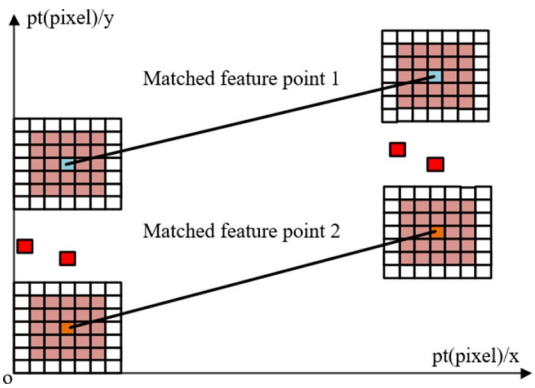

Fig. 6 Scope of the Hu moment

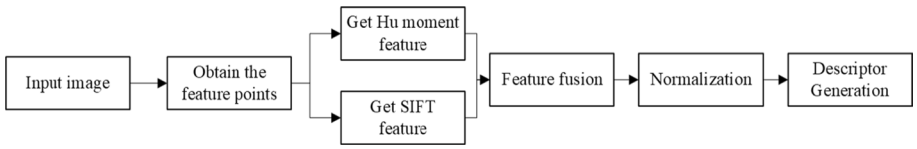

Fig. 7 The block diagram of the parallel feature fusion process

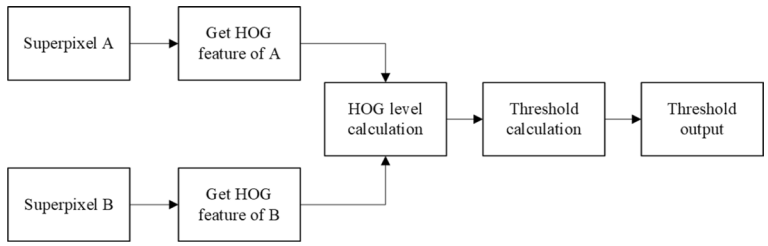

Fig. 8 The block diagram of the adaptive threshold generation process

For each feature point, a seven-dimension vector of the Hu moment feature (Hu_7) and a 128-dimension vector of the SIFT feature of the neighborhood pixels ($SIFT_{128}$) are generated. Since the first to fourth components in the vector of the Hu moment feature have strong invariance, only the first four-dimension vector of the Hu feature (Hu_4) and $SIFT_{128}$ are combined to generate the final 134-dimension feature vector. Then, it is normalized to eliminate the dimensionality effect and used as a feature descriptor in region matching, namely parallel fusion feature ($ParallelF_{134}$) expressed by Eq. (4), where concat(·) denotes a combinatorial function and Normalize(·) represents a normalized function provided by OpenCV.

$$\mathrm{ParallelF}_{134} = \mathrm{Nomailze}(\mathrm{concat}((\mathrm{SIFT}_{128}, \mathrm{Hu}_4)) \tag{4}$$

The way of progressive feature fusion extracts the Hu moment feature from the matched feature points and performs the secondary matching on this feature. The parallel feature fusion directly extracts the SIFT and Hu moment features from the extracted feature point set and combines them, which expands the extraction range of the Hu moment feature and enhances the expression ability of the parallel fusion feature.

3.5 Adaptive threshold generation based on HOG level

Generally, traditional methods use thresholds in two situations: (1) to measure whether there is a similarity between local regions or features, and (2) to measure whether the similarity of regions meets the standard of a copy-move forgery. At present, there have been no uniform standards for selecting a fixed threshold. In addition, different images have different characteristics such as color, illumination, or texture, so it is challenging to choose a threshold that will be suitable for most images. In this paper, an adaptive threshold generation algorithm based on the HOG level is adopted. After the description and matching of super-pixels by the parallel fusion feature, a threshold is automatically generated to determine whether two matched super-pixels denote tampering regions. The schematic of this process is shown in Fig. 8.

The HOG is a feature descriptor representing the texture information of an image's local regions through the gradient information. If the super-pixels A and B contain a tampering region, their texture information for both should be the same.

For super-pixels A and B containing the candidate tampering regions, their HOG features are extracted, and the corresponding HOG levels representing their texture richness are calculated by Eqs. (5) and (6), respectively, where $i = 1, 2, 3, \ldots, n$, and $c = 1, 2$; n represents the total dimension of the HOG feature, x_i represents the ith component of the HOG feature, and E_c represents the average gradient intensity of a local region.

$$E_c = \sum x_i / n \tag{5}$$

$$\text{HOG\_Level} = E_1 + E_2/2 \tag{6}$$

Most of the SIFT feature points exist in the high entropy region of the image, which is the region with rich texture, and the texture richness of a region will directly affect the number of SIFT feature points. When the tampering region is relatively flat, the feature points will attenuate to a certain extent. But when the texture of the tampering region is rich, it will have more feature points. That is, the number of feature points directly affects the amount of information available for similarity calculation. Thus, the HOG level of the pair of matched local regions can be used for dynamically adjusting the threshold T, which can be calculated by Eq. (7), where m is the proportionality factor, with the default value of one. The pseudocode of the adaptive threshold generation algorithm is given in Algorithm 2.

$$T = \text{HOG}_{\text{Level}} \times m \tag{7}$$

Algorithm 2: Adaptive threshold generation

Input: suspected tampering regions *s1and s2*
Output: threshold T
1) HOG_Feature_Detector(*s1*) →(***desc1***) //Obtain HOG feature
2) HOG_Feature_Detector(*s2*) →(***desc2***)
3) E_1 = Sum(***desc1***) / Len(***desc1***) //Obtain the average gradient intensity
4) E_2 = Sum(***desc2***) / Len(***desc2***)
5) *HOG_Level* = (E_1+ E_2) / 2 //Obtain the HOG level
6) T = *HOG_Level* × m
7) **return** T

The adaptive threshold generation algorithm sets the thresholds according to the characteristics of the local regions, which increases the generalization and robustness of the proposed detection method. The generated threshold value is used as a criterion to determine whether the local region is a tampering region. Namely, the correlation between super-pixels A and B is compared with the threshold value T, and if the similarity is greater than T, the region is considered as a tampering region.

Table 1 Basic information on datasets used in the experiments

Datasets	Number of original images	Number of tampering images	Resolutions	Image formats	Number of attack types
COMOFOD	200	4800	512 × 512	JPEG	6
MICC-F220	110	110	739 × 492	JPEG	1
MICC-F2000	700	1300	739 × 492	JPEG	1

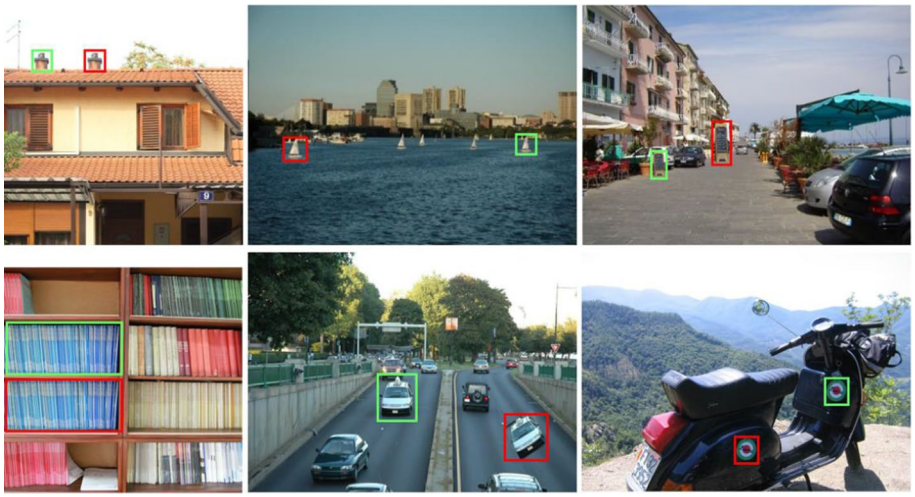

Fig. 9 Some examples in test images of three differents datasets

4 Results and discussion

4.1 Datasets and evaluation metrics

In the experiments, the hardware includes a PC with an Intel I7-9700K CPU and Nvidia Tesla P40, running on Windows 10 operating system. The software is Microsoft Visual Studio 2019. The true positive rate (*TPR*), false positive rate (*FPR*) and *F*-measure (*F*1) are used as the evaluation metrics of the proposed algorithm's detection performance.

The performance of the proposed method is verified by experiments on three public datasets, namely, MICC-F220, MICC-F2000 and COMOFOD datasets [17, 37]. The basic information on the datasets is given in Table 1. And some examples of tampered images in the datasets are shown in Fig. 9. where the green boxes are the source target regions and the red boxes are the tampered regions.

The MICC-F220 and MICC-F2000 datasets are used to verify the robustness of the proposed method against geometric attacks, including translation, rotation, and stretch and the different combinations of the above three operations. According to the degrees of rotation, stretch and translation, there are different requirements for algorithm robustness. The scaling scales in the x-axis direction and y-axis direction are denoted as S_x and S_y respectively; the rotation angle of a local region is denoted as θ; the attack degrees of the MICC-F220 and MICC-F2000 datasets are H and J, respectively. The attack degrees of these two datasets are given in Tables 2 and 3, respectively.

Table 2 Type of geometric attack in MICC-F220 dataset

	H1	*H2*	*H3*	*H4*	*H5*	*H6*	*H7*	*H8*	*H9*	*H10*
θ	0	10	20	30	40	0	0	0	10	20
S_x	1	1	1	1	1	1.2	1.3	1.4	1.2	1.4
S_y	1	1	1	1	1	1.2	1.3	1.4	1.2	1.4

Table 3 Type of geometric attack in MICC-F2000 dataset

	J1	*J2*	*J3*	*J4*	*J5*	*J6*	*J7*	*J8*	*J9*	*J10*	*J11*	*J12*	*J13*	*J14*
θ	0	5	25	70	90	0	0	0	0	0	0	0	40	30
S_x	1	1	1	1	1	1.2	1.5	2.0	0.7	0.5	1.4	2.6	3.4	1.4
S_y	1	1	1	1	1	1.2	1.5	2.0	0.7	0.5	1.7	1.3	1.2	0.7

Table 4 Attack types in COMOFOD dataset

Attack types	Attack degree levels	Related parameters
JPEG compression	*JC1, JC2, …, JC9*	Compression factor = [20, 30, 40, 50, 60, 70, 80, 90, 100]
Blur attack	*IB, IB2, IB3*	Fuzzy window size = [3 × 3, 5 × 5, 7 × 7]
Contrast change	*CA1, CA2, CA3*	Adjustment interval = [(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]
Color adjustment	*CR1, CR2, CR3*	Variations in brightness for each color channel: [32, 64, 128]
Brightness change	*BC1, BC2, BC3*	Adjustment interval = [(0.01, 0.95), (0.01, 0.9), (0.01, 0.8)]
Gaussian noise	*NA1, NA2, NA3*	Mean = 0, variance = [0.0009, 0.005, 0.0005]

Table 5 Detection results of different schemes with different module combination

Name	Description	*TPR* (%)	*FPR* (%)	*F1*
Scheme 1 [33]	Uniform-type segmentation + progressive fusion feature	97.2	6.4	92.9
Scheme 2	SLIC + progressive fusion feature	97.5	6.2	93.3
Scheme 3	SLIC + parallel fusion feature	97.9	5.5	94.1
Scheme 4 (our method)	SLIC + parallel fusion feature + adaptive threshold generation	**98.5**	**5.7**	**94.3**

Bold text indicates that the current method has the highest value

The COMOFOD dataset is used to test the robustness of the algorithm from two aspects: attack type and attack degree. Among them, tampered images are accompanied by various post-processing attacks of different degrees, including JPEG compression, blur, contrast change, color adjustment, brightness attack and Gaussian noise. The information on the attack types in this dataset is given in Table 4.

4.2 Module validity testing

For verifying the module validity of the SLIC, parallel feature fusion and adaptive threshold generation algorithm, four different schemes are conducted and evaluated on the MICC-F2000 dataset. The method proposed in [33] (Scheme 1) is used as a baseline, Scheme 4 is our proposed method. The experimental results are shown in Table 5.

Table 6 Comparison of different methods on the MICC-F220 dataset

	TPR (%)	*FPR* (%)	*F*1
Das [16]	90.9	**4**	93.0
Resmi [21]	90.9	6	91.3
Soni [23]	97.6	8.4	94.7
Peng [33]	98.2	8.1	95.1
Alberry [34]	99.1	9.2	95.1
Proposed method	**99.1**	7.2	**95.9**

Bold font indicates that the current method has the highest value

Table 7 Comparison of different methods on the MICC-F2000 dataset

	TPR (%)	*FPR* (%)	*F*1
Amerini [17]	93.4	12.5	86.25
Amerini [20]	94.8	9.15	89.5
Soni [23]	96.4	9.8	89.8
Peng [33]	97.2	6.4	92.9
Proposed method	**98.5**	**5.7**	**94.3**

Bold font indicates that the current method has the highest value

Compared with Scheme 1, the *TPR* of Scheme 2 increased by 0.3% and *FPR* is decreased by 0.2%, indicating that SLIC can improve the detection performance to a certain extent. Compared with Scheme 2, the *TPR* and *FPR* of Scheme 3 are increased by 0.4% and decreased by 0.7%, respectively, indicating that the parallel fusion feature is stronger than the progressive fusion feature in characterizing the local region and could accurately identify the tampering region without being disturbed by the similar natural region. In Scheme 4, the adaptive threshold generation algorithm is added to improve the detection ability of the tampering region further, and the *TPR* of this scheme is 0.6% higher than that of Scheme 3. Although the *FPR of* Scheme 4 is increased by 0.2%, *F*1 is still 0.2% higher than that of Scheme 3, indicating that the comprehensive performance of proposed Scheme 4 is better than that of other schemes.

4.3 Comparison with other methods

The proposed method is compared with other methods, and the comparison results are given in Tables 6 and 7. Table 6 shows the effects of different methods on the MICC-F220 dataset. As given in Table 6, the *TPR* of the proposed method is 99.1%, which is consistent with that of Alberry's method [34]. However, for the proposed method, the *FPR* is 2% lower and *F*1 is 8% higher than those of Alberrys' method. Although the *FPR* of the proposed method is 1.2% and 3.2% higher than those of Resmi [21] and Das [16], its *TPR* is 8.2% higher, and its *F*1 is 4.6% and 2.9% higher than those of these two methods, respectively. Thus, the proposed method can guarantee higher accuracy, lower false alarm rate, and the better comprehensive detection performance. As shown in Table 7, the *TPR*, *FPR* and *F*1 of the proposed method are the highest on the MICC-F2000 dataset among all the methods.

As shown in Tables 6 and 7, the detection effect of the proposed algorithm on the MICC-F220 dataset is not significantly improved compared with the results on the MICC-F2000 dataset. The main reason for this is that the degree of post-processing attacks in the MICC-F220 dataset is not as rich as that in the MICC-F2000 dataset. Namely, there is only a small amount of equal stretching in the MICC-F200 dataset, while the functions of unequal stretching and combination are included in MICC-F2000, which requires higher robustness of the detection methods. The existing methods have certain robustness against small scale equal stretching, but the resistance against unequal stretching and its combination attacks still needs further improvement. Therefore, the performance of the existing methods on the MICC-F2000 dataset is slightly lower than those on the MICC-F220 dataset.

4.4 Robustness analysis of different methods

The detection accuracy comparison of the proposed method and the method presented in [33] under different degrees of geometric attacks is displayed in Fig. 10, where *H1–H9* contains equal rotation and equal proportional pressure and their combination, and the value range of the scale factor is 1–1.5. As shown in Fig. 10, the methods performed well against the *H1–H9* attack types on the MICC-F220 dataset. The results show that with the deepening of the attack degree, the proposed method could still remain the accuracy higher than 92% under the *H10* attack.

The MICC-F2000 dataset contains tampering images of both equal and unequal stretches, and the scale factor range is wider than that of the MICC-F220 dataset. In addition, unequal stretches have different scaling factors in different directions, resulting in a relatively large distortion in the target region, which affects the similarity between local regions and thus the detection effect, so a detection method with high robustness is required to recognized the geometric attack. As shown in Fig. 11, the *TPR* of the proposed method is improved obviously in three levels of *J*11, *J*12 and *J*13. Compared with Peng's method [33], the increase is 2%, 2% and 4%, respectively. Therefore, the proposed method shows stronger robustness against the combined geometric attacks of unequal scale transformation and rotation than Peng's method.

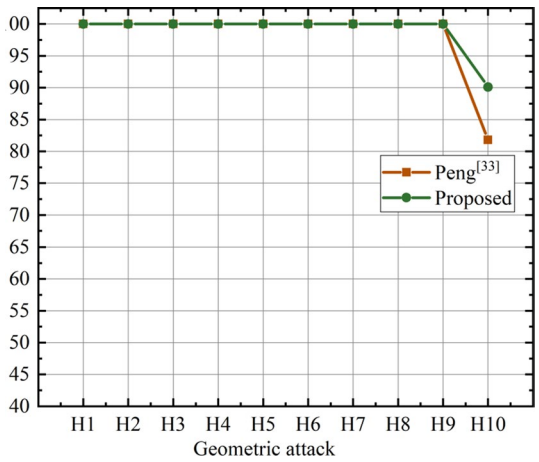

Fig. 10 Robustness comparison on the MICC-F220 dataset

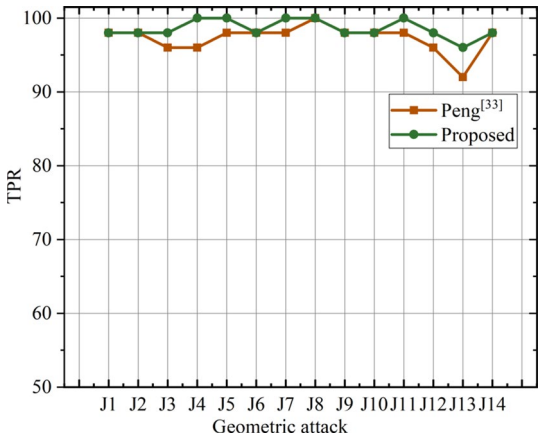

Fig. 11 Robustness comparison on the MICC-F2000 dataset

Table 8 Labels of different existing methods

Methods	Ryu [10]	Cozzolino [11]	Wu [28]	Wu [29]
Labels	Zernike	Patch	DVN	BusterNet

The resistance performances of different methods to the post-processing attacks are presented in Fig. 11. For the convenience of observation, the compared methods are marked in Fig. 11 using the labels shown in Table 8. Based on the results, in the case of different attacks, the detection ability of the proposed methods is better than those of the other methods.

As shown in Fig. 12a, the recognition ability of the proposed method is excellent for the JPEG attack, and the accuracy is about 40% higher than that of the BusterNet in the case of the *JC4* attack. In addition, the increase in the compression factor does not significantly affect the *TPR* of the proposed method, indicating that the proposed method also has a strong resistance to JEPG compression. As shown in Fig. 12b, our method also has a good resistance to brightness changes; namely, its *TPR* does not decrease with the increase in the brightness adjustment space, which is due to the illumination invariance of the SIFT features. For the contrast attack, according to Fig. 12c, the *TPR* of the proposed method decreases with the expansion of the contrast region, and its accuracy is low in the case of the *CA3* attack. The contrast transformation is mainly implemented by adopting the gray histogram equalization method for local regions and thus leads to the difference in features between the copied region and pasted region. Therefore, the proposed method is more sensitive to the contrast attack than the other methods, but it could still achieve a good accuracy. In addition, Fig. 12d shows that the proposed method can effectively resist the color attack.

However, Fig. 12e shows that under the fuzzy attack, the accuracy of the proposed method is low, which is in a suboptimal position at the *IB1* level, and its *TPR* is 4% lower than that of the BusterNet; also, *TPR* decreases with the increase in blur intensity, and only 35% accuracy could be achieved under the *IB3* attack. Namely, the essence of the blur attack is the weighted average of the pixels in the local region,

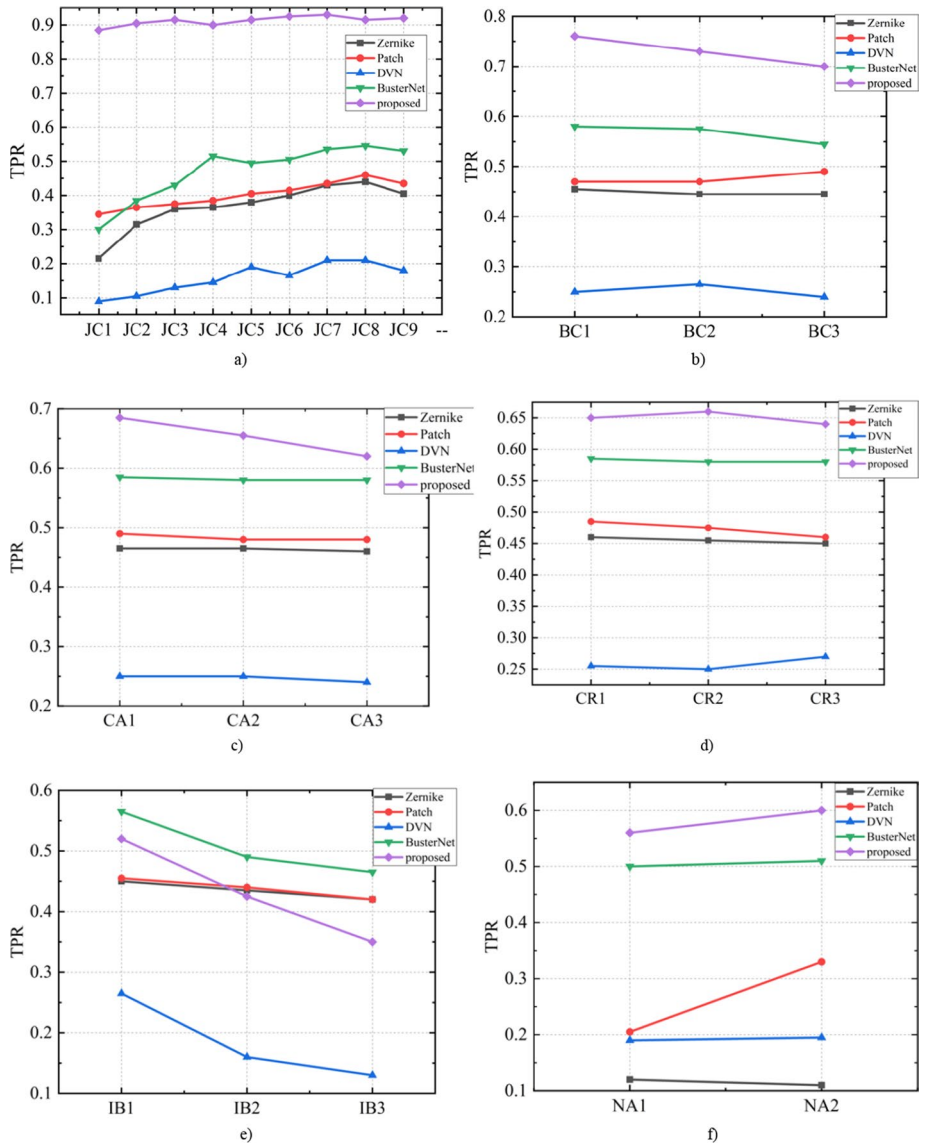

Fig. 12 Robustness comparison of different methods for different attack types. **a** JPEG attack, **b** brightness change, **c** contrast change, **d** color change, **e** fuzzy attack, **f** noise addition

which greatly weakens the gradient information of local regions, especially those with a rich texture. The key point of the SIFT is the extreme value in the local region, which mostly has a rich texture. Therefore, the reduction in regional gradient information will result in a decrease in the number of key points of the SIFT; that is, the amount of information used to describe the similarity of local regions will decrease sharply, leading to a significantly decrease in the detection performance of the proposed method. As shown in Fig. 12f, the proposed scheme also has a strong resistance to noise.

As analyzed above, the proposed method achieves a good robustness to the JPEG compression, color change, brightness change and noise addition, and could

withstand a certain degree of contrast change, noise addition and fuzzy attack, among which, the ability to resist the fuzzy attack still could be further improved.

4.5 Comparison with deep-learning-based methods

The recent success of deep learning in the field of pattern recognition has motivated many scholars to try to apply deep learning technology to the field of image forensics. In the copy-move forgery detection applications, both the BusterNet and the convolutional kernel network (CKN) proposed by Liu et al. [29]. have been used in recent years. The BusterNet uses a two-stream network structure to identify the tampering regions of an image. The robustness of the BusterNet is stronger than that of the proposed method only under the fuzzy attack but slightly weaker than the proposed scheme under other attacks, as shown in Fig. 12.

The CKN represents a variant of the CNN network, which accelerates the CNN's training speed. The comparison results of the proposed method and the CKN are given in Table 9, where it can be seen that in the experiments, the proposed scheme is superior to the CKN network in terms of *TPR*, *FPR* and *F*1 metrics. Compared with the CKN, the *TPR* of the proposed method is 5.5% higher and its *FPR* is 5.3% lower, indicating that the overall performance of the proposed method is better than that of the CKN.

Although deep learning technology has the advantages of automatic feature extraction and strong generalization, it still has certain technical difficulties in the field of copy-move forgery detection, which can be summarized as follows.

(1) Fewer features to be learned. The traditional recognition task is mainly to detect various objects in an image, and a set of object features of objects that can be learned in the training process is relatively rich, including eyes, hair, and contour in the task of cat and dog recognition. However, in the task of copy-move forgery detection, the tampering regions can be randomly selected, and the training dataset cannot provide significant training features to the network.
(2) Fewer public datasets. Network model training requires a labeled dataset of a certain size. At present, the application research on deep learning technology in the field has still been in the preliminary stage. In addition, typically used databases, such as GRIP, CASIA, MICC-F220, and MICC-F2000, include a small number of images and contain a variety of post-processing methods, which makes it difficult to provide enough valuable learning information to the model. In contrast, personally-made datasets, while being a good choice, are difficult to label effectively.
(3) Forensics technology based on deep learning has a strong dependence on the training dataset and requires that the training set and testing sets have the same data

Table 9 Comparison of different methods

Methods	*TPR* (%)	*FPR* (%)	*F*1 (%)
CKN	93	11	87.2
Peng [30]	97.2	6.4	92.9
Our	98.5	5.7	94.3

distribution. However, in the practical application, the consistency between a random image to be detected and data used to train the network cannot be guaranteed.

(4) In addition, the training process of a deep learning-based model has a high time cost. Conversely, the proposed scheme neither depends on the training set, nor needs to train the detection model, but it has strong robustness, which has a certain practical significance.

4.6 Comparison of running times

This section compares the running times of different methods. In the test, 25 original images and 25 tampering images are randomly selected from the MICC-F2000 dataset. The proposed method is used to detect these 50 images, and the average running time of processing an image is calculated. The running time comparison of the proposed method and the existing methods is shown in Fig. 13.

The results show that compared with Peng's method [33], the running time of the proposed method ranks in the middle, which increases mainly in two situations. In the preprocessing step of the first stage, instead of using the uniform-type segmentation, the proposed method adopts the SLIC algorithm with an iterative mechanism to cluster pixel values and to obtain irregular and meaningful super-pixels. The clustering process involves complex steps such as feature construction, distance measurement, and seed point updating, which is time-consuming. In the second stage, the processes of parallel feature fusion and adaptive threshold generation are needed to extract three types of features, which requires much time. To improve the detection accuracy and robustness, the SLIC segmentation is introduced, which represents adaptive threshold generation algorithm with high complexity. However, as observed in Fig. 13, the time complexity of the proposed method is within a tolerable range, so this method has a strong practical significance.

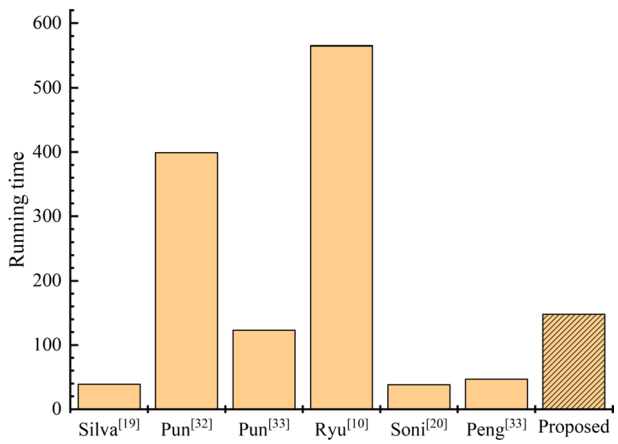

Fig. 13 Running time comparison of different methods

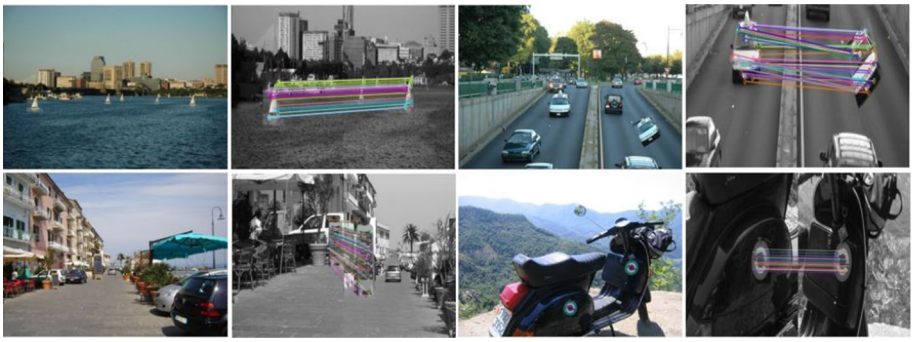

Fig. 14 The results of proposed method on FICC-F220 and FICC-F2000 dataset

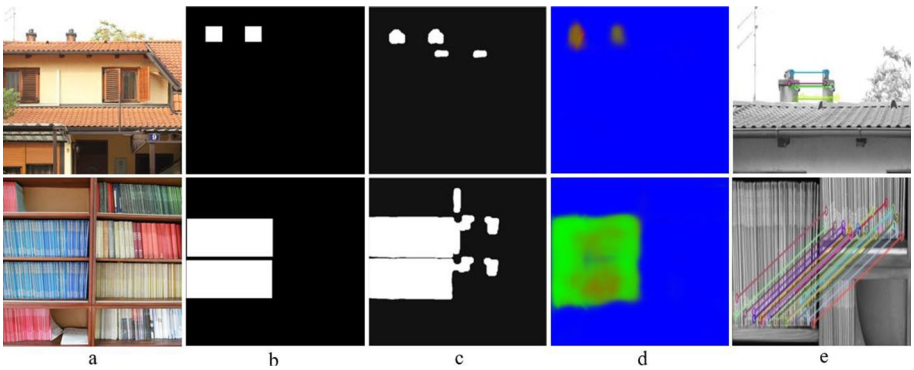

Fig. 15 The results of copy-move forgery region localization by different methods. **a** is Forged image, **b** is Ground truth, **c** is the results of CKN [29], **d** is the results of BusterNet [28], and **e** is Ours

4.7 Localization performance analysis of tampering regions

This subsection evaluates the tampered region location performance of the proposed method. As shown in Fig. 14, the first and second rows are the results of locating tampered regions on FICC-F220 and FICC-F2000 datasets by the proposed method respectively. The results show that the proposed method can detect copy-move forgery and mark forgery feature points accurately. Figure 15 give the results of tampered region localization by different methods, a is Forged image, b is Ground truth, c is the results of CKN [29], d is the results of BusterNet [28], and e is Ours.

As illustrated in Fig. 15, we observe that BusterNet and CKN models based on deep learning can realize the location of tampered regions by using real labelled data for training. Although there are certain noises and misidentified regions, the source/target locations are roughly accurate. The proposed method can also accurately obtain the content information of the tampered region by obtaining the tampered feature points, but does not accurately give the location of the tampered source/target. Therefore, in the future, we will explore the combination of the technology in this paper and semantic segmentation technology based on deep learning, and study how to achieve a more accurate location of source/target.

5 Conclusion

In this paper, an improved two-stage forgery detection method based on parallel fusion feature and an adaptive threshold generation algorithm, which includes coarse-grained detection and fine-grained detection. In the coarse-grained detection stage. the SLIC algorithm is used to preprocess an image and to divide the image into irregular superpixels, solving the problem of local regional correlation attenuation caused by uniform segmentation. In the fine-grained detection stage, a parallel fusion feature is used to enhance the feature expression ability of a local region. To improve the robustness of the proposed method, an adaptive threshold generation algorithm based on the HOG level is designed to generate a suitable threshold conforming to the characteristics of different local regions for the final detection of suspected tampering regions. The proposed method is verified by experiments and compared with the other methods. The experimental results show that the proposed method achieves highest accuracy among all compared methods, and it has higher robustness which can resist several common attacks such as noise and brightness change.

However, there is room for further improvement of this method's resistance to fuzzy attack, which needs further study. Compared with the deep learning methods, the proposed method is still weak in locating the tampered region, and it is difficult to accurately give the specific coordinates and contours of the tampered region. Thus, It is necessary to combine with deep learning methods to achieve accurate detection and positioning. In the future, it is also needed to continue to explore different types of feature fusion and new feature mining to further improve detection capabilities.

Abbreviations

CNN: Convolutional neural network; HOG: Histogram of oriented gradient; SLIC: Simple linear iterative cluster algorithm; RANSAC: Random sample consensus algorithm; TPR: True positive rate; FPR: False positive rate; *F*1: *F*-Measure.

Acknowledgements

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that helped to improve the quality of this manuscript.

Authors' contributions

WY and YL conceived and designed the study. YL and CC contributed to refining the ideas. WY, QZ and YP performed the research, collected the data and analyzed the results. WY and YL drafted the manuscript, YL and CC revised it. All authors read and approved the final manuscript.

Funding

This work was supported in part by Key-Area Research and Development Program of Guangdong Province under Grant Nos. 2018B030338001, 2018B010115002, 2018B010107003, and in part by Innovative Talents Program of Guangdong Education Department and Young Hundred Talents Project of Guangdong University of Technology under Grant No. 220413548.

Availability of data and materials

Not available online. Please contact the author for data requests.

Declarations

Ethical approval

Ethical approval was obtained from the Ethics Committee of Guangdong University of Technology. And the datasets are publicly available on the Internet.

Competing interests

The authors declare that they have no conflict of interest.

Author details

[1]School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, Guangdong, China.
[2]Department of Information Engineering and Computer Science, Feng Chia University, Taichung 407802, Taiwan.

Received: 25 October 2021 Accepted: 10 March 2022
Published online: 01 April 2022

References

1. S.P. Chalamalasetty, S.R. Gidituri, Research perception towards copy-move image forgery detection: challenges and future directions. Int. J. Image Graph. **21**(4), 2150054 (2021). https://doi.org/10.1142/S0219467821500546
2. B. Soni, P.K. Das, D.M. Thounaojam, CMFD: a detailed review of block based and key feature based techniques in image copy-move forgery detection. LET Image Process. **12**(2), 67–178 (2018). https://doi.org/10.1049/iet-ipr.2017.0441
3. J. Yang, Z. Liang, Y. Gan, J. Zhong, A novel copy-move forgery detection algorithm via two-stage filtering. Digit. Signal Process. **113**, 103032 (2021). https://doi.org/10.1016/j.dsp.2021.103032
4. S. Teerakanok, T. Uhara, Copy-move forgery detection: a state-of-the-art technical review and analysis. IEEE Access **7**, 40550–40568 (2019). https://doi.org/10.1109/ACCESS.2019.2907316
5. J. Fridrich, D. Soukal, J. Lukáš, Detection of copy-move forgery in digital images, in *Proceedings of Digital Forensic Research Workshop*, pp. 1–10 (2003)
6. J. Zhao, J. Guo, Passive forensics for copy-move image forgery using a method based on DCT and SVD. Forensic Sci. Int. **233**(1–3), 158–166 (2013). https://doi.org/10.1016/j.forsciint.2013.09.013
7. A.C. Popescu, H. Farid, Exposing digital forgeries by detecting duplicated image regions. Computer Science Technical Report. TR2004-515 (2004)
8. W. Luo, J. Huang, G. Qiu, Robust detection of region-duplication forgery in digital image, in *18th International Conference on Pattern Recognition (ICPR'06)*, pp. 746–749 (2006). https://doi.org/10.1109/ICPR.2006.1003
9. G. Muhammad, M. Hussain, G. Bebis, Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digit. Investig. **9**(1), 49–57 (2012). https://doi.org/10.1016/j.diin.2012.04.004
10. S. Ryu, M. Kirchner, M. Lee, H. Lee, Rotation invariant localization of duplicated image regions based on zernike moments. IEEE Trans. Inf. Forensics Secur. **8**(8), 1355–1370 (2013). https://doi.org/10.1109/TIFS.2013.2272377
11. D. Cozzolino, G. Poggi, L. Verdoliva, Efficient dense-field copy-move forgery detection. IEEE Trans. Inf. Forensics Secur. **10**(11), 2284–2297 (2015). https://doi.org/10.1109/TIFS.2015.2455334
12. Y. Gan, J. Zhong, Application of AFMT method for composite forgery detection. Nonlinear Dyn. **84**, 341–353 (2016). https://doi.org/10.1007/s11071-015-2524-0
13. P. Yap, X. Jiang, A.C. Kot, Two-dimensional polar harmonic transforms for invariant image representation. IEEE Trans. Pattern Anal. Mach. Intell. **32**(7), 1259–1270 (2010). https://doi.org/10.1109/TPAMI.2009.119
14. Y. Wang, X. Kang, Y. Chen, Robust and accurate detection of image copy-move forgery using PCET-SVD and histogram of block similarity measures. J. Inf. Secur. Appl. **54**, 102536 (2020). https://doi.org/10.1016/j.jisa.2020.102536
15. N.B.A. Warif, M.Y.I. Idris, A.W.A. Wahab, R. Salleh, A. Ismail, CMF-iteMS: an automatic threshold selection for detection of copy-move forgery. Forensic Sci. Int. **295**, 83–99 (2019). https://doi.org/10.1016/j.forsciint.2018.12.004
16. T. Das, R. Hasan, M.R. Azam, J. Uddin, A robust method for detecting copy-move image forgery using stationary wavelet transform and scale invariant feature transform, in *2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2)*, pp. 1–4 (2018). https://doi.org/10.1109/IC4ME2.2018.8465668
17. I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, A SIFT-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. **6**(3), 1099–1110 (2011). https://doi.org/10.1109/TIFS.2011.2129512
18. H. Huang, W. Guo, Y. Zhang, Detection of copy-move forgery in digital images using SIFT algorithm, in *2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, pp. 272–276 (2008). https://doi.org/10.1109/PACIIA.2008.240
19. E. Silva, T. Carvalho, A. Ferreira, A. Rocha, Going deeper into copy-move forgery detection: exploring image telltales via multi-scale analysis and voting processes. J. Vis. Commun. Image Represent. **29**, 16–32 (2015). https://doi.org/10.1016/j.jvcir.2015.01.016
20. I. Amerini, L. Ballan, R. Caldelli, A.D. Bimbo, L.D. Tongo, G. Serra, Copy-move forgery detection and localization by means of robust clustering with J-Linkage. Signal Process. Image Commun. **28**(6), 659–669 (2013). https://doi.org/10.1016/j.image.2013.03.006
21. M.R. Resmi, S. Vishnukumar, A novel segmentation based copy-move forgery detection in digital images, in *2017 International Conference on Networks & Advances in Computational Technologies (NetACT)*, pp. 346–350 (2017). https://doi.org/10.1109/NETACT.2017.8076793
22. B. Xu, J. Wang, G. Liu, Y. Dai, Image copy-move forgery detection based on SURF, in *2010 International Conference on Multimedia Information Networking and Security*, pp. 889–892 (2010). https://doi.org/10.1109/MINES.2010.189
23. B. Soni, P.K. Das, D.M. Thounaojama, Geometric transformation invariant block based copy-move forgery detection using fast and efficient hybrid local features. J. Inf. Secur. Appl. **45**, 44–51 (2019). https://doi.org/10.1016/j.jisa.2019.01.007
24. A. Shahroudnejad, M. Rahmati, Copy-move forgery detection in digital images using affine-SIFT, in *2016 2nd International Conference of Signal Processing and Intelligent Systems (ICSPIS)*, pp. 1–5 (2016). https://doi.org/10.1109/ICSPIS.2016.7869896
25. R. Kaur, A. Kaur, Copy-move forgery detection using ORB and SIFT detector. Int. J. Eng. Dev. Res. **4**(4), 804–813 (2016)
26. J. Zhao, W. Zhao, Passive forensics for region duplication image forgery based on Harris feature points and local binary patterns. Math. Probl. Eng. **2013**, 619564, 1–12 (2013). https://doi.org/10.1155/2013/619564
27. G. Tahaoglu, G. Ulutas, B. Ustubioglu, V.V. Nabiyev, Improved copy move forgery detection method via L* a* b* color space and enhanced localization technique. Multimed. Tools Appl. **80**, 23419–23456 (2021). https://doi.org/10.1007/s11042-020-10241-9

28. Y. Wu, W. Abd-Almageed, P. Natarajan, Deep matching and validation network: an end-to-end solution to constrained image splicing localization and detection, in *The 25th ACM international conference on Multimedia (MM '17)* (Association for Computing Machinery, 2017), pp. 1480–1502. https://doi.org/10.1145/3123266.3123411
29. Y. Wu, W. Abd-Almageed, P. Natarajan, BusterNet: detecting copy-move image forgery with source/target localization, in *The 15th European Conference on Computer Vision (ECCV)*, pp. 168–184 (2018)
30. A.K. Jaiswal, R. Srivastava, Detection of copy-move forgery in digital image using multi-scale, multi-stage deep learning model. Neural Process. Lett. **54**, 1–26 (2021). https://doi.org/10.1007/s11063-021-10620-9
31. Y. Liu, Q. Guan, X. Zhao, Copy-move forgery detection based on convolutional kernel network. Multimed. Tools Appl. **77**, 18269–18293 (2018). https://doi.org/10.1007/s11042-017-5374-6
32. K. Sunitha, A.N. Krishna, Efficient keypoint based copy move forgery detection method using hybrid feature extraction, in *The 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)* (2020). https://doi.org/10.1109/ICIMIA48430.2020.9074951
33. Y. Peng, W. Ye, Y. Liu, Copy-move tampered image detection based on progressive hybrid features. Laser Optoelectron. Prog. **59**(2), 1–15 (2022). https://doi.org/10.3788/LOP202259.0211001
34. U.A. Khan, M.A. Kaloi, Z.A. Shaikh, A.A. Arain, A hybrid technique for copy-move image forgery detection, in *The 3rd International Conference on Computer and Communication Systems (ICCCS)*, pp. 212–216 (2018). https://doi.org/10.1109/CCOMS.2018.8463337
35. C. Pun, J. Chung, A two-stage localization for copy-move forgery detection. Inf. Sci. **463–464**, 33–55 (2018). https://doi.org/10.1016/j.ins.2018.06.040
36. C. Pun, X.X. Yuan, Bi image forgery detection using adaptive oversegmentation and feature point matching. IEEE Trans. Inf. Forensics Secur. **10**(8), 1705–1716 (2015). https://doi.org/10.1109/TIFS.2015.2423261
37. D. Tralic, I. Zupancic, S. Grgic, M. Grgic, CoMoFoD—new database for copy-move forgery detection, in *The 55th International Symposium ELMAR*, pp. 49–54 (2013)

Publisher's Note