Copy-move Forgery Detection Robust to Various Transformation and Degradation Attacks

Jiehang Deng[1], Jixiang Yang[1], Shaowei Weng[2], Guosheng Gu[1], and Zheng Li[1]
[1] School of Computers, Guangdong University of Technology, Guangzhou, Guangdong 510006 - China
[e-mail: dengjiehang@gdut.edu.cn]
[2] School of Information Engineering, Guangdong University of Technology, Guangzhou,Guangdong 510006 - China
[e-mail: wswweiwei@126.com]
*Corresponding author: Guosheng Gu

Received December 21, 2017; revised March 24, 2018; accepted April 28, 2018; published September 30, 2018

Abstract

Trying to deal with the problem of low robustness of Copy-Move Forgery Detection (CMFD) under various transformation and degradation attacks, a novel CMFD method is proposed in this paper. The main advantages of proposed work include: (1) Discrete Analytical Fourier-Mellin Transform (DAFMT) and Locality Sensitive Hashing (LSH) are combined to extract the block features and detect the potential copy-move pairs; (2) The Euclidian distance is incorporated in the pixel variance to filter out the false potential copy-move pairs in the post-verification step. In addition to extracting the effective features of an image block, the DAMFT has the properties of rotation and scale invariance. Unlike the traditional lexicographic sorting method, LSH is robust to the degradations of Gaussian noise and JEPG compression. Because most of the false copy-move pairs locate closely to each other in the spatial domain or are in the homogeneous regions, the Euclidian distance and pixel variance are employed in the post-verification step. After evaluating the proposed method by the *precision-recall-*F_1 model quantitatively based on the Image Manipulation Dataset (IMD) and Copy-Move Hard Dataset (CMHD), our method outperforms Emam *et al.*'s and Li *et al.*'s works in the *recall* and F_1 aspects.

Keywords: Copy-move forgery detection, Discrete Analytical Fourier-Mellin transform, Locality sensitive hashing, Block variance

1. Introduction

With the great development in the technology of computers, there are numerous digital image processing products, such as Photoshop, ACDSee and GIMP, which are widely applied to difference fields. Their functions become so powerful and simple, that they are convenient for tampering and counterfeiting. The main goal of a tampered image is the alteration of the image information to achieve an unknown purpose. In the past, there were a lot of forgery images appearing in the media, court and scientific journals. Many researchers have devoted more immediate attention to solve the problem of image forgery, and the topic of image authentication has drawn increasing attentions [1]. Copy-move [2] is a most common forgery operation in which at least one snippet of an image is copied and pasted to the other region of the same image for concealing the key information. **Fig. 1** shows a typical example of copy-move forgery, in which the two yellow ellipses represent the copied region and the pasted one. In normal conditions, copy-move operation includes geometrical transformations and post-processing degradation, such as rotation, scaling, JPEG compression and so on. Because the source region has same properties similar to the forgery region, such as textures, noise and illumination, many copy-move forgery detection (CMFD) algorithms would exploit these properties to detect the forgery regions.

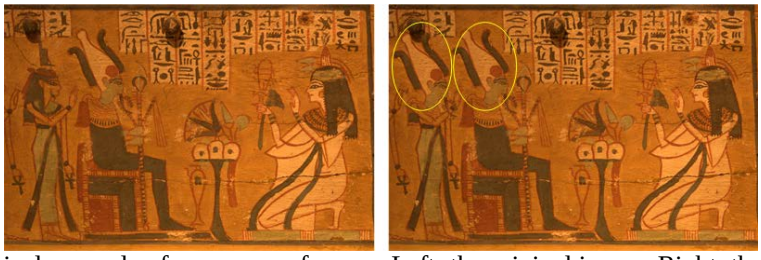


Fig. 1. A typical example of copy move forgery. Left: the original image. Right: the forgery one

The CMFD methods can be roughly divided into three main categories: block-based, keypoint-based and hybrid methods. The block-based methods [3-13] generally extract image features using invariant moment through overlapping block subdivided in rectangular regions. As an alternative to the CMFD, the keypoint-based methods [14-22] extract the features from the whole image. In the third family of techniques, block-based and keypoint-based mehtods are integrated to form the hybrid algorithms [23, 24].

For CMFD, a lot of block-based methods were proposed in the past fifteen years. Quantized Discrete Cosine Transform (DCT) was firstly proposed by Fridrich *et al*. [3] to extract features of an image block. Zhang *et al*. [4] proposed an improved method based on discrete consine transform(DCT) to detect copy move forgery image. Popescu *et al*. [5] have proposed combining Principal Components Analysis (PCA) with DCT for CMFD to reduce computation complexity and improve the performance of the algorithm. Mahdian *et al*. [6] have proposed blur moment invariants to detect the copy move forgery, even if the duplicated region undergoes blur degradation, additive noise. Zhao *et al*. [7] have proposed a method based on Singular Value Decomposition (SVD) and DCT against blur and JPEG compression. Muhammad *et al*. [8] have proposed undecimated Dyadic Wavelet Transform (DyWt). However, when the duplication snippets undergo geometric transformations, such as rotation and scaling, the above-mentioned methods cannot work well, so a lot of researchers have proposed methods with the robustness of anti-rotation and anti-scaling operations. Ryu *et al*.

[9] have proposed a technique based on Zernike moments to detect copy move forgeries. Zernike moments are robust against rotation, additive Gaussian noise, moderate scaling and JPEG compression. But it had a complex kernel, so the method has high computational complexity. In order to surmount the defect of Zernike moments, Polar Harmonic Transforms (PHTs) [10] has been proposed. The kernel function of PHTs is simpler than Zernike moments. In [11], Polar Cosine Transform (PCT) has been proposed to extract image block features, which could address the rotation problem. Eman *et al.* [12] have proposed Polar Complex Exponential Transform (PCET) to extract the circle block features. However, most of block-based methods have inherent drawbacks. They could not play an effective role when the copied snippet is attacked by various transformations and degradation.

In order to reduce the running time and enhance the efficiency, the keypoint-based method is another alternative. In CMFD, a lot of researchers have proposed Scale Invariant Feature Transform (SIFT) [14-20] and Speeded Up Robust Features (SURF) [21, 22]. SIFT and SURF achieves better performance than the DCT, PCET, Zernike moments and PCT in the aspects of processing the geometry transformations effectively. Li *et al.* [14] have proposed a scheme which firstly segments the image into non-overlapping patches for key point extraction. Huang *et al.* [15] extracted SIFT descriptors as image features. Amerini *et al.* [16] have proposed SIFT with Hierarchical clustering to detect the copy move forgery. Zhao *et al.* [17] have proposed a SIFT-based algorithm combining with block-based method to locate the forgery region. Sudhakar *et al.* [18] have proposed a hybrid method which included SIFT and Chan-Veses methods. SIFT is a solution for keypoint-based CMFD and the SURF is the other solution. The differences between SIFT and SURF lie in the post-processing step [2]. Debbarma *et al.* [21] have combined SIFT with SURF to extract image features. Bo *et al.* [22] have used SURF as the single image feature for CMFD. Comparing with the block-based methods extracting features from overlapping blocks, the keypoint-based methods extract features from the whole image. Keypoint-based method achieves great robustness to geometric manipulation in CMFD, even if the duplicated region was attacked under large rotation and scaling transformations. However, the keypoint-based methods used points to mark the forgery regions, which could not represent and locate all forgery snippets. What's more, the keypoint-based methods cannot play an effective role in detecting copy-move forgery with smooth snippets. Therefore, the keypoint-based methods cannot achieve an ideal effect.

To address the above-mentioned problems of block-based and keypoint-based methods, the hybrid methods have been proposed, which extract image features based on keypoint-based methods and apply block-based methods for the forgery regions matting. Pun *et al*. [23] have proposed a scheme integrating both SIFT and Adaptive Over-Segmentation algorithm to detect the copy-move forgery regions. Ardizzone *et al*. [24] have proposed a hybrid scheme which combine the most common keypoint-based detectors with a Delaunay triangulation. The hybrid methods can mark the forgery regions effectively. However, their feature extracting methods are all based on the keypoint-based methods which cannot extract features from the homogenous region effectively.

Although the above methods can detect a lot of forgery regions, they do not work well when the image is attacked by various transformations and degradation. To address these problems, Discrete Analytical Fourier-Mellin transform (DAFMT) [13] is investigated and applied to extracting the image features, which has rotation invariance. A pair of matched features in copy-move forgery regions, is the neareat neighbors. The post-processing operations are used in some pasted reigons, which make the pair of feature transfrom to the approximate near neighbors. Li *et al*.[11] and Emam *et al*.[12] have employed Locality Sensitive Hashing (LSH)

[25] to classify features of overlapping blocks and identify the approximate near neighbors effectivley. Finally, Euclidean distance and block variance are combined to filter out the false copy-move pairs. Comparing with PCT [11] and PCET [12], the image features based on DAFMT are suited for CMFD. And then LSH can effectively classify the image features and match copy move pairs. The post-verification step using the property of false matched pairs can filter out most of false matched pairs. Experiment results demonstrated that the proposed method play the key role in CMFD, even if the forgery image went through geometric transformation and degradation attacks.

In the rest of this paper, the proposed method based on DAFMT, LSH and the post-verification step are given in section 2. Extensive experimental results for CMFD are given in section 3. Conclusion is given in section 4.

2. The proposed method

The process of searching the similar snippets that are cloned and pasted to other regions is called CMFD. In this paper, a novel CMFD method is proposed to detect and locate the forgery regions even when copied regions undergo several kinds of transformations and degradation. These transformations and degradation include rotation, scale, additive Gaussian noise, JPEG compression. The proposed CMFD procedure is depicted in **Fig. 2**, which is interpreted in detail as follows.

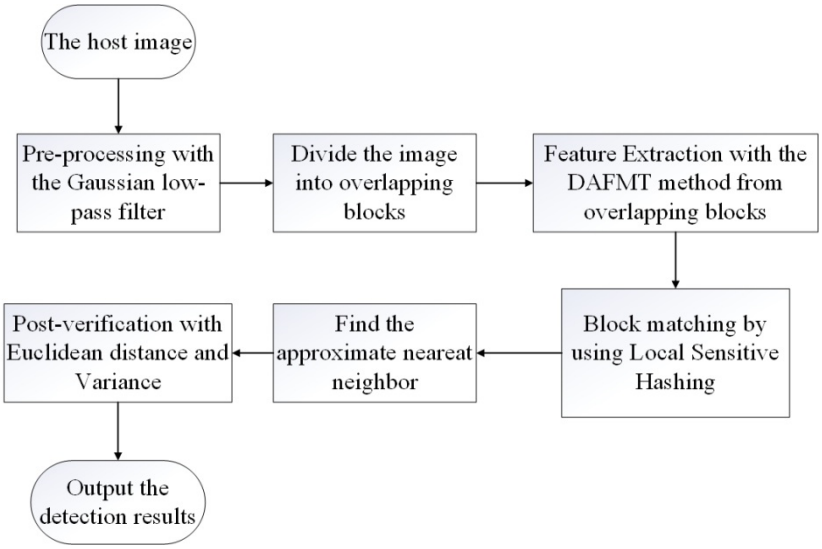


Fig. 2. Copy Move Forgery Detection Procedure

Algorithm Copy-move forgery detection

Input: The host image

Output: The detection result

Step-1: Apply a Gaussian filter to filter out the high frequency components of the image;

Step-2: Divide the image into overlapping blocks with a circular sliding window;

Step-3: Extract features from the divided blocks by DAFMT;

Step-4: Obtain the candidate matched pairs by applying LSH. The LSH can classify the extracted features, and search the approximate near neighbors of each feature;

Step-5: Keep the candidate matched pairs whose Euclidean distance satisfies the condition of threshold T;

Step-6: Keep the blocks whose variance is bigger than the threshold V of variance. These blocks are the suspected forgery blocks;

2.1 Feature extraction using Discrete Analytical Fourier-mellin Transform

Moments with invariant features are widely used for extracting image features, not only in pattern recognition and image watermark but also in CMFD. Particularly, the DAFMT is well known among the various kinds of moments because its image representation is robust against noise, compression, and geometric transformation. Comparing with other invariant moment, DAFMT has two properties which can prove its descriptors to be suitable for CMFD. Firstly, the DAFMT kernel is orthogonal, and therefore, it is better than non-orthogonal moments in CMFD. Secondly, according to the experimental statistic data [13], DAFMT is robust to rotation. In this subsection, the mathematical principle of DAFMT is briefly reviewed and the rotational invariant property is analyzed. Before extracting the image features by DAFMT, the suspicious image needs to be pre-processed for enhancing the detecting effect. Comparing with high frequency components, low frequency components have much greater effect in feature matching step [12]. Therefore, the high frequency noise needs to be suppressed by a low-pass filter. Emam *et al.* [12] apply a Gaussian filter to suppress the high frequency components for image dataset IMD. This filter can preserve the low frequency components effectively. Therefore, the Gaussian filter with the same parameter setting to Emam *et al.*'s filter is applied in this paper. That is, the standard deviation is 0.5 and the template size is 5×5.

Unlike a lot of block-based methods that exploit square template, the Analytical Fourier-Mellin Transform (AFMT) [26] is defined in the polar coordinates, so a sliding circle window with radius R is employed to divide the image into overlapping blocks. The pixels in the same radius are the same distance to the center of the circular block, so the circle block is suit for the rotation invariance extraction. The rectangle, by contrast, doesn't have this advantage. Before extracting the features, the image block $f^d(x,y)$ of the Cartesian coordinates is transformed into polar coordinates $f^\rho(r,\theta)$, firstly. The expression of AFMT with order n and repetition l is given as follows:

$$E_{f,nl}(r,\theta) = \frac{1}{2\pi}\int_0^{\infty}\int_0^{2\pi} f^\rho(r,\theta)K_{nl}^\rho(r,\theta)rd\theta dr \tag{1}$$

$$K_{nl}^\rho(r,\theta) = r^{\sigma-in-2}e^{-il\theta} \tag{2}$$

where n and l are integers whose rang is $[0,\infty]$, $K_{nl}^\rho(r,\theta)$ is the kernel of AFMT in polar coordinates.

In order to obtain rotation invariant for CMFD, the rotation invariant character of AFMT is explored hereafter. Assuming that $f^\rho(r,\theta)$ is rotated α degree around the origin, the rotated image can be expressed as Eq.(3).

$$f_{Rot}^\rho(r,\theta) = f^\rho(r,\theta+\alpha) \tag{3}$$

$$\begin{aligned} E_{f,nl}^{R} &= \frac{1}{2\pi}\int_0^{\infty}\int_0^{2\pi} f_{Rot}^{\rho}(r,\theta)K_{nl}^{\rho}(r,\theta)rdrd\theta \\ &= \frac{1}{2\pi}\int_0^{\infty}\int_0^{2\pi} f^{\rho}(r,\theta+\alpha)K_{nl}^{\rho}(r,\theta)rdrd\theta \\ &= \frac{1}{2\pi}\int_0^{\infty}\int_0^{2\pi} f^{\rho}(r,\theta+\alpha)K_{nl}^{\rho}(r,\theta+\alpha)e^{il\alpha}rdrd(\theta+\alpha) \\ &= E_{f,nl}\cdot e^{il\alpha} \end{aligned} \tag{4}$$

In Eq. (4), the procedure of the image rotation can be separated into the invariant magnitude, i.e. $\left|E_{f,nl}\right|=\left|E_{f,nl}^{R}\right|$, and the variable rotation degree $e^{il\alpha}$. That means the AFMT magnitude remains stable although the block is rotated. Therefore, the AFMT coefficients are used as features to detect the CMFD regions even if the forgery region suffered from rotation transform.

According to the description of Eq. (1), AFMT must be transformed into the discrete space as follows:

$$\begin{aligned} &E_{f,nl}^{'}(x,y) = \frac{1}{2\pi(pixel\_num)}\sum\sum K_{nl}^{d}(x,y)f^{d}(x,y)\ \ s.t.\ x^2+y^2\le R^2 \\ &\rightarrow E_{f,nl}(x,y) = \sum\sum K_{nl}^{d}(x,y)f^{d}(x,y) \end{aligned} \tag{5}$$

In the processing of computing the coefficients of DAFMT, the center of each block is the origin and R=16 is the radius of circular block. The *pixel_num* is the number of the calculated pixels in each block. The $\frac{1}{2\pi(pixel\_num)}$ is a constant number, so it is removed to raise computational efficiency. The value of n and l are chosen as $n+l\le 3, n\ge 0, l\le 2$. $K_{nl}^{d}(x,y)$ is the kernel of AFMT in Cartesian coordinates. An AFMT kernel contains order n and repetation l, so 8 different AFMT kernels have been proposed to extract each circular block feature. And there are three (R/G/B) channels in a colour block. Therefore, 24 (8×3) coefficients are extracted by DAFMT in one block. These with small values of n and l capture the coarse skeleton of the patch, and the others characterize its visual details [11]. In this sense, DAFMT coefficients extracted from different channels can provide a rich representation of the block and can improve the correct detection rate.

2.2 Block matching by using Local Sensitive Hashing

In the above subsection, the block features are extracted by DAFMT. The block features need to be used to find the similar block, because the original region and the forgery one are similar to each other. In the past, lots of researchers employed Nearest Neighbor (NN) to search the similar block features. However, some of the copy-move pairs could not be found out by NN. Let $E_{f,nl}$ be a feature space R^d, ε be a factor which is larger than 0 and less than 1, R_{min} be a distance between the feature vector v and its nearest neighbor. $(1+\varepsilon)$ rather than R_{min} is set as the threshold to identify the similar in Approximate Nearest Neighbor (ANN). Because $(1+\varepsilon)$ is larger than 1, more effective similar features can be identified by ANN with comparing to NN [11]. Furthermore, ANN can remove the curse of dimensionality and improve the running

efficiency, comparing to the lexicographic sorting scheme. Therefore, ANN is employed to search the similar features in this paper.

For ANN searching scheme, LSH is a frequently-used technique. The process of generating one or more hash tables by means of one or more hash functions is called LSH. LSH is widely used in lots of fields effectively, such as fingerprint matching and image retrieval. During the implementation course of LSH, many hash functions are used to hash the feature vectors, in which the identical hash values are selected. This can ensure that the similar features can match together as much as possible. Therefore, LSH is employed in ANN in this paper, also. Since the proposed method detects copy-move forgery image in Euclidean space, hashing functions are applied based on *p*-stable distribution to match the similar blocks. The hash function $h(v)$ with fixed *r* and *a* could be defined as:

$$h(E_{f,nl}) = \left\lfloor \frac{v \cdot E_{f,nl} + b}{w} \right\rfloor \tag{6}$$

where *v* is a two-dimensional random vector complied with a *p*-stable distribution; $v \cdot E_{f,nl}$ represents the result that the image feature vector $E_{f,nl}$ is mapped onto the direction of the random vector *v*; *w* is the width of the hash barrel; *b* is a real number whose range is $[0, w]$ and $\lfloor \cdot \rfloor$ is the floor operation. For acquiring the ANN result, a linear searching scheme is employed to look for all the similar vectors dropping into the same barrel. If the width *w* of hash barrel increase, the possibility that lots of feature vectors dropping into same barrel will be increased.

2.3 Post-verification

In the previous step, a lot of similar pairs are matched as potential pairs. The potential matched pairs are not always the true copy-move forgery pairs, because LSH has the random characteristics and leads to false matched pairs. The false potential pairs occur in the following situations mostly: one is their locations in the image are close to each other; the other is their pixel values are almost the same. Therefore, Euclidean distance is employed to filter out the false potential pairs which are close to each other. The variance of the block is used to filter out the false matched potential pairs whose pixel values are almost the same.

2.3.1 Preliminary filtration step using Euclidean distance

If two potential blocks are adjacent to each other, their structure correlation is highly related. Based on this reason, it is possible that they are identified as forgery pairs by the proposed method. To filter out these false matched pairs, a threshold *T* of Euclidean distance is proposed and defined as follows:

$$T = \begin{cases} \dfrac{M}{100} + \dfrac{N}{100}, & s.t. \ \left(\dfrac{M}{100} + \dfrac{N}{100} \right) > 100 \\ 100, & others \end{cases} \tag{7}$$

where *M* and *N* are the width and height of a suspicious image, respectively. The bigger the image size is, the larger the distance between the copied and pasted regions is. To obtain a

distance threshold according to the image size, Eq. (7) is designed. In Eq. (7), M and N being divided by 100 are attributed to measure the distance between the copied region and pasted region. Based on the experiment statistics, most of the distances in different images are larger than 100 pixels, so we set the shortest distances as 100 pixels.

The similar pairs whose geometric distance is larger than T can be considered as candidate matched forgery pairs. In addition, let b_i and b_j denote the i^{th} and j^{th} blocks being matched. The blocks b_i and b_j are also classified into candidate matches [12] when the following conditions are setisfied: b_i has at least six neighboring blocks matching up with the six neighboring blocks of b_j among eight neighboring blocks of b_i and b_j.

2.3.2 The second filtration step using Variance

The Euclidean distance can filter some false matched features which are adjacent to each other in spacial domain. But, some other pairs are located in homogeneous regions cannot be removed by Euclidean distance. To remove these pairs in the homogeneous regions, variance is introduced to measure the local complexity of the blocks. To this end, a variance threshold V of an image block is proposed in this step. The more homogeneous the image block is, the smaller the variance is. Those candidate pairs are considered as false matched pairs when their variances are less than V.

The value of the threshold V is decided by testing the whole Image Manipulation Dataset (IMD)[2]. The deciding procedure is shown in **Fig. 3** through two representative images. In **Fig. 3**, (a1) and (b1) are original images. (a2), (a3), (a4) and (a5) are the corresponding results when V equals to 10, 52, 100 and 400, respectively. The processed results of original image (b1) are shown from **Fig. 3**-(b2) to (b5). The larger the value of V is, the less the number of the red and blue pixels become. The larger the value of V is, the more the yellow pixels become. As aforementioned above, the red, blue and yellow pixels stand for the false, correct and missing detected regions, respectively. As shown in **Fig. 3**, both the false and missing detected regions become less and the correct detected ones remain larger when V is set at 52, which can remove most of the outliers.

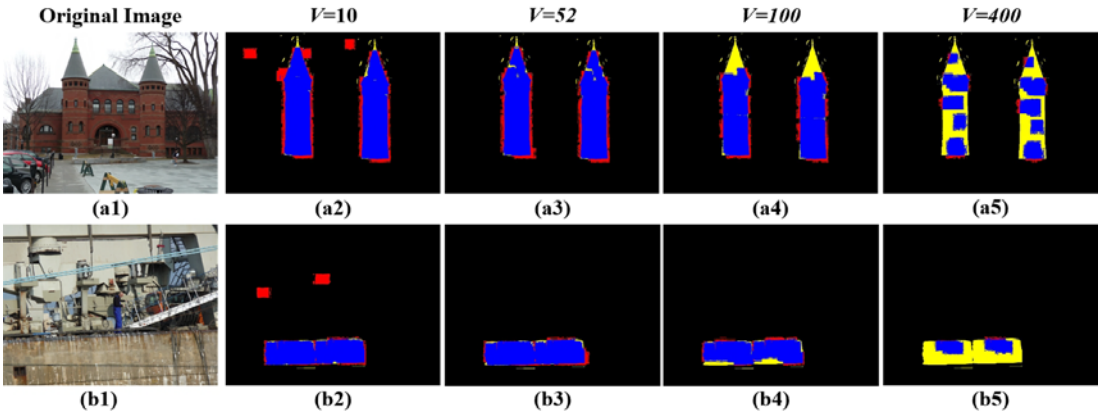


Fig. 3. The experimental results of different variance threshold V.

There are still some small holes and isolate points in the results after processing by using Euclidean distance and variance. These small holes and isolated points are removed by the dilation and erosion operation in this paper.

3. Experiments and Discussion

In this section, experiments are conducted to expound the validations of the proposed method. Comparing with the state-of-the-art methods based on the same dataset, a lot of experimental data support that the proposed method can achieve better effects.

3.1 Datasets and experimental evaluation metrics

In this paper, Image Manipulation Dataset (IMD) [2] and Copy-move Hard Dataset (CMHD) [27] are used as test condition to measure the effectiveness between the proposed method and some state-of-the-art methods. The image datasets include various kinds of scenes and objects. In IMD, 18 bases images with different transformations and degradation are selected. The copied snippets of the images include diverse objects, e.g. sky, persons, buildings, ocean or animals. The images include various kinds of transforms and degradation implemented on the copied snippets, which include geometry transformations, noise and JPEG compression degradations. The geometry transformations include plain, rotation, scaling. The duplicated regions are scaled to different size (e.g., large, medium, or small) and they can be pasted with different ways (e.g., 1-to-1, 1-to-many, and many-to-many). The size of these images is quite large, with average size 3000×2400 pixels. Furthermore, CMHD is also used in the experiments, which comprises 108 copy-move forgery images, with size in the range of 845×634 to 1296×972. CMHD contains three type of copy-move forgery image, namely simple case, rotation transformation with a degree range of -90°–180° and scaling transformation with a scaling factor range of 80%-154%. According to this condition, the two image datasets can provide substantial experimental materials to comprehensively evaluate the proposed method and other state-of-the-art methods. IMD is made the careful classification to the forgery case. For example, in the copy-move forgery with JPEG compression, it is divided into five categories, namely JPEG compression of quality 20, 40, 60, 80 and 100. Therefore, the discussions on the robustness are made in the experiments. Then CMHD isn't divided into different categories in detail, which just contains three types of copy-move forgery images. The performances can only be analyzed generally between the proposed method and the state-of-the-art ones in CMHD.

In order to evaluate the performance of the method at pixel level objectively and particularly [2], a kind of important criteria model, namely Precision Recall model (PRm), is applied in the following experiment. the True Positive (T_p) in blue represented the number of pixels that are correctly detected as forgery. The False Positive (F_p) in red denoted the number of pixels that are incorrectly detected as forgery. The False Negative (F_n) in yellow denoted the number of pixels that are incorrectly detected as genuine. The *precision* equals to $T_p/(T_p + F_p)$ and represents the ratio of the correctly detected pixels to the ground-truth pixels. The *recall* equals to $T_p/(T_p+F_n)$ and represents the ratio of the correctly detected pixels to the total detected pixels.

In the last evaluation step, F_1 score [2] is introduced to synthesize the *precision* and the *recall* for comprehensively evaluating the experimental results, as shown in Eq.(8).

$$F_1 = \frac{2 \cdot precision \cdot recall}{precision \cdot recall} = \frac{2 \cdot T_p}{2 \cdot T_p + F_p + F_n} \tag{8}$$

3.2 Experimental comparisons based on IMD

3.2.1 Verification results of block variance

As mentioned in the above contents, the post-verification step can be divided into two main steps, namely Euclidean distance and variance. In the following, the effect of the post-verification step with or without variance is evaluated based on IMD to prove its essentiality to the forgery detection. **Fig. 4** shows the difference between with and without variance method. The first row shows the host images suffered from copy move forgery. The second row represents the experimental results without the variance processing. The third row denotes the results with the variance processing. In **Fig. 4**, after processing by variance step, the number of false detected points in red drop down dramatically while the true detected points remain almost the same. On the same time, the false negative points in yellow stay stable. It proves that the variance method works well to detect the forgery region more precisely. **Table 1** shows the results of comparison between nonexistence and existence of variance step. It is observed that proposed method with variance step further improve the *precision* from 71.56% to 85.68%. The *recall* and F_1rise from 94.85% and 81.58% to 96.16 to 90.62%, respectively. Therefore, the variance step can guarantee the proposed method achieve much accurate detection results.

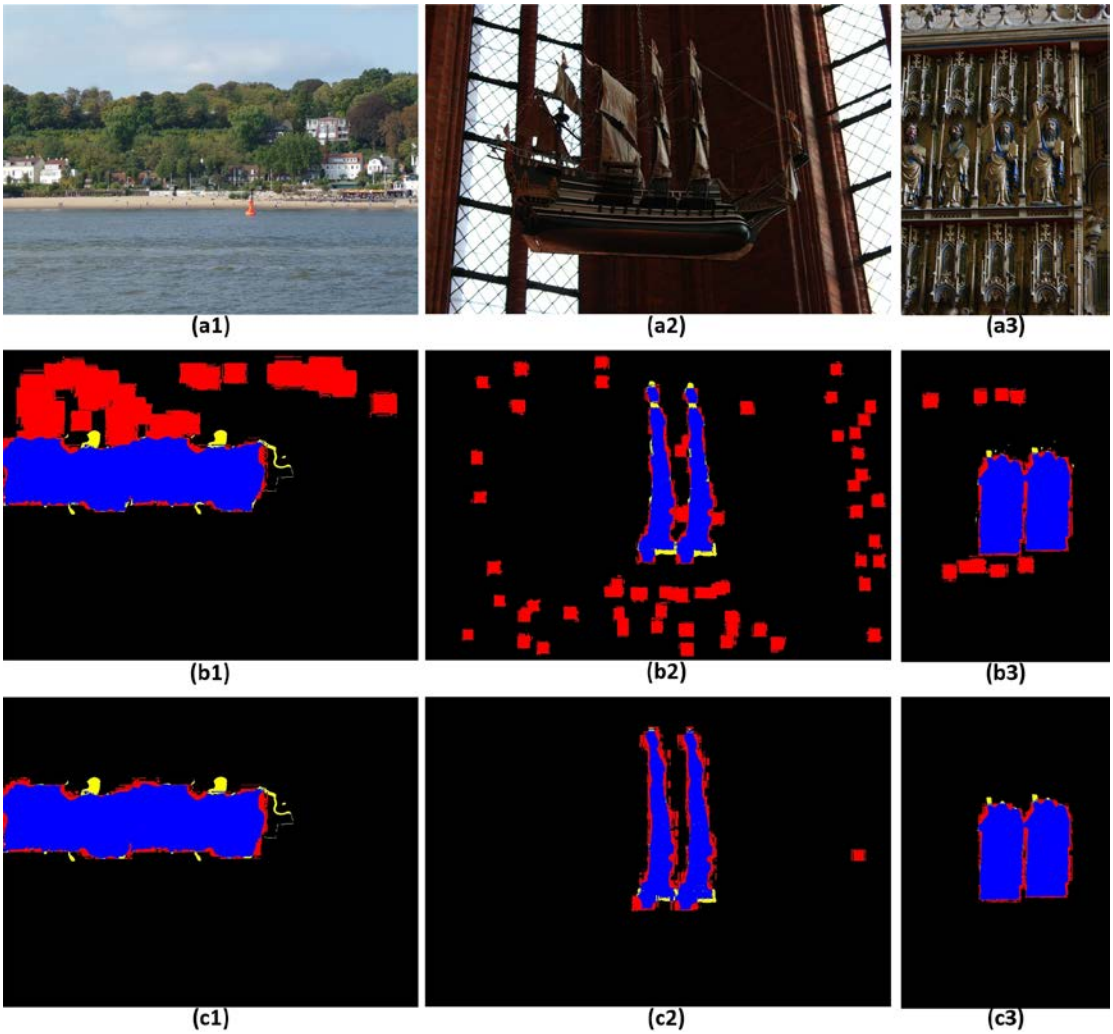


Fig. 4. The comparison between with and without variance method. (a1)~(a3) are the copy-move forgery images; (b1)~(b3) represent the experimental results without using variance method; (c1)~(c3) denote the experimental image with variance method.

Table 1. The comparison of with and without variance method

	Without variance method	With variance method
precision	71.56%	85.68%
recall	94.85%	96.16%
F_1	81.58%	90.62%

3.2.2 Experimental comparisons under plain attack

In this section, the experiments under plain attack are carried out to compare the performance of the proposed and the state-of-the-art methods at pixel level. The state-of-the-art methods include PCET [12] and PCT [11]. To show the experimental results precisely, PRm and F_1 are employed to measure the performance of these methods.

The calculated PRm and F_1 results are plotted in **Fig. 5**. The red, black and blue bars represent results calculated from the proposed, Eman *et al.*'s PCET and Li *et al.*'s PCT methods. As shown in the **Fig. 5**, it is observed that the *precision* (0.920) of our proposed method is higher than PCT but lower than PCET a little bit, while the *recall* (0.906) of our proposed method is higher than both of the PCET and the PCT. In the F_1 aspect, the score obtained by the proposed method is 0.913. It is better than PCET's result about its 10% and is better than PCT's result about its 20%. Hence, except the comparison of *precision* value, the proposed method achieves better performance than those state-of-the-art methods at pixel level. Comparing with PCET and PCT, the ability of representing image feature with DAFMT is better, so the *recall* of the proposed method is higher than theirs. In post-processing step, the Euclidian distance and pixel variance are employed to filter out most of the false matched region. Therefore, the proposed method can obtain satisfactory *precision*. Although the *precision* of the proposed method is less than Eman *et al.*'s results a little, it is more than Li *et al.*'s results about 45%. Therefore, the F_1 score of the proposed method is better than PCET and PCT. According to above analysis, the proposed method outperforms PCET and PCT in the detection of the plain copy-move attack.

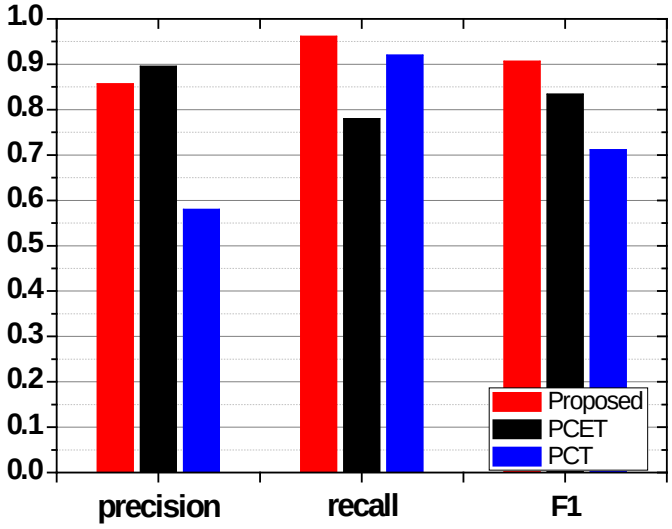


Fig. 5. The comparison between the proposed and other state-of-the-art methods by PRm and F_1 at pixel level for the plain attack. The red, black and blue bars represent PRm and F_1 results coming from the proposed, PCET and PCT methods.

3.2.3 Experimental comparisons under other forgery attacks

In order to comprehensively assess the performance of our proposed method and the state-of-the-art methods, this section shows various kinds of results of copy move forgery detection, such as rotation, scaling, JPEG compression and Gaussian noise. The types and total number of copy move forgery images under the above-mentioned attacks are listed in **Table 2**. For roundly comparing experimental results, plain copy-move forgery images are considered as three kinds of forgeries: rotating an image 0°, resizing the image to 100% and adding Gaussian noise with zero standard deviation.

Table 2. The types of copy move forgeries and total number of experimental images

Types	**rotation angles**	**scaling factors**	**standard deviations of Gaussian noise**	**quality factors of JPEG compression**
Parameters	0°,2°, 10°, 60°, 180°.	93%, 97%, 100%, 101%, 105%, 109%	0, 0.02, 0.04, 0.06, 0.08	20, 40, 60, 80, 100
The number of image	18×5=90	18 × 6 = 108	18 × 5 = 90	18 × 5 = 90

In **Fig. 6**, the experimental results show the robustness of the proposed method with regard to the above-mentioned attacks. **Fig. 6**-(a1) and **Fig. 6**-(a2) show the host images whose copied regions are attacked by the rotation transformations at 10° and 180°, respectively. The corresponding detected results are shown in the **Fig. 6**-(a3) and **Fig. 6**-(a4). The proposed method obtains a great performance. The *precision* of **Fig.6**-(a3) and **Fig. 6**-(a4) is 83.78% and 80.35%, while the *recall* is 96.79% and 93.56%, respectively. **Fig. 6**-(b1) and **Fig. 6**-(b2) show the host images whose copy snippets were attacked by the scaling transforms with 93% and 109% scaling factor, respectively. The corresponding detected results are shown in the **Fig. 6**-(b3) and **Fig. 6**-(b4).The proposed method can precisely locate the copied regions and forgery regions. The *precision* of **Fig. 6**-(b3) and **Fig. 6**-(b4) is 80.75% and 94.39%, while the *recall* is 93.39% and 98%, respectively. **Fig. 6**-(c1) and **Fig. 6**-(c2) show the host images whose copied regions are added Gaussian noise with standard deviation of 0.02 and 0.08, respectively. The corresponding detected results are shown in the **Fig. 6**-(c3) and **Fig. 6**-(c4).The *precision* of **Fig. 6**-(c3) and **Fig. 6**-(c4) is 84.95% and 86.34%, while the *recall* is 96.53% and 97.30%, respectively. **Fig. 6**-(d1) and **Fig. 6**-(d2) show the host images which are attacked by JPEG compression with quality factor of 20 and 80, respectively. The corresponding detected results are shown in the **Fig. 6**-(d3) and **Fig. 6**-(d4).The *precision* of **Fig. 6**-(d3) and **Fig. 6**-(d4) is 80.62% and 88.67%, while the *recall* is 91.24% and 90.48%, respectively. The *recall* for all the above-detected results is better than 90%. Specially, for the scaling transformation with 109% factor and degraded by Gaussian noise with standard deviation of 0.08, the *recall* almost reaches 100%. That is the proposed method can detect all forgery regions almost without losing any genuine regions in these cases. The *precision* for all the above-detected results is better than 80%. That is, the proposed method works well to recognize all the forgery regions with the rate of incorrectly detected as forgery less than 20% for the vast majority of the forgery snippets.

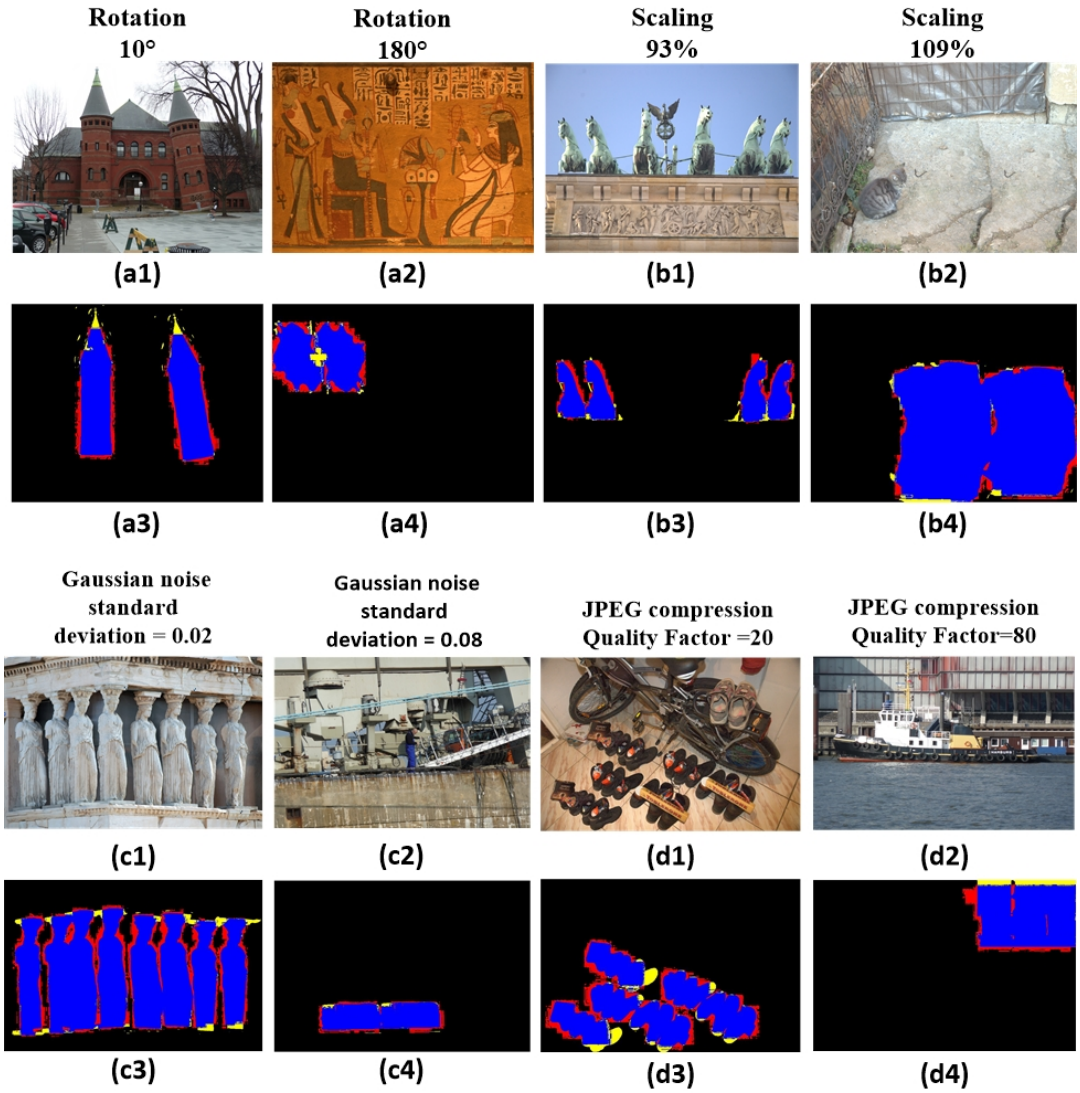


Fig. 6. The experimental results of CMFD of our proposed method.(a1), (a2), (b1), (b2), (c1), (c2), (d1), (d2)denote the host images under various kinds of attacks. (a3), (a4), (b3), (b4), (c3), (c4), (d3), (d4) show the experimental results under rotation transforms, scaling transforms, added Gaussian noise and JPEG compression.

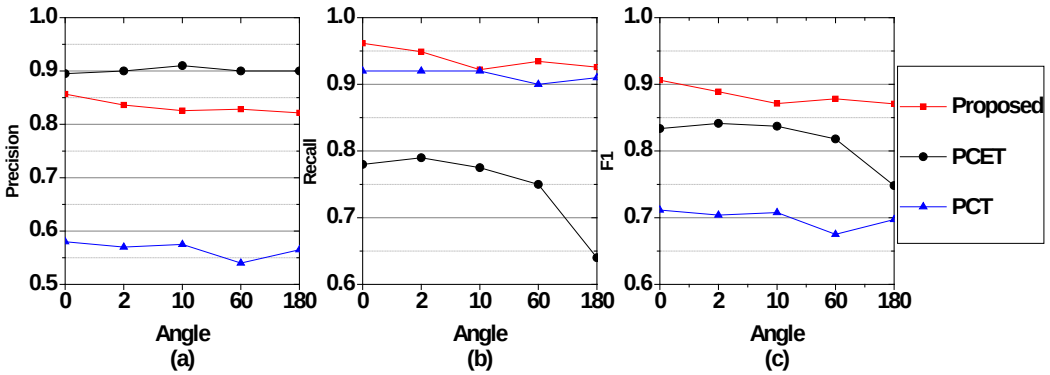


Fig. 7. The comparison result of above method under rotation transform

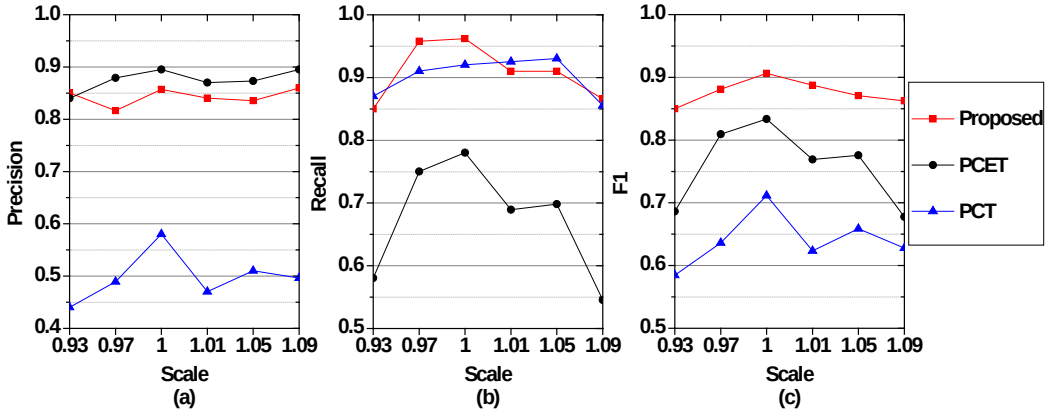


Fig. 8. The comparison result of above method under scaling transform

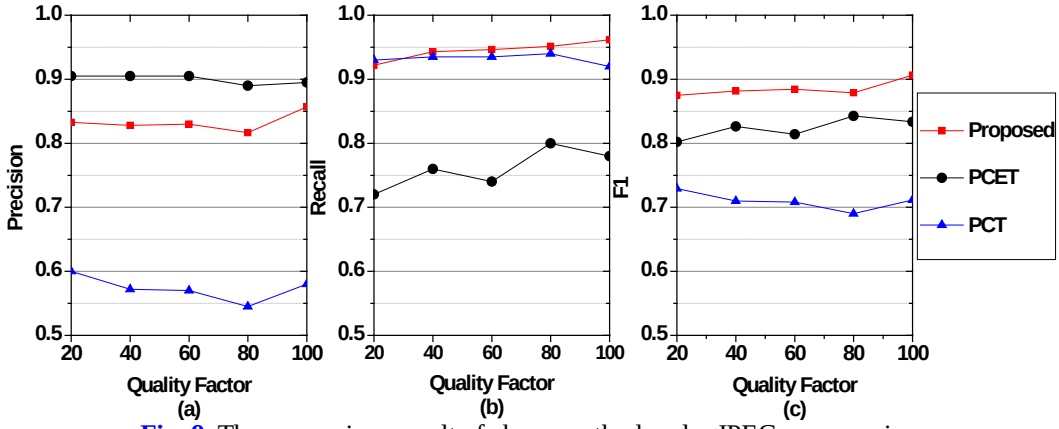


Fig. 9. The comparison result of above method under JPEG compression

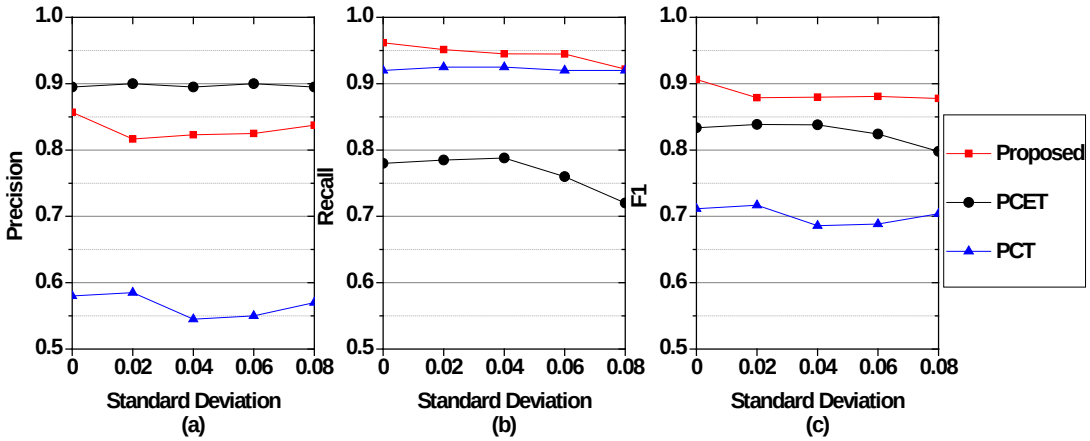


Fig. 10. The comparison result of above method under additive Gaussian noise

In the following content, PCT [11], PCET [12] and the proposed method are applied to evaluating their performances under various kinds of forgery attacks, such as rotation transform, scaling transform, JPEG compression and Gaussian noise. **Figs. 7-10** show the

comparing results of *precision*, *recall* and F_1 of all above methods under each kind of forgery attack. The x-axis in **Fig.7** represents the rotation angle, **Fig.8** represents the scale factor, **Fig. 9** represents the quality factor of JPEG compression and **Fig.10** represents the standard deviation of Gaussian noise. The red square represents the experimental results of our proposed method. The black circle and blue triangle represent the experimental results of PCET and PCT, respectively.

In **Fig. 7~10**, the subgraph (a) shows the precession results of the proposed scheme compared with the existing methods for various transformation and degradation attacks. It can be easily observed that the *precesion* of both the proposed method and PCET work much better than PCT. That is, the regions incorrectly detected as forgery from the results of the proposed method and PCET are much less than that of PCT. Furthermore, both the *precision* values of our proposed method and PCET are better than 0.8, some of them even close to 0.9, which shows most of the forgery regions can be located precisely.

At the same time, the subgraph (b) in **Fig. 7~10** shows the *recall* results of the proposed method compared with the existing ones. It can be observed that the *recall* results of both the proposed method and PCT are much better than that of PCET when under various attacks. The advantages of both our proposed method and PCT can be shown in two aspects: one is high score of *recall*, the other is the stability. In terms of the *recall* score, most of the results of both the proposed method and PCT are better than 0.9, some of them even close to 1.0. On the contrary, the results of PCET are only close to 0.8, some of them even below 0.6. With respect to the stability, the *recall* results of both the proposed method and PCT change a little under various attacks, while the results of PCET vibrate violently.

The subgraph (c) in **Fig. 7~10** shows the F_1 scores, which combine both the *precision* and *recall* into a single value. These subgraphs indicate that the F_1 scores of the proposed method is better than that of PCET and much better than that of PCT for all forgery attacks. Specially, only the proposed method can achieve the F_1 score almost reaching 0.9. The score of PCET stayed close to 0.8, while PCT kept close to 0.65. That is, the proposed method can almost identify all the forgery pixels and outperform PCET and PCT when the images are under attack of various transformation and degradation attacks.

In summary, the most of *recall* of the proposed method larger 0.9 against all kinds of attacks mentioned above. What is more, the *recall* of the proposed method is highest among the comparative methods. The F_1 score synthesizes *precision* and *recall*, so that it can veritably evaluate the performance of methods. The F_1 score of the method is always higher than those of PCET and PCT. There are two reasons why the proposed method can achieve best performance in terms of *recall* and F_1 for various transformations and degradations mentioned above. First, the proposed method uses a circular image block to detect forgery images. If the block contains a part of a forgery snippet, the whole window is considered to be a forgery snippet, so some of the detected regions include a few false detected pixels in the edge of the detected snippets. That is why the *precision* scores of PCET are higher a little than those of the proposed method in some occasions. Second, the coefficients of DAFMT are more effective to extract the features of an image than those of PCET and PCT.

3.3 Experimental comparisons based on CMHD

In order to verify the validation of the proposed method further, the comparisons between PCET, PCT and the proposed methods are conducted using the CMHD. The CMHD contains various kinds of rotation and scaling transformation. To visually demonstrate the results of the proposed method, an illustration of detection results is showed in **Fig. 11**. **Fig.11**-(a1) shows the host image with simple case forgery. The *precision* of the corresponding result showed in

Fig.11-(a2) is 0.8136, while the *recall* is 0.9259. **Fig.11**-(b1) and **Fig.11**-(c1) show the host image with rotation transformation. The *precision* of **Fig.11**-(b2) and **Fig.11**-(c2) is 0.8476 and 0.7628, while the *recall* of **Fig.11**-(b2) and **Fig.11**-(c2) is 0.9908 and 0.8952, respectively. **Fig.11**-(d1) shows the host image with scaling transformation. The *precision* of the corresponding result is 0.7387, while the *recall* is 0.99. As shown in below images, the proposed method works well to identify all the forgery regions.

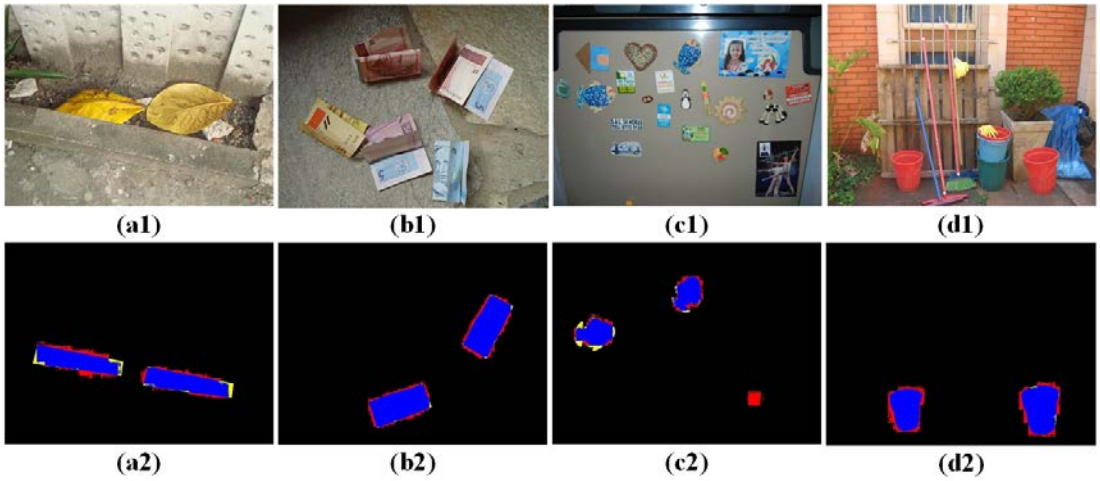


Fig. 11. The detected results of the proposed method. (a1)~(d1) denote the forgery images. (a2), (b2), (c2) and (d2) denote the detected results.

To measure the performance of the proposed methods with other approaches quantitatively, *precision*, *recall* and F_1 from different results are plotted in **Fig. 12**. The red, black and blue bars represent results calculated from the proposed, Eman *et al.*'s PCET and Li *et al.*'s PCT methods, respectively. As shown in **Fig. 12**, the *precision* (0.7385) of the proposed method is highest than the state-of-the-art, while the *recall* (0.7328) of the proposed method lower than the PCT method a little bit but higher than the PCET method. Therefore, the F_1 score (0.7357) achieved by the proposed method is best among these methods. The CMHD contain three types of forgery (simple case, rotation and scaling) in one dataset, so that it is more practical to verify the performance of the forgery detection methods. Except the *recall* value of the proposed method being lower than the PCT's result, the proposed method achieve better and more stable performance in *precision* and F_1 score among the state-of-the-art methods. Therefore, the proposed method is much more suitable for applying to reality.

By comparing the experimental results between IMD and CMHD, F_1 scores from IMD are larger than that from CMHD for all degradation situations. In some CMHD images, the textures, structures and color of the forgery regions are similar to the backgrounds. The proposed method cannot detect all the forgery regions effectively, and have lots of false detecting pixels in these images. That causes *precision* and *recall* become low scores in CMHD. Therefore, F_1 scores is larger in IMD than CMHD.

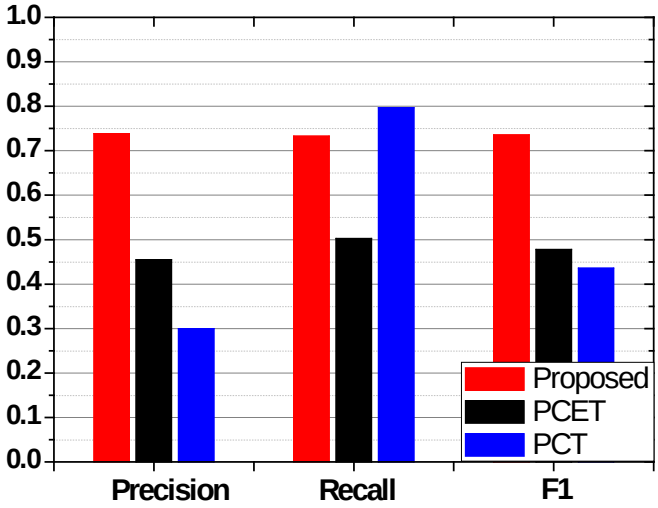


Fig. 12. The comparison between the proposed and the state-of-the-art methods by PRm and F_1 based on CMHD. The red, black and blue bars represent PRm and F_1 results coming from the proposed, Eman *et al.*'s PCET and Li *et al.*'s PCT methods.

4. Conclusion

With fast development of the image process technology, image authentication has been an important topic. In this paper, a novel algorithm for CMFD using the DAFMT, LSH, Euclidian distance and pixel variance is proposed. The proposed method is robust to various attacks. The DAFMT possesses the rotation and slight scaling invariance, so it is able to resist attacks based on rotation and scaling. And the LSH is utilized to solve the problem of similar feature identification. In order to make further improvement on the *precision* of the proposed method at pixel level, the post-verification step is applied to filtering out the false matched features. The experimental results based on IMD and CMHD show that the proposed detection scheme achieved remarkable performances and outperforms PCET and PCT for CMFD in terms of *recall* and F_1. In particular, the experimental results verified that the Euclidian distance and pixel variance are able to filter out most of false matched features and improve *precision* for experiments. On account of its simplicity, it can be widely applied to other CMFD schemes.

Acknowledge

This work is supported by the National Nature Science Foundation of China (No. 61201393, No. 61571139 and No. 61202267), the Science and Technology Planning Project of Guangdong Province (No. 2017A050501035) and Star of Pearl River on Science and Technology of Guangzhou (No. 2014J2200085).

References

[1] H. Farid, "Image forgery detection," *IEEE Signal processing magazine*, vol. 26, no. 2, pp. 16-25, March, 2009. Article (CrossRef Link)

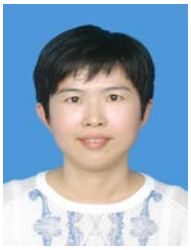
[2] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on information forensics and security*, vol. 7, no. 6, pp. 1841-1854, September, 2012. Article (CrossRef Link)

[3] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," in *Proc. of 3rd Digital Forensic Research Workshop*, August 6-8, 2003. Article (CrossRef Link)
[4] Z. Zhang, D. Wang, C. Wang, and X. Zhou, "Detecting Copy-move Forgeries in Images Based on DCT and Main Transfer Vectors," *KSII Transactions on Internet & Information Systems*, vol. 11, no. 9, pp. 4567-4587, September, 2017. Article (CrossRef Link)
[5] A. Popescu, and H. Farid, "Exposing digital forgeries by detecting duplicated image region," Department of Computer Science, Dartmouth College, *Technology Report TR2004-515*, 2004. Article(CrossRef Link)
[6] B. Mahdian, and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic science international*, vol. 171, no. 2, pp. 180-189, September, 2007. Article (CrossRef Link)
[7] J. Zhao, and J. Guo, "Passive forensics for copy-move image forgery using a method based on DCT and SVD," *Forensic science international*, vol. 233, no. 1, pp. 158-166, December, 2013. Article (CrossRef Link)
[8] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," *Digital Investigation*, vol. 9, no. 1, pp. 49-57, June, 2012. Article (CrossRef Link)
[9] S.-J. Ryu, M. Kirchner, M.-J. Lee, and H.-K. Lee, "Rotation invariant localization of duplicated image regions based on Zernike moments," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1355-1370, July, 2013. Article (CrossRef Link)
[10] P.-T. Yap, X. Jiang, and A. C. Kot, "Two-dimensional polar harmonic transforms for invariant image representation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 7, pp. 1259-1270, July, 2010. Article (CrossRef Link)
[11] Y. Li, "Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching," *Forensic science international*, vol. 224, no. 1, pp. 59-67, January, 2013. Article (CrossRef Link)
[12] M. Emam, Q. Han, and X. M. Niu, "PCET based copy-move forgery detection in images under geometric transforms," *Multimedia Tools and Applications*, vol. 75, no. 18, pp. 11513-11527, September, 2016. Article (CrossRef Link)
[13] J. Zhong, and Y. Gan, "Detection of copy–move forgery using discrete analytical Fourier–Mellin transform," *Nonlinear Dynamics*, vol. 84, no. 1, pp. 189-202, April, 2016. Article (CrossRef Link)
[14] J. Li, X. Li, B. Yang, and X. Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 507-518, March, 2015. Article (CrossRef Link)
[15] H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in *Proc. of 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, vol. 2, pp. 272-276, December 19-20, 2008. Article (CrossRef Link)
[16] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099-1110, September, 2011. Article (CrossRef Link)
[17] F. Zhao, R. Zhang, H. Guo, and Y. Zhang, "Effective digital image copy-move location algorithm robust to geometric transformations," in *Proc. of 2015 IEEE International Conference on Signal Processing, Communications and Computing*, pp. 1-5, September 19-22, 2015. Article (CrossRef Link)
[18] K. Sudhakar, V. Sandeep, and S. Kulkarni, "Speeding-up SIFT based copy move forgery detection using level set approach," in *Proc. of International Conference on Advances in Electronics, Computers and Communications*, pp. 1-6, October 10-11, 2014. Article (CrossRef Link)
[19] L. K. Bhullar, S. Budhiraja, and A. Dhindsa, "DWT and SIFT based Passive Copy-Move Forgery Detection," *International Journal of Computer Applications*, vol. 95, no. 23, pp. 14-18, June, 2014. Article (CrossRef Link)
[20] N. Yadav, and R. Kapdi, "Copy move forgery detection using SIFT and GMM," in *Proc. of 5th Nirma University International Conference on Engineering*, pp. 1-4, November 26-28, 2015. Article (CrossRef Link)

[21] S. Debbarma, A. B. Singh, and K. M. Singh, "Keypoints based copy-move forgery detection of digital images," in *Proc. of International Conference on Informatics, Electronics & Vision*, pp. 1-5, May 23-24, 2014. Article (CrossRef Link)
[22] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in *Proc. of International Conference on Multimedia information networking and security*, pp. 889-892, Novenber 4-6, 2010. Article (CrossRef Link)
[23] C.-M. Pun, X.-C. Yuan, and X.-L. Bi, "Image forgery detection using adaptive oversegmentation and feature point matching," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1705-1716, April, 2015. Article (CrossRef Link)
[24] E. Ardizzone, A. Bruno, and G. Mazzola, "Copy–move forgery detection by matching triangles of keypoints," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2084-2094, October, 2015. Article (CrossRef Link)
[25] M. Datar, N. Immorlica, P. Indyk, and V. S. Mirrokni, "Locality-sensitive hashing scheme based on p-stable distributions," in *Proc. of the 20th annual symposium on Computational geometry*, pp. 253-262, June 08-11, 2004. Article (CrossRef Link)
[26] M. Sellami, and F. Ghorbel, "An invariant similarity registration algorithm based on the analytical fourier-mellin transform," in *Proc. of the 20th European conference on Signal Processing*, pp. 390-394, August 27-31, 2012. Article (CrossRef Link)
[27] E. Silva, T. Carvalho, A. Ferreira, and A. Rocha, "Going deeper into copy-move forgery detection: Exploring image telltales via multi-scale analysis and voting processes," *Journal of Visual Communication and Image Representation*, vol. 29, pp. 16-32, May, 2015. Article (CrossRef Link)

Jiehang Deng received the B.S. and Ms. degrees in 2002 and 2005 from Xi'an University of Technology, China, the Ph.D. degree in 2009 from University of Fukui, Japan. Now he is an Associate Professor in the School of Computers, Guangdong University of Technology, China. His research interest includes image processing and pattern recognition.

Jixiang Yang received the B.S. degree in 2016 from Guangdong University of Foreign Studies South China Business College , China. He is currently pursuing his M.S. degree in the School of Computers, at Guangdong University of Technology, China. His research interest includes image processing and pattern recognition.



Shaowei Weng received her Ph.D. degree from the Institute of Information Science at Beijing Jiaotong University in July 2009. She is currently an associate professor in the School of Information Engineering at Guangdong University of Technology. Her research interests include image processing, data hiding and digital watermarking, pattern recognition, computer vision, etc. Now she is in charge of a NSFC (Natural Science Foundation of China) project. In addition, she participates in 973 and 863 projects as the backbone. She publishes more than 20 papers, and applies two national patents.

Guosheng Gu received the M.S. Degree in Applied Mathematics from South China Normal University, Guangzhou, China, in 2004 and the Ph. D. Degree in Computer Application Technology from South China University of Technology, Guangzhou, China, in 2007. Currently, he is a teacher at School of Computers, Guangdong University of Technology, Guangzhou, China. His research interests include multimedia information security and image processing.

Zheng Li received his Ph.D. from Sun Yat-Sen University in 2008, and finished a post-doctoral program in 2010. He is now a lecturer at the School of Computers in Guangdong University of Technology. His main research interests are computer graphics and image processing.