Effective Medical Image Copy-Move Forgery Localization Based on Texture Descriptor

Jiaqi Shi, Gang Wang(✉), Ming Su, and Xiaoguang Liu

College of CS, TJ Key Lab of NDST, Nankai University, Tianjin, China
{shijq,wgzwp,suming,liuxg}@nbjl.nankai.edu.cn

Abstract. Medical images are vulnerable to be maliciously tampered during network transmission, affecting diagnosis of doctors. Moreover, some images in medical research papers are intentionally manipulated, which reduce the credibility of the conclusions. Therefore, it is essential to research an effective and robust algorithm for medical image tamper detection ans localization. In this paper, we propose a copy-move forgery localization algorithm for medical images called MITD-CMFL. Due to texture structure information is complex and important for medical images, we obtain textural images from noise-reduced images by utilizing texture descriptor to gain more accurate features. It is difficult to extract a sufficient number of feature points with strong representation ability in smooth regions to characterize textures, we extract SIFT keypoints in texture images and decrease the contrast threshold. The experiments conducted on 2,898 tampered breast cancer images randomly selected from DDSM dataset show the pixel-level F_1 of MITD-CMFL reaches up to 95.07% under plain copy-move attack, and the method has superior performance even under typical image transformations compared to the state-of-the-art algorithms.

Keywords: Medical images · Copy-move · Forgery localization · Texture · DDSM dataset

1 Introduction

The telemedicine system is rapidly emerging with the vigorous development of computer networks. Through this system, doctors can judge health status of their patients according to the digital medical images. Especially modern image editing software have been able to achieve the degree of realism, sensitive information of patients in the telemedicine system may be maliciously tampered during network transmission. The lesion regions may be spread or covered up,

This work is partially supported by National Science Foundation of China (61872201, 61702521, U1833114); Science and Technology Development Plan of Tianjin (18ZXZNGX00140, 18ZXZNGX00200).

S. Goel et al. (Eds.): ICDF2C 2020, LNICST 351, pp. 62–77, 2021.
https://doi.org/10.1007/978-3-030-68734-2_4

causing doctors to misdiagnose. Furthermore, from 1995 to 2004, 20,621 medical research papers published in 40 different journals in the fields of microbiology, immunology, cancer biology, and general biology, 3.8% of the papers contained problematic figures, with at least half exhibiting features suggestive of deliberate manipulations [3]. If the medical images in scientific papers are honest wrong or intentional falsification, it will make unscientific conclusions, reduce the credibility of the articles, and seriously affect the integrity of the authors. Based on the above two points, it is significant to identify the authenticity and locate tampering regions of medical images. Since medical images involve smoother regions and more complex texture structure information compared with nature images, the accuracy and practicality of medical image tamper detection and localization technologies still face significant challenges.

Digital image forensics methods are divided into *active tampering* and *passive tampering*. In the literature, most of the medical image tampering localization algorithms utilize the watermarking technique in active tampering [7,16,27,29]. Although the watermarking forensics methods achieve the goal of pixel-level forgery localization, the watermarking is embedded in the medical image in the form of additional information, which impairs the visual quality of the image. More importantly, doctors may misdiagnose and endanger the health status of patients. Even in reversible watermarking, additional preprocessing steps are required.

There are many existing passive tampering methods, where *copy-move* is one common manipulation which refers to duplicate one or more areas to other locations in the same image in order to conceal or duplicate some information. The copied areas may be rotated or scaled before pasting. The forgery detection methods for copy-move are divided into three groups: *blocked-based* [2,5,6,8,14,17,19,21,24,26,32], *keypoint-based* [1,4,11,13,15,18,22,28], and *keypoint-segmentation-based* [12,20,30,31]. For the block-based copy-move forgery detection algorithms, the original images are first divided into overlapping regular image blocks, then features are extracted separately for each block. At present, common block features include Discrete Cosine Transform (DCT) [8,26], Discrete Wavelet Transform (DWT) [17], Principal Component Analysis (PCA) [19], Singular Value Decomposition (SVD) [32], and other approaches. However, the robustness of these features are unsatisfactory to image scaling and rotation. Techniques based on circular harmonic transformation, like Zernike moment [21], Polar Cosine Transform (PCT) [14], Log Polar Transformation [24], Fourier-Merlin Transform [2], are performed well in rotation and scale invariant, which further improve the robustness of the block-based forgery detection approaches. In order to achieve higher robustness, Davide et al. proposed a fast approximation nearest neighbour search algorithm [6] suitable for computing image dense fields, but taking longer processing times. The keypoint-based methods are more robust to geometric attacks. The Scale-Invariant Feature Transform (SIFT) is the classic and popular keypoint extraction method [1,4,11], but has a higher computational cost. Many approaches improved the detection speed by improving SIFT algorithm [22,28]. Both SIFT algorithm and

improved SIFT algorithm generally have a disadvantage that they cannot extract large and accurate keypoints when the regions are small or smooth. Li et al. [13] solved this problem well by lowering SIFT contrast threshold and rescaling the input image size. In recent years, the algorithms combining block-based and keypoint-based technologies have emerged, which avoid the high computational complexity of block-based technologies and the low recall rate of keypoint-based technologies. [20] integrated image segmentation and SIFT algorithm for the first time. Mohsen et al. [30] combined with PCT features and Simple Linear Iterative Clustering (SLIC) image segmentation, which located tampering regions more accurately. Li et al. [12] segmented the image into non-overlapping blocks and performed copy-move forgery detection algorithm in two stages.

The forgery detection methods mentioned above are all directed at natural images, which are not good at medical images. Medical images are smoother than natural images, whose texture and structure information is significant. The general forensic approaches perform normally when detecting smooth regions, and they can not extract high discriminating features in complex texture structures. There are currently few articles devoted to detecting medical images [9,23,25]. Surbhi et al. [23] located image copy-move forged regions by dividing medical images into overlapping blocks and calculating the Central Symmetric Local Binary Pattern of each block as the features, but the method could not resist geometric attacks. Guzin et al. [25] extracted the medical image texture information by using the Local Binary Pattern Rotational Invariant (LBPROT), and extracted SIFT feature points in the texture image for matching the copy-move regions. Ahmed et al. [9] proposed a medical image forgery detection system which used Wiener-filter to extract noise maps from images and utilized multi-resolution regression filters on noise maps. Unfortunately, the system only detects whether the medical image has been tampered with and cannot locate the tamper regions. Due to the particularity of medical images and the low applicability of existing tamper detection approaches, developing a forgery detection scheme suitable for medical images is imperative.

In this paper, we propose an efficient and robust copy-move forgery localization scheme for medical images combining image blocks and keypoints. The main contributions are as follows:

- We obtain texture images by applying LBPROT texture descriptor to highlight texture structural information of medical images.
- We decrease the contrast threshold of SIFT and extract SIFT keypoints in LBPROT images to ensure that plenty of feature points which have high discrimination in smooth regions can be extracted.
- Experimental results on the forged DDSM dataset demonstrate that the proposed MITD-CMFL achieves higher F_1 compared with the existing schemes, even under rotation, scaling, adding Gaussian noise, and JPEG compression.

The remainder of this paper is organized as follows. A novel forgery detection and localization method called MITD-CMFL is detailed in Sect. 2. Section 3 analyzes experimental results and performance comparisons. Finally, the conclusion is in Sect. 4.

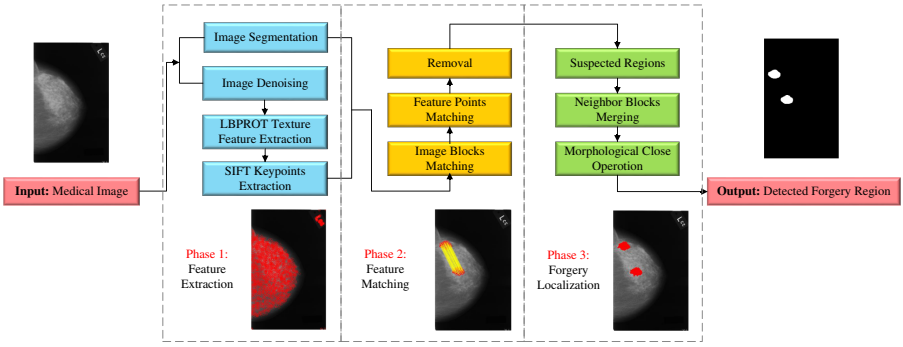


Fig. 1. Framework of the proposed MITD-CMFL.

2 Proposed Method

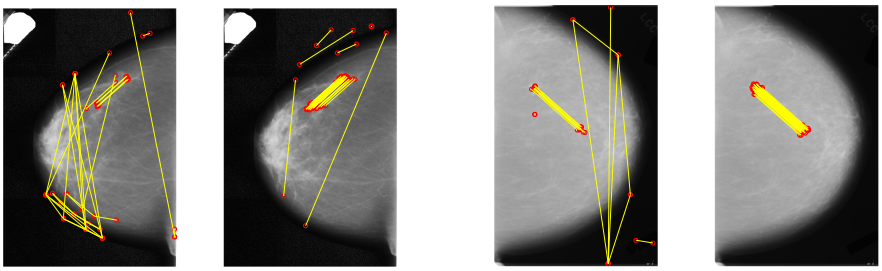
The algorithm MITD-CMFL follows the classic image forgery detection workflow. The process framework is shown in Fig. 1. It is roughly divided into three parts: feature extraction, feature matching, and forgery localization.

2.1 Feature Extraction

Feature extraction is a key step in our method. The quality of feature discrimination directly affects the accuracy of forgery detection and localization, especially for medical images with rich texture information. The proposed MITD-CMFL extracts texture feature points on the original image while segmenting this image into small patches.

Image Segmentation. We utilize SLIC method to segment the medical image into non-overlapping and irregular superpixel patches according to the texture structure and content characteristics, the obtained patches are meaningful and follow the boundary well. The SLIC initial sizes of different images are different. In general, the proper initial size of the patches is important to gain convincing forgery detection results for different shapes of forgery regions. When the initial size is too small, it will have a large computational expense; otherwise, the forgery detection results will not be sufficiently accurate. We adjust the initial size of superpixel according to the image size, which can achieve balances between localization accuracy and computational cost.

Image Denoising. In reality, medical images are often affected by imaging equipment and external environmental noise during acquisition, conversion, and transmission, resulting in degradation. Most real medical images are noisy images. The medical image to be tested is subjected to mean filtering, which eliminates irrelevant information and extracts useful image features.



(a) (b) (c) (d)

Fig. 2. (a) and (c): SIFT keypoints extracted from original medical images; (b) and (d): SIFT keypoints extracted from LBPROT texture images.

LBPROT Texture Feature Extraction. Noise reduction results in loss of information such as texture and edges, but LBPROT can enhance images and increase the contrast between foreground and background so that creating a relatively clean input for the subsequent extraction of SIFT features and achieving better detection results.

Doctors diagnose the disease through image texture analysis. The texture information of the image cannot be ignored in medical image forgery detection. On the contrary, the complex texture structure information helps the forgery localization to be more precise. It is a serious challenge that how to extract high discriminating features in smooth and texture-rich medical images. LBPROT can extract the texture information of smooth regions from medical images effectively. As shown in Fig. 2(a) and Fig. 2(c), these pictures are obtained by directly extracting SIFT keypoints in the original medical images and then applying simple threshold matching. It can be seen that there are some mismatched feature points and the number of feature points that are correctly matched is not much. Figure 2(b) and Fig. 2(d) show SIFT keypoints extracted and matched in the LBPROT texture map. Since LBPROT can enhance the texture structure information, the feature points can be matched more accurately and in larger quantities in contrast.

SIFT Keypoints Extraction. LBP operator eliminates the problem of lighting changes to a certain extent, and the low dimension of texture features makes the calculation fast. The LBPROT makes the LBP operator more robust by introducing a rotation invariant definition. But it also makes the LBP lose the direction information. We need to address this shortcoming to ensure the accuracy and robustness of the proposed algorithm. Due to the SIFT algorithm has direction information and has excellent robustness against various attacks, we combine SIFT keypoints to characterize image blocks which overcome the shortcomings of LBPROT. SIFT and LBPROT can complement each other which both are indispensable to ensure the accuracy and robustness of the algorithm.

In the proposed MITD-CMFL, each image block consists of a set of SIFT feature points. Because of the rich texture information of medical images, the SIFT algorithm is applied to the LBPROT texture image to extract feature points, so that the obtained keypoints have higher ability to represent image texture information and stronger discrimination. Medical images are smoother compared with nature images, in smooth areas, the extreme contrast values are often very low. Any extreme value with a contrast value less than the threshold is rejected as the final SIFT keypoint. As a result, the number of SIFT keypoints detected in smooth areas will be reduced. A small number of feature points obviously cannot be accurately located in forged regions. To guarantee that a sufficient number of feature points can be generated in smooth regions, we decrease the SIFT contrast threshold (set to 0.6 in our experiments), allowing for a large number of extreme values with low contrast values.

2.2 Feature Matching

In this subsection, we propose a simple feature matching scheme. Typically, our method comprises three steps.

Step 1): we match the SIFT keypoints extracted from the LBPROT texture image with the superpixel blocks obtained by SLIC segmentation according to the position information, and obtain a many-to-one relationship diagram between the feature points P and the image blocks B as shown in (1):

$$\{P_m, P_n, \cdots \in B_i \quad m, n, i = 1, 2, \cdots\}, \tag{1}$$

where P_m represents the m-th SIFT keypoint; B_i is the i-th image block.

Step 2): we calculate the distance d between the feature points in different image blocks as shown in (2):

$$\begin{gathered} d(P_a, P_b) = \sqrt{\textstyle\sum_{s=1}^{128}(f_a^s - f_b^s)^2}, \\ a, b = 1, 2, \cdots, N, \ \textit{and}\ a \neq b, \\ P_a \in B_i, \ P_b \in B_j, \ i \neq j, \end{gathered} \tag{2}$$

where f_a^s represents the s-th dimension SIFT descriptor of the a-th feature point, and each SIFT keypoint has a 128-dimensional feature descriptor; N denotes the total number of SIFT keypoints; where P_a and P_b belong to different image blocks, respectively.

The matching between the feature points is successful if the distance is not greater than the threshold T_P (the threshold is set to 0.5), that is, $d(P_a, P_b) \leq T_P$. Then we mark the feature points whose matching is successful.

Step 3): we record the number of feature points successfully matched between each pair of image patches as the matching coefficient. It is necessary to remove the image block pair if the matching coefficient is smaller than the threshold T_B (the threshold is set to 2), which means deleting the feature points in the two image blocks that were successfully matched in step 2).

2.3 Forgery Localization

After the feature matching, the marked feature point pairs are obtained, but this is only the approximate location of the forged regions, and we need to locate precise forged regions. Forgery localization of our method involves three steps.

Step 1): we perform SLIC superpixel segmentation again, but this time the SLIC initial size is small (set to 20 in the experiments), which can result in small superpixel blocks. We replace the matching feature point pairs with small superpixel blocks, so that the separated pixels are converted into suspected regions with strong connectivity.

Step 2): for each suspected region, we compare it with the superpixel blocks adjacent to it. We check whether their color features are similar. Specifically, we calculate the mean value R of the pixels in the suspected region and the mean value S_i of the pixels in the i-th adjacent superpixel block. If $|R - S_i| \leq T_s$ (the threshold T_s is set to 5), the superpixel block is included in the suspected regions.

Step 3): we apply the morphological close operation into the suspected regions. A circular structural element is used in the closing operation whose radius is related to the size of the suspected regions. The close operation can fill the gaps in the merged regions in step 2) while maintaining the shape of the region unchanged.

3 Experiment Results

In this section, we conduct a series of experiments to evaluate the detection and localization performance of the proposed method for medical image copy-move forgery. The medical image dataset we used is the DDSM database [10] established by medical institutions to store breast cancer images and the lesion regions are marked by expert radiologists. The database includes more than 10,000 medical images in 2,620 cases. We randomly copy an area that has arbitrary shape in the cancer regions of the medical image and paste it to any random position of the same image, which do not leave a mark and the naked eyes cannot distinguish whether it is tampering or not and tampering with the localization.

Our experimental evaluation indicators are divided into image-level and pixel-level. Image-level indicators focus on assessing the ability of medical images to be correctly identified as forged or genuine. Pixel-level indicators analyze the performance for the accuracy of medical image forgery localization. In the following experiments, the three characteristics F_1 scores, True Positive Rate (TPR), and False Positive Rate (FPR) are used to evaluate the performance of the proposed MITD-CMFL, which are respectively defined as:

$$\begin{aligned} F_1 &= \frac{2TP}{2TP + FP + FN}, \\ TPR = \frac{TP}{TP + FN}, &FPR = \frac{FP}{TN + FP}. \end{aligned} \tag{3}$$

Table 1. Forgery localization performance of different methods.

Methods	Image level			Pixel level		
	F_1(%)	TPR(%)	FPR(%)	F_1(%)	TPR(%)	FPR(%)
FE-CMFD-HFPM [13]	99.92	99.85	0.00	90.01	98.10	0.19
Segment-CMFD [20]	99.63	99.27	0.00	58.68	79.61	1.27
Iterative-CMFD [30]	99.78	99.56	0.00	42.96	98.94	4.81
CMFD-PM [6]	99.85	99.71	0.00	86.23	87.35	0.07
RITD-MITD [23]	99.84	99.68	0.00	77.61	97.91	0.43
MITD-PIA [25]	99.81	99.63	0.00	81.93	95.65	0.29
MITD-CMFL	**100.00**	**100.00**	**0.00**	**95.07**	**98.81**	**0.08**

The F_1 score is a performance indicator of the integrated TPR and FPR. The higher the F_1, the better the performance of the algorithm. In this work, we use F-image and F-pixel to represent the F_1 scores at the image level and the pixel level, respectively. At the image level, TPR is the probability of detecting a forged image, which is defined as the ratio of the number of correctly detected fake images to the actual number of forged images; FPR is defined as the ratio of the number of correctly detected pristine images to the actual number of genuine images. Where TP (true positive) indicates the number of correctly detected fake images; TN (true negative) is the number of correctly detected genuine images; FN (false negative) calculates the number of undetected forged images; and FP (false positive) is the number of wrongly detected pristine images. In the pixel level, TPR is the probability that the relevant regions are detected, which is defined as the ratio of the number of correctly detected forged pixels to the number of forged pixels in the ground-truth fake image; FPR is expressed as the ratio of the number of genuine pixels detected correctly to the actual number of pristine pixels. Where TP, TN, FN, and FP represent the number of correctly detected fake pixels, correctly detected pristine pixels, wrongly undetected forged pixels, and missing detected genuine pixels. In general, a higher TPR and a lower FPR simultaneously indicate superior performance.

All experiments in this paper are conducted on the PC with Core-i7 and 12-GB RAM, operating in the MATLAB R2016a.

3.1 Evaluation Under Plain Copy-Move Attack

In this subsection, we evaluate the proposed MITD-CMFL under plain copy-move attack, namely no further attack is performed on the copy-move regions. The experiments of the subsection are performed on 1362 medical images randomly selected from DDSM. We selected six different copy-move forgery detection schemes as the baselines, including block-based [6,23], keypoint-based [13,25], and keypoint-segmentation-based [20,30]. Among them, [23] and [25] are algorithms for tampering localization of medical images. Table 1 lists the results on medical images of the DDSM dataset obtained by different copy-move

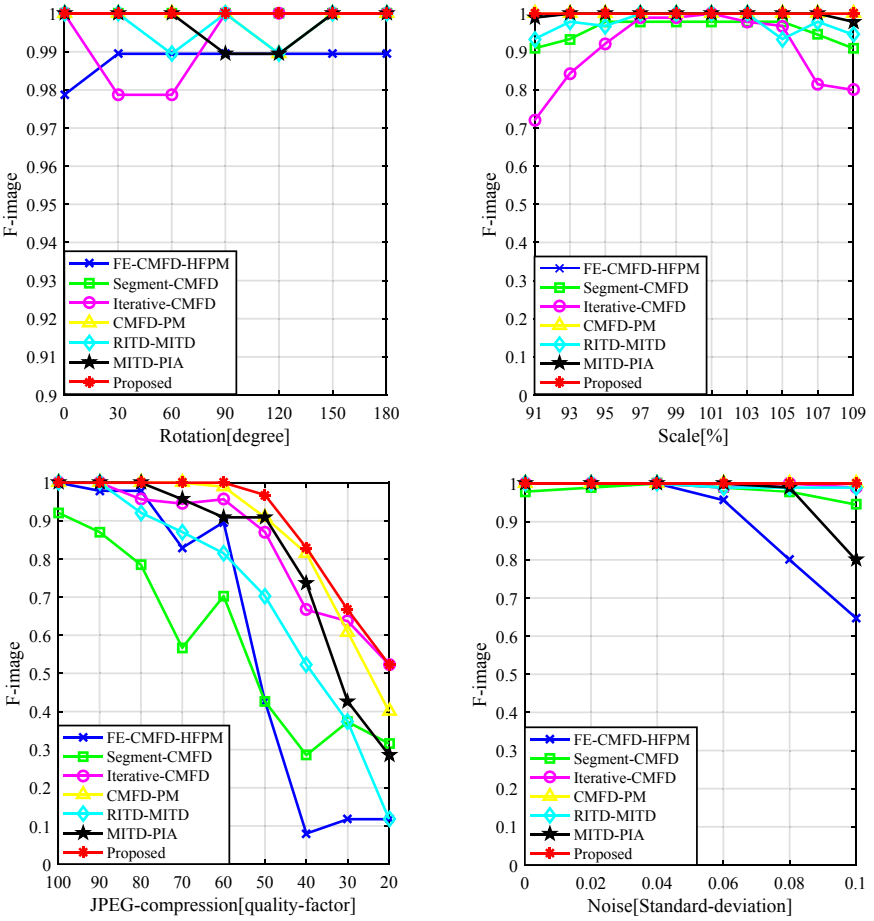


Fig. 3. Image level F_1 curves for different methods against rotation, scaling, JPEG compression, and Gaussian noise addition.

forgery detection methods. The algorithm FE-CMFD-HFPM improves the number of keypoints extracted in smooth regions, but cannot provide good support for texture information. The methods RITD-MITD and MITD-PIA are aimed at medical image tampering detection which extract the texture features of images. But other parts of RITD-MITD do not combine well with the texture information, and do not give full play to the advantages of texture features. Since medical images are relatively smooth, MITD-PIA cannot guarantee that enough keypoints with high discriminative ability in smooth regions are extracted to characterize texture features. The other three algorithms have poor detection capabilities which are unable to adapt to rich texture features and smooth regions of medical images. The proposed algorithm MITD-CMFL greatly overcomes such limitation which not only realizes the importance of texture information of med-

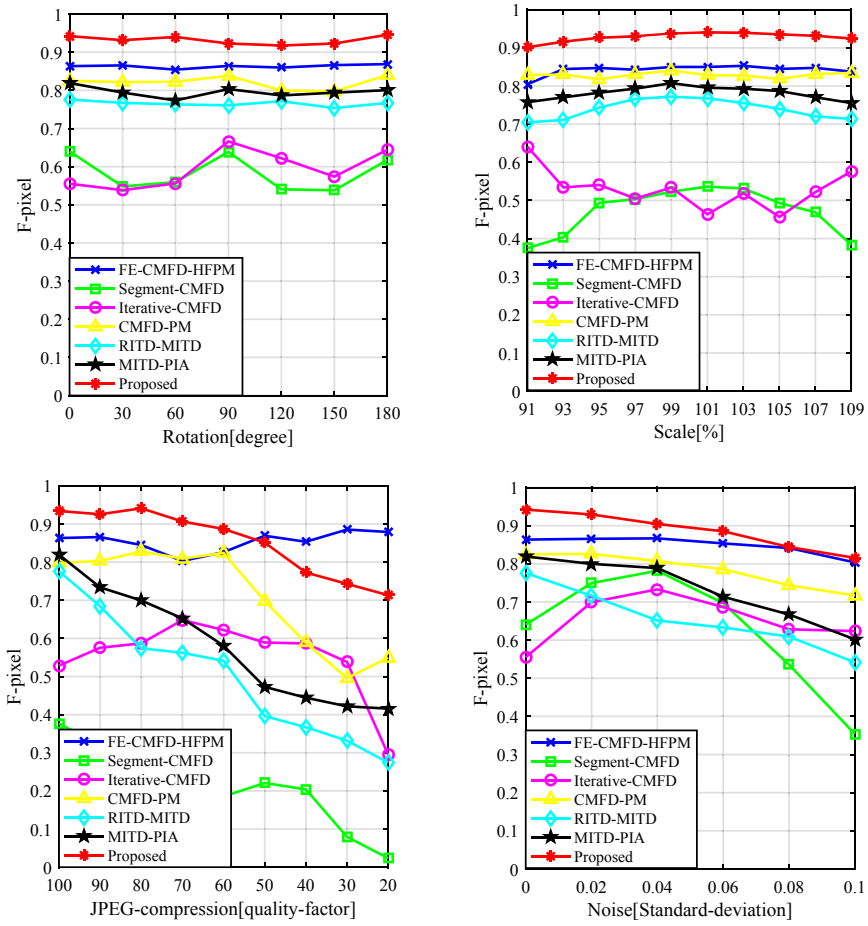


Fig. 4. Pixel level F_1 curves for different methods against rotation, scaling, JPEG compression, and Gaussian noise addition.

ical images, but also can well handle the problem of small number of SIFT feature points in smooth regions and weak representation ability. MITD-CMFL has considerable performance compare to other algorithms and achieves 95.07% high-precision tampering localization results.

3.2 Evaluation Against Different Attacks

In this subsection, we test the performance of MITD-CMFL against various attacks. The dataset used is 48 medical images randomly selected from the DDSM. We use image editing software to generate an image set containing 1536 images in total under different attacks comprising rotation, scaling, JPEG compression, and Gaussian noise addition. The details are as follows:

- Rotation: The rotation angle of each copied region ranges from 0° to 180° by a step size 30°. There are $7 \times 48 = 336$ medical images in total;
- Scaling: Each copied region is scaled from 91% to 109% of the scale factor with a step size of 2%, which can generate $10 \times 48 = 480$ medical images;
- JPEG compression: JPEG compression for each medical image using quality factor (QF) between 20 and 100 by a step size 10, in this case, we test $9 \times 48 = 432$ medical images;
- Gaussian noise addition: Gaussian noise is added to each medical image with standard value from 0 to 0.1 and the step size is 0.02. This produces a total of $6 \times 48 = 288$ medical images.

Figure 3 and Fig. 4 respectively show the F_1 curves for the image level and the pixel level against different attacks. At the image level, our proposed algorithm is completely superior to other algorithms. At the pixel level, our scheme is more sensitive to JPEG compression with the QF less than 60. After JPEG compression, especially when the QF is low, medical images lose their texture structures in a distorted manner, but texture information is the guarantee of detection accuracy. In addition, it exhibits better stability under other attacks. Although the stability of JPEG compression is slightly inferior to the method FE-CMFD-HFPM at the pixel level, the F1-measure curve at the image level of the FE-CMFD-HFPM indicates that its performance of correctly detecting whether the forged medical image is poor. Especially when the QF is less than 60, the detection performance is rapidly degraded, and it is basically impossible to resist this attack. Taken together, the proposed MITD-CMFL achieves better robustness gains over all the cases against the competing algorithms. The tampering localization algorithm RITD-MITD and MITD-PIA specifically for medical images cannot well resist these common attacks, which is a fatal disadvantage for medical images.

3.3 Evaluation of Different Phases

In this subsection, we test how the feature extraction scheme affects the performance of MITD-CMFL. The dataset for this part of the experiments is the same as Subsect. 3.1. Since the experiments involved in this subsection have little effect on the image-level evaluation indicators, we only show the experimental results at the pixel level.

The Initial Block Size of Superpixels in SLIC. The choice of initial block size of superpixels in SLIC affects the tampering localization accuracy and detection speed of the proposed algorithm. A larger initial block reduces the localization accuracy, while a smaller initial block brings a greater computational cost. In order to choose a suitable initial block size, we weigh the localization accuracy and detection speed. As shown in Fig. 5, during the process of changing the initial block from large to small, the accuracy of tampering localization is continuously improved, and the calculation cost is continuously increased. When the segmented image blocks are large, the probability of un-tampered regions being

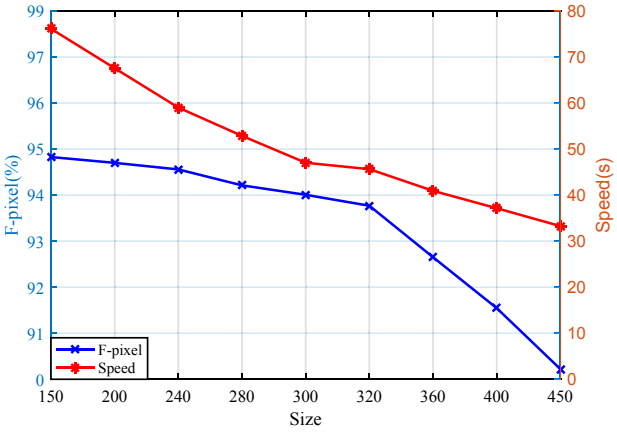


Fig. 5. F-pixel and speed of MITD-CMFL for different initial block sizes of superpixels in SLIC.

judged as tampered regions increases, which will cause the *FPR* to increase, and eventually reduce the *F-pixel*. When the initial blocks are small, the number of segmented image blocks increases, and the amount of SLIC calculations increases. Most importantly, the computational cost of the feature block matching process after segmentation will increase sharply. Considering that when the initial blocks are less than 300, the calculation cost rises sharply, but the improvement in positioning accuracy brought by it is not so obvious. After weighing, we chose 300 as the initial block size of SLIC in the proposed algorithm. Because the medical images in the DDSM dataset used for experiments are relatively large, more than 80% of the images are larger than 3000×3000, the overall calculation speed of the algorithm is relatively slow.

Table 2. The performance of different noise reduction methods.

Methods	$F_1(\%)$	$TPR(\%)$	$FPR(\%)$
MITD-CMFL+Mean filtering	**95.07**	**98.81**	**0.08**
MITD-CMFL+Wiener filtering	85.12	75.80	0.008
MITD-CMFL+Median filtering	79.56	66.89	0.01

The Noise Reduction Methods Table 2 shows the performance of different noise reduction methods on our algorithm. We compare three different noise reduction methods including mean filtering, Wiener filtering, and median filtering. We use *MITD-CMFL+Mean filtering*, *MITD-CMFL+Wiener filtering*, and *MITD-CMFL+Median filtering* represent these noise reduction methods respectively. According to the results in Table 2, we can see that the forgery detection

Table 3. Forgery localization performance of different methods with or without mean filtering.

Methods	With mean filtering			Without mean filtering		
	$F_1(\%)$	$TPR(\%)$	$FPR(\%)$	$F_1(\%)$	$TPR(\%)$	$FPR(\%)$
FE-CMFD-HFPM [13]	89.99	98.07	0.19	90.01	98.10	0.19
Segment-CMFD [20]	57.93	86.35	1.34	58.68	79.61	1.27
Iterative-CMFD [30]	41.91	98.64	3.96	42.96	98.94	4.81
CMFD-PM [6]	85.71	87.01	0.06	86.23	87.35	0.07
RITD-MITD [23]	77.83	97.52	0.41	77.61	97.91	0.43
MITD-PIA [25]	84.14	96.87	0.18	81.93	95.65	0.29
MITD-CMFL	**95.07**	**98.81**	**0.08**	**91.17**	**85.79**	**0.02**

method with mean filtering can extract more useful image features for MR medical image. Median filtering is easy to cause medical images discontinuity, and Wiener filtering is a non-stationary random process that is less friendly to noise reduction.

Noise reduction is a pre-treatment process for medical images, and noise reduction is an optional option, but it results in loss of information such as texture and edges. LBPROT texture descriptor can enhance images and increase the contrast between the foreground and the background so that creating a relatively clean input for the subsequent extraction of the SIFT features and achieving better localization results. Since both MITD-PIA and the proposed MITD-CMFL extract the texture features of medical images through LBPROT, we can observe from the Table 3 that the tampering localization accuracy of these two algorithms is improved after the mean filtering, while noise reduction has no effect on the other algorithms or reduces their performance.

Table 4. Forgery localization performance of different texture descriptors.

Methods	$F_1(\%)$	$TPR(\%)$	$FPR(\%)$
MITD-CMFL+NO_LBP	86.91	79.21	0.02
MITD-CMFL+LBP	90.20	85.51	0.01
MITD-CMFL+LBPEQU	47.42	41.07	0.002
MITD-CMFL+LBPROT	**95.07**	**98.81**	**0.08**

The LBP Operators. In the field of medical information, research on the physical characteristics of medical images is helpful to improve the positioning accuracy of image tampering detection. LBP is an indispensable step for MITD-CMFL owing to medical images have rich texture information, which can

emphasize texture structures of medical images. Different LBP texture descriptors have different effects on MITD-CMFL. As shown in Table 4, we have no LBP (*MITD-CMFL+NO_LBP*), LBP basic descriptor (*MITD-CMFL+LBP*), LBP equivalent descriptor (*MITD-CMFL+LBPEQU*), and rotation-invariant LBP descriptor (*MITD-CMFL+LBPROT*) are tested. The texture structure information of medical images is more complicated and more important than natural images, so it is necessary to specifically extract texture information. LBPROT is the best choice among different LBP descriptors which extends the 3×3 neighbourhood to any neighbourhood and replaces the square neighbourhood with a circular neighbourhood, it can adapt to texture features of different scales and achieve the grayscale and rotation invariant. Therefore, the extracted SIFT feature points representation ability under LBPROT descriptor is stronger, and the forgery localization performance is better.

4 Conclusion

Medical images are smooth and have complex texture structures. Accordingly, we propose an effective and robust method MITD-CMFL for medical image copy-move forgery detection and localization. MITD-CMFL combines block-based and keypoint-based technologies, which segments the medical image into semantically independent patches by using SLIC and matches the block features consisting of SIFT keypoints. LBPROT can reflect texture information of medical images, so that the obtained SIFT keypoints from texture images have high discriminating ability. To extract a larger number of feature points even in smooth regions of medical images, we decrease the SIFT contrast threshold. Experimental results demonstrate the proposed MITD-CMFL achieves higher success rate of detection and higher accuracy of localization. Despite these, there is much room for improving the robustness against JPEG compression and increasing the practicality of our method.

References

1. Amerini, I., Ballan, L., Caldelli, R., Del Bimbo, A., Serra, G.: A sift-based forensic method for copy-move attack detection and transformation recovery. IEEE Trans. Inf. Forensics Secur. **6**(3), 1099–1110 (2011)
2. Bayram, S., Sencar, H.T., Memon, N.: An efficient and robust method for detecting copy-move forgery. In: 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 1053–1056 (2009)
3. Bik, E.M., Casadevall, A., Fang, F.C.: The prevalence of inappropriate image duplication in biomedical research publications. MBio **7**(3), e00809–16 (2016)
4. Chen, C.-C., Lu, W.-Y., Chou, C.-H.: Rotational copy-move forgery detection using SIFT and region growing strategies. Multimedia Tools Appl. **78**(13), 18293–18308 (2019). https://doi.org/10.1007/s11042-019-7165-8
5. Cozzolino, D., Poggi, G., Verdoliva, L.: Copy-move forgery detection based on patchmatch. In: 2014 IEEE International Conference on Image Processing (ICIP), pp. 5312–5316 (2014)

6. Cozzolino, D., Poggi, G., Verdoliva, L.: Efficient dense-field copy-move forgery detection. IEEE Trans. Inf. Forensics Secur. **10**(11), 2284–2297 (2015)
7. Eswaraiah, R., Reddy, E.S.: Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest. IET Image Process. **9**(8), 615–625 (2015)
8. Fridrich, A.J., Soukal, B.D., Lukáš, A.J.: Detection of copy-move forgery in digital images. In: Proceedings of Digital Forensic Research Workshop (2003)
9. Ghoneim, A., Muhammad, G., Amin, S.U., Gupta, B.: Medical image forgery detection for smart healthcare. IEEE Commun. Mag. **56**(4), 33–37 (2018)
10. Heath, M., Bowyer, K., Kopans, D., Moore, R., Kegelmeyer, P.: The digital database for screening mammography. In: Proceedings of the Fourth International Workshop on Digital Mammography (2000)
11. Jin, G., Wan, X.: An improved method for sift-based copy-move forgery detection using non-maximum value suppression and optimized j-linkage. Signal Process. Image Commun. **57**, 113–125 (2017)
12. Li, J., Li, X., Yang, B., Sun, X.: Segmentation-based image copy-move forgery detection scheme. IEEE Trans. Inf. Forensics Secur. **10**(3), 507–518 (2014)
13. Li, Y., Zhou, J.: Fast and effective image copy-move forgery detection via hierarchical feature point matching. IEEE Trans. Inf. Forensics Secur. **14**(5), 1307–1322 (2018)
14. Li, Y.: Image copy-move forgery detection based on polar cosine transform and approximate nearest neighbor searching. Forensic Sci. Int. **224**(1–3), 59–67 (2013)
15. Manu, V., Mehtre, B.M.: Copy-move tampering detection using affine transformation property preservation on clustered keypoints. Signal Image Video Process. **12**(3), 549–556 (2018)
16. Memon, N.A., Chaudhry, A., Ahmad, M., Keerio, Z.A.: Hybrid watermarking of medical images for ROI authentication and recovery. Int. J. Comput. Math. **88**(10), 2057–2071 (2011)
17. Muhammad, G., Hussain, M., Bebis, G.: Passive copy move image forgery detection using undecimated dyadic wavelet transform. Digital Invest. **9**(1), 49–57 (2012)
18. Muzaffer, G., Ulutas, G.: A fast and effective digital image copy move forgery detection with binarized sift. In: 2017 40th International Conference on Telecommunications and Signal Processing (TSP), pp. 595–598 (2017)
19. Popescu, A.C., Farid, H.: Exposing digital forgeries by detecting duplicated image regions. Technical Report TR2004-515, Department of Computer Science, Dartmouth College, pp. 1–11 (2004)
20. Pun, C.M., Yuan, X.C., Bi, X.L.: Image forgery detection using adaptive oversegmentation and feature point matching. IEEE Trans. Inf. Forensics Secur. **10**(8), 1705–1716 (2015)
21. Ryu, S.J., Kirchner, M., Lee, M.J., Lee, H.K.: Rotation invariant localization of duplicated image regions based on Zernike moments. IEEE Trans. Inf. Forensics Secur. **8**(8), 1355–1370 (2013)
22. Shahroudnejad, A., Rahmati, M.: 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)
23. Sharma, S., Ghanekar, U.: A rotationally invariant texture descriptor to detect copy move forgery in medical images. In: 2015 IEEE International Conference on Computational Intelligence & Communication Technology, pp. 795–798 (2015)
24. Tejas, K., Swathi, C., Rajesh, K.M.: Copy move forgery using Hus invariant moments and log polar transformations (2018)

25. Ulutas, G., Ustubioglu, A., Ustubioglu, B., Nabiyev, V.V., Ulutas, M.: Medical image tamper detection based on passive image authentication. J. Digital Imaging **30**(6), 695–709 (2017)
26. Wang, H., Wang, H.: Perceptual hashing-based image copy-move forgery detection. Secur. Commun. Netw. (2018)
27. Wu, J.H., et al.: Tamper detection and recovery for medical images using near-lossless information hiding technique. J. Digital Imaging **21**(1), 59–76 (2008)
28. Yang, B., Sun, X., Guo, H., Xia, Z., Chen, X.: A copy-move forgery detection method based on CMFD-SIFT. Multimedia Tools Appl. **77**(1), 837–855 (2017). https://doi.org/10.1007/s11042-016-4289-y
29. Zain, J.M., Fauzi, A.R.: Medical image watermarking with tamper detection and recovery. In: 2006 International Conference of the IEEE Engineering in Medicine and Biology Society, pp. 3270–3273 (2006)
30. Zandi, M., Mahmoudi-Aznaveh, A., Talebpour, A.: Iterative copy-move forgery detection based on a new interest point detector. IEEE Trans. Inf. Forensics Secur. **11**(11), 2499–2512 (2016)
31. Zhao, F., Shi, W., Qin, B., Liang, B.: Image forgery detection using segmentation and swarm intelligent algorithm. Wuhan Univ. J. Nat. Sci. **22**(2), 141–148 (2017)
32. Zhao, J., Guo, J.: Passive forensics for copy-move image forgery using a method based on DCT and SVD. Forensic Sci. Int. **233**(1–3), 158–166 (2013)