Image-Based Copy-Paste Tamper Detection Technology Based on Improved Surf

Yanzhu Hu, Yingjian Wang* and Xinbo Ai

School of Automation, Beijing University of Posts and Telecommunications, 100876, Beijing, China

*Corresponding author e-mail: wangyjbupt@163.com

Abstract. Aiming at the problem that the existing copy-paste tamper detection algorithm has poor detection effect on the image area, and the speed is slow, an image region copy-paste tampering detection algorithm based on improved SURF is proposed. The detected image extracts feature points by improving the fast Hessian matrix, and uses k-g2NN method to match the feature points, then estimates the affine transformation parameters between the matching points, and combines the R-RANSAC and SPRT to eliminate the mismatch and finally obtain the copy-paste area. The experimental results show that the proposed algorithm can accurately locate the image copy-paste tampering region, and has strong robustness to Gaussian blur, rotation and scaling operations, and the detection speed is greatly improved.

1. Introduction

With the rapid development of computer networks and the popularization of smart devices, multimedia such as images brings people a better life experience and work convenience. But with the image tampering technology and image processing software features increasingly powerful, Image authenticity and reliability cause doubt. Even a series of problems, including the law, have been triggered by this, which has brought bad influence to society. Therefore, the identification of the authenticity of images by technical means is of great significance for combating malicious modification and maintaining judicial justice.

Copy-paste tampering is an important branch of image tampering. Detection techniques are mainly divided into two categories: block-based statistical algorithms and feature-based matching algorithms. At present, the block-based statistical algorithm mainly includes the PCA [1] algorithm based on dimensionality reduction, the fast algorithm of Zernike [2] moment, the Circle [3] algorithm based on gray value, and the DCT [4] quantization coefficient algorithm based on frequency. The above algorithm are very sensitive to noise and camera models in the image, cannot resist geometric transformation operations such as rotation and scaling. In addition, in order to make the image more vivid and realistic, tampering is usually accompanied by processing such as blurring, scaling, and noise addition. At this time, the block-based statistical algorithm is greatly limited. In response to this problem, scholars propose a detection algorithm based on feature point matching. Such as SIFT [5] algorithm, SURF [6] algorithm, MIFT algorithm and ORB [7] algorithm. The existing algorithm based on feature point matching improves the robustness of post-processing operations, but most of the copy-paste tampering images have poor detection effect, which is prone to misjudgment and slow detection speed.
This paper proposes an improved SURF copy-paste tamper detection algorithm. The algorithm extracts feature points and vectors by fast Hessian, and uses k-g2NN method to match the feature points, estimates the affine transformation parameters between the matching points, and finally rejects the error matching by R-RANSAC combined with SPRT. The experimental results show that the proposed algorithm can not only locate the accurate copy-paste area, but also improve the detection accuracy of tampering area.

2. "Copy-paste" tampering model
Copy-paste tampering in the same picture refers to copying an existing area $R_1$ in the image, pasting it into the target area $R_2$ in the original image, and combining the operations of blurring, scaling, and compression to make the tampering image appear more realistic to cover the original image. Some important goals in the middle or make up scenes that don't exist. Since the copy area comes from the image itself, other features such as the noise component and the direction of the light source are consistent with the rest of the image, so it is difficult for the naked eye to recognize it.

The copy-paste tampering model is shown in Figure 1, with the following assumptions:

1) The copied area $R_1$ is one connected area inside the image;
2) The $R_1$ area should not be too small, at least 1% larger than the original image size;
3) There is no coincidence part in the image copy-paste area;
4) The $R_2$ region can be obtained by rotating and scaling the $R_1$ region.

Image copy-paste tampering example shown in Figure 2:

Figure 2(a) is an original image of birds and branches. Copy the bird on the left side of the image, paste it on the left side of the image to form image 2(b). The falsified image is very realistic. It is difficult to distinguish the authenticity of an image by the naked eye.

3. Image copy-paste tamper detection algorithm to achieve
The algorithm of this paper first extracts the feature points and vectors of the detected image through the improved Hessian matrix. The k-g2NN method is used to perform feature point matching. Finally,
the affine transformation parameters between the matching points are estimated and the error matching is eliminated.

3.1. SURF feature point detection

The SURF algorithm has scale and rotation invariant characteristics, and the computational efficiency is improved by introducing integral images. The algorithm uses a box filter instead of second-order Gaussian filter, and uses a second-order fast Hessian matrix to implement feature point detection, extracting feature points in the image and expressing them as descriptors.

3.1.1. Integral image. Assuming that the input image is $I$, and the coordinates of a given point in the image $I$ are $(x, y)$. The integral image $I(x, y)$ can be obtained by calculating the sum of all pixel values in the rectangular region composed of the point and the origin [8]. The calculation expression is as shown in (1):

$$I_{\Sigma}(x, y) = \sum_{i=0}^{i=x} \sum_{j=0}^{j=y} I(x, y)$$

In the formula: $I(x, y)$ is the pixel value corresponding to the pixel point $(x, y)$ in the image $I$. Then, the sum of the pixel values($\sum$) of all points in the rectangular area determined by the vertices A, B, C, and D in FIG.3 is as shown in (2):

$$\sum = I_{\Sigma}(A) + I_{\Sigma}(D) - I_{\Sigma}(B) - I_{\Sigma}(C)$$

![Figure 3. Schematic of the integral image](image)

3.1.2. Fast Hessian matrix detection. Suppose $X = (x, y)$ is a pixel of image $I$, Then the Hessian matrix $H(X, \sigma)$ can be defined as a function of $X$ and scale $\sigma$:

$$H(X, \sigma) = \begin{bmatrix} L_{xx}(X, \sigma) & L_{xy}(X, \sigma) \\ L_{xy}(X, \sigma) & L_{yy}(X, \sigma) \end{bmatrix}$$

(3)

Where: $L_{xy}(X, \sigma)$ means at scale $\sigma$, Pixel point $X$ and second-order Gaussian filter $\frac{\partial^2 (g(\sigma))}{\partial x^2}$ convolution result. The definitions of $L_{xy}(X, \sigma)$ and $L_{yy}(X, \sigma)$ are similar. As shown in FIG.4, a Gaussian second-order differential template is approximated by a box filter to improve the operation speed.
Figure 4. Box filter

The result of convolving the integral image with the box filter is denoted by $D_{xx}$, $D_{yy}$, $D_{xy}$, and the expression of the Hessian determinant is obtained:

$$\det(Hessian) = D_{xx}D_{yy} - (\alpha D_{xy})^2$$  \hspace{1cm} (4)

Where: $\alpha$ is the weight coefficient, balance the energy between the second-order Gaussian filter and the box filter.

If $\det(Hessian) \geq 0$, $(x, y)$ is the extreme point. Set the scale factor $\sigma = 1.2$, Then there are:

$$\frac{||L_{xy}(1.2)||}{||L_{xx}(1.2)||} \approx 0.9$$  \hspace{1cm} (5)

Which is:

$$\det(Hessian) = D_{xx}D_{yy} - (0.9D_{xy})^2$$  \hspace{1cm} (6)

Since the feature points directly detected by the matrix approximation determinant are more and irregularly distributed. Therefore, constructing a circular screener constrains the SURF feature points to improve algorithm efficiency. When the number of detected feature points is greater than the threshold $K$, the following adjustment is made:

1) Select the feature point corresponding to the largest $\det(Hessian)$ value as the first feature point, Then follow step 2) to set the number of feature points. If the number of feature points is still $>K$ after tuning, the feature point corresponding to the second largest value is selected as the first feature point, and the number of feature points in step 2) is set, and so on;

2) Set the detection area size to $M \times N$, Setting threshold $S = i\% \sqrt{M^2 + N^2}$, $i = 1, 2, 3…$, With the first feature point as the center, select the appropriate i value, create a circular area with radius $S$, and delete all the feature points in the circular area.
3.1.3. Generating feature descriptors. First, the first-order Haar wavelet is used to distribute the direction of the feature points. Select a feature point (corresponding to the scale $\sigma$) and set it as the center of the circle. Forming a circular area of radius $6\sigma$. Calculate the Haar wavelet response in the x and y directions with a Haar wavelet of size $4\sigma$. Then, a sector-shaped area (the center angle is $60^\circ$, the feature point is the origin) is rotated one week, and the sum of the Haar wavelet responses of the included points is calculated to form a vector set, and the largest vector is selected as the main direction of the feature points.

The feature descriptor of the feature point is generated after the main direction is selected. Determining a square area centered at the feature point and having a size of $20\sigma \times 20\sigma$, it is divided equally into 4 sub-regions. Select $5 \times 5$ sampling points for each sub-area, and calculate the Haar wavelet response corresponding to each sub-area. The response in the X direction of the Haar wavelet is recorded as $dx$, and the response in the Y direction is recorded as $dy$. Each sub-area is then evenly subdivided into 4 sub-sub-areas, and the sum of the Haar wavelet responses in the X, Y directions and the sum of the absolute values is counted for each sub-sub-area. In the process of statistics, the Gaussian function centered on the feature points is still weighted. At this time, each sub-region has a 4-dimensional descriptor, and the expression is:

$$V_{sub} = \left( \sum dx, \sum dy, \sum d|x|, \sum d|y| \right)$$  \hspace{1cm} (7)

The entire square region contains a feature vector of 64 dimensions, which is the feature descriptor of the feature point.

3.2. Feature point matching

When feature point matching is performed according to feature descriptors, the traditional g2NN matching algorithm solves the problem of copy-paste tampering by searching for multiple neighbors. It is assumed that the feature point set $S = \{s_1, s_2, ..., s_n\}$ and the corresponding feature descriptor are extracted for the image $I$. For a certain feature point $s_i$, the Euclidean distance of the descriptor corresponding to the remaining feature points is obtained, and the obtained Euclidean distances are sorted in ascending order to obtain a distance vector $D = \{d_1, d_2, ..., d_n\}$. If it satisfies:

$$\frac{d_1}{d_2} < \tau, \hspace{0.5cm} (0 \leq \tau \leq 1)$$  \hspace{1cm} (8)

Then it indicates that the feature point matches the feature point closest to it that is the 2NN criterion. The smaller the value of $\tau$, the less the mismatch, but the leak matching may occur. Calculate in order:

$$T_i = \frac{d_i}{d_{i+1}} (i = 1, 2, ..., n-2)$$  \hspace{1cm} (9)

If $Z$ satisfy $T_2 \leq \tau$, the feature point $s_i$ and the Z feature points from the $\{d_i, d_2, ..., d_n\}$ are matched, and all the feature points are traversed to obtain a matching pair set $P = \{p_1, p_2, ..., p_n\}$, $P_i = (s_i, S_j)$ is a two-dimensional vector composed of the feature points and the matching points.

In the matching process, the number of feature points extracted is large, and the g2NN method takes a lot of time and efficiency in sorting and threshold comparison.

This paper uses k-g2NN algorithm to improve matching efficiency [9]. The main improvements of the algorithm are:
1) The nearest $k$ feature points of the Euclidean distance corresponding to the descriptor of the feature point are directly selected, and the value of $k$ is proportional to the obtained number of feature points and satisfies $k < n / 2$. For the order of $n$ distances, the optimal time complexity is $O$, and the time complexity corresponding to the $k$ feature points with the smallest Euclidean distance is:

$$O(k \log k + (n - k))$$ (10)

2) Loop 2 neighbor criteria within the range of $k$ feature points, reducing the number of comparisons with the threshold and eliminating some mismatches.

3) Mark the feature points that have been matched with the remaining feature points, and the subsequent matches will skip the feature points, eliminating the computational redundancy.

3.3. Eliminate mismatches

In the image, the feature descriptors of the two points are also similar because of the similar texture attributes or color brightness, which leads to mismatching.

The affine transformation between the copied region and the tamper region is estimated based on the matching feature points, The affine transformation $X_2 = TX_1 + \Delta X$ is obtained by a given set of matching feature points $X_1 = (x, y)^T$ and $X_2 = (\tilde{x}, \tilde{y})^T$. The R-RANSAC algorithm with sequential probability ratio test (SPRT) is used to eliminate the mismatch.

The R-RANSAC is a RANSAC algorithm for evaluating hypothetical models, which is improved on the basis of the standard RANSAC algorithm. The SPRT method is to detect whether each sample data matches the model and calculate a likelihood ratio. If the likelihood ratio is greater than the threshold, the model is considered to be inaccurate and discarded until all sample points have been detected.

By combining R-RANSAC with SPRT to detect inconsistencies [10]. All the mismatches are eliminated, and all matching points that meet the conditions are connected by lines to obtain an image of the detection result.

4. Analysis and discussion of experimental results

The test image set used in this experiment was from the self-built tamper data set of the laboratory. According to different tampering behaviors, the library has further classified the tampering maps, copy-paste tampering, zoom tampering and rotation tampering.

4.1. Copy-paste tamper detection

As shown in FIG.5, FIG.5 (a) is an original image, FIG.5(b) is a copy-paste tamper-modified image, and FIG.5 (c) is a result of detecting and recognizing a tamper image by the algorithm of the present invention. In the detection result, the copied area and the pasted area are connected by line, and the label is displayed.

![Figure 5. Copy-paste tampering test results](image-url)
4.2. Rotation, zoom tamper detection
Rotation and scaling are common post-processing operations for tampering techniques in tampering areas. The zoom operation is as shown in Fig. 6. On the basis of the original figure 6(a), the right target is zoomed out and pasted to the upper right corner of the image to obtain a reduced figure 6(b), and Fig. 6(c) is detected by the algorithm of the present invention. The obtained result, FIG. 6(d) is a picture obtained by rotating the tamper region by a certain angle on the basis of FIG. 6(b), and FIG. 6(e) is the result of the detection by the algorithm of the present invention.

(a) The original image (b) Reduce image (c) Detection image
(d) Rotate-zoom image (e) Detection image

Figure 6. Anti-rotation and scaling detection experimental results

4.3. Algorithm precision and efficiency analysis
In order to quantify the performance of the algorithm, the experiment selects SIFT and SURF two tamper detection techniques and the algorithm to compare the accuracy and efficiency. The accuracy rates TPR and FPR were chosen as the accuracy detection criteria. The detection time is used as a criterion for the detection efficiency.

The randomly selected pictures in the picture library are detected. The obtained TPR, FPR and detection time are shown in Table 1. The algorithm is higher than the SIFT and SURF algorithms in both detection accuracy and detection time.

Table 1. Comparison of test results between SIFT, SURF and the proposed algorithm

| Algorithm name     | TPR  | FPR  | Detection |
|-------------------|------|------|-----------|
| SIFT              | 0.83 | 0.06 | 7.1       |
| SURF              | 0.90 | 0.04 | 3.2       |
| Algorithm of this paper | 0.94 | 0.04 | 2.6       |

5. Conclusion
This paper proposes an image region copy-paste tampering detection algorithm based on improved SURF. The algorithm extracts SURF feature points by fast Hessian matrix combined with circular screen remover, and uses the improved g2NN algorithm to match the obtained feature points. Finally, the affine transformation parameters between matching points are estimated, and R- RANSAC and SPRT combine to eliminate mismatches and identify complete replication-moving areas. The experimental results show that the proposed algorithm can accurately identify the copy-paste tampering region of the image, and has higher detection accuracy and detection speed than the SIFT and SURF algorithms. Moreover, the detection algorithm of this paper is more robust.

Acknowledgments
This work was financially supported by Beijing Science and Technology Project (NO.Z181100000618006) fund.
References

[1] Gan Y, Cang J. A detection algorithm for image copy-move forgery based on improved circular projection matching and PCA [J]. Sensors & Transducers, 2013, 159 (11): 19-25.

[2] Ryu S J, Kirchner M, Lee M J, et al. Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments [J]. IEEE Transactions on Information Forensics and Security, 2013, 8 (8): 1355-1370.

[3] Prakash CS, Maheshkar S, Detection Algorithm for Copy-Move Forgery Based on Circle Block [C] //Proceedings of International Conference on Computer Vision and Image Processing. Singapore: Springer, 2017: 355-364.

[4] Kumar S, Desai J, Mukherjee S. A fast DCT based method for copy move forgery detection [C]// IEEE Second International Conference on Image Information Processing. IEEE, 2014.

[5] Lowe D G. Distinctive Image Features from Scale-Invariant Keypoints [J]. 2004.

[6] Bay H, Tuytelaars T, Gool L V. SURF: Speeded Up Robust Features [C] // European Conference on Computer Vision. 2006.

[7] Zhu Y, Shen X, Chen H. Copy-move forgery detection based on scaled ORB [J]. Multimedia Tools and Applications, 2016, 75 (6): 3221-3233.

[8] [IEEE 2013 18th International Conference on Digital Signal Processing (DSP)-Fira, Santorini, Greece (2013.07.1-2013.07.3)] 2013 18th International Conference on Digital Signal Processing (DSP) - Improving the detection and localization of duplicated regions in copy-move image forgery

[9] Bo X, Junwen W, Guangjie L, et al. [IEEE 2010 International Conference on Multimedia Information Networking and Security - Nanjing, China (2010.11.4-2010.11.6)] 2010 International Conference on Multimedia Information Networking and Security - Image Copy-Move Forgery Detection Based on SURF [J]. 2010: 889-892.

[10] Chum, Ondřej, Matas, and Jiří. Optimal Randomized RANSAC [J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 2008, 30 (8): 1472-1482.