FI-SIFT Algorithm for Exposing Image Copy-Move Forgery with Reflection Attacks

You-Jian Yu[1], Guang-Fu Wang[2], and Jie Zhao[1]
(Corresponding author: Jie Zhao)
School of Computer and Information Engineering, Tianjin Chengjian University, Tianjin 300384, China[1]
Tianjin Surveillance Technology Company Limited, Tianjin 300392, China[2]
(Email: zhaoj@tju.edu.cn)
(Received July 16, 2018; Revised and Accepted Dec. 6, 2018; First Online Sept. 16, 2019)

Abstract

In order to improve the robustness of SIFT algorithm to reflection attack, a flip-invariant SIFT (FI-SIFT) descriptor is proposed to detect copy-move forgery of digital images based on the study on the arrangement of SIFT descriptor after reflection attack in this paper. The proposed descriptor FI-SIFT is designed to improve the invariance to reflection and perform as well as SIFT in other situations. Our method starts by extracting FI-SIFT descriptors for detected SIFT key points in the suspicious image. Then, the g2NN method is adopted to implement multiple key points matching. Next, the possible affine transform between matched key points is estimated to remove the mismatched key points. Extensive experimental results are presented to confirm that our method performs well to detect copy-move forgeries distorted by common attacks including rotation, scaling, reflections and their mixture, especially for the sophisticated scenario, such as multi-objects forgery with combination of reflections.

Keywords: Copy-Move Forgery; FI-SIFT; Image Forensics; Reflection Attack

1 Introduction

Nowadays, we are living in an era of digital revolution which makes it easier for people to access, process, and share digital information. Digital media is playing a significant role in our daily life. However, with the popularity of sophisticated editing tools like Photoshop, it is becoming very difficult to discriminate between an authentic picture and its manipulated version, which poses a serious social problem of debasing the credibility of photographic images as definite records of events. To tackle this crisis of confidence and attempt to restore the credibility in society regarding digital images, the field of digital forensics aiming to reveal forgery operations in digital images is receiving more and more attention.

Among forgery techniques using typical image processing tools, copy-move is the most common type due to its simplicity and effectiveness, where a region of an image is copied and then pasted to another nonintersecting region in the same image to conceal an important element or to emphasize a particular object. The existing copy-move forgery detection methods are based on the fact that, at the end of the manipulation process, the resulting image will have relatively similar areas since the duplicated regions come from the same image. Although not always necessary, some additional operations are often performed on the duplicated regions before pasting them to make the forgery unnoticeable. These operations are used to provide a type of spatial synchronization and homogeneity between the copied region and its neighbors, including rotation, scaling, reflection, illumination modifying, or chrominance modifying. In a practical situation, the processing could be a combination of two or more operations. Thus, the effectiveness of copy-move forgery detection depends on the ability to detect forgery regions with these attacks.

In this work, we proposed a novel flip-invariant SIFT descriptor called FI-SIFT for automatic detection and localization of copy-move forgery regions based on the classical SIFT algorithm in order to resist to reflection-based attacks. We then compared the performance with two state-of-the-art methods to verify the validity of our algorithm. The remainder of the paper is organized as follows. In Section 2, the related research about the past works is introduced. Section 3 presents FI-SIFT descriptor which is the core contribution and novelty of our method. In Section 4, the proposed detection approach is described in detail. Section 5 gives experimental results and the corresponding analysis. Finally, a brief conclusion is drawn in Section 6.

2 Related Work

During the last decade, a large number of techniques have been proposed to address the problem of copy-move forgery detection. First attempt in identifying tampered areas was investigated by Fridrich *et al.* [5] who proposed

a method using discrete cosine transform (DCT) of overlapping blocks and their lexicographical representation to avoid the computational burden. Later, with the purpose of improving robustness and detection efficiency, Huang *et al.* [8], Cao *et al.* [4] and Zhao *et al.* [17] proposed improved block matching detection schemes based on DCT respectively. Luo *et al.* [11] divided image blocks into four sub-blocks, which were evaluated according to the averages of the red, green, and blue color values. Although these methods proved robust to some attacks such as additive noise, Gaussian blurring, and JPEG compression to some extent, they might fail if the duplicated regions underwent geometrical transformations such as rotation or scaling before they were pasted. To solve the above-mentioned problem, several methods have been explored by matching interest point descriptors to identify forged regions as an alternative to the block-matching based detection methods. Such interest point descriptors include scale invariant feature transform (SIFT) [13] descriptor and speeded up robust feature (SURF) [2] descriptor, which are robust to rotation and scaling. Huang *et al.* [7] exploited the SIFT interest point descriptor to reveal the duplicate regions in the forged image through direct matching among these interest points. Furthermore, Amerini *et al.* [1] proposed a SIFT-based detection scheme that could detect and then estimate the geometric transformation used in the copy-move forgery. Similar to Amerini's algorithm, Pan and Lyu [12] proposed another SIFT-based detection algorithm that had the ability to obtain the precise location and extent of the detected duplicated regions using the estimation of affine transformation between matched key points and the correlation of corresponding regions. Xu *et al.* [15] adopted SURF descriptor to detect this forgery with higher efficiency.

Although the feature points-based methods show promising performance, SIFT and SURF feature extraction techniques have two inevitable weaknesses. Firstly, they have difficulties in locating feature points in flat regions and misdetect in uniform regions. In the recent year, Bi *et al.* [3] proposed a multi-level dense descriptor and a hierarchical feature matching method to address this issue. Zandi *et al.* [16] applied an iterative improvement strategy to a new dense descriptor to improve algorithm performance. Secondly, they fail in the situation of reflection as shown in Figure 1. Despite the invariance of SIFT is remarkably robust, it naturally lacks the ability to describe the reflection transformation of feature points. In view of the above problem, Guo X *et al.* [6] proposed a reflection invariant descriptor inspired from SIFT, which resulted in high false alarming rate for authentic images with planar symmetric objects. Warif *et al.* [14] combined the SIFT-based copy-move forgery detection method with symmetry-based matching to enhance the robustness to reflection attack, which was proven to be inefficient by our experiments as a result of double matching in nature. In this paper, the proposed FI-SIFT descriptor was designed to improve the invariance to reflection and perform as well as SIFT in other situations. Particularly, we reorganize the structure of SIFT descriptor, and also adjust the matching strategy accordingly.

3 FI-SIFT Descriptor

Although the classical SIFT descriptor has been proven to perform better than the other existing local descriptors, it does not gain sufficient robustness in the case of reflection. That is to say, as a consequence, the descriptors extracted from two identical but flipped local patches could be completely different in feature space. To overcome the above limitation, we propose a flip-invariant SIFT descriptor, which enhances SIFT with flip invariance property.

Reflection is one of the most common used operations in copy-move forgery, which can be divided into two types: horizontal and vertical reflection. Since vertical reflection image can be obtained by rotating the horizontal flipped version by 180 degrees, the two kinds of reflections are equivalent by rotating the dominant orientations of coordinate system. Thus, in this section we just consider the case of horizontal reflection.

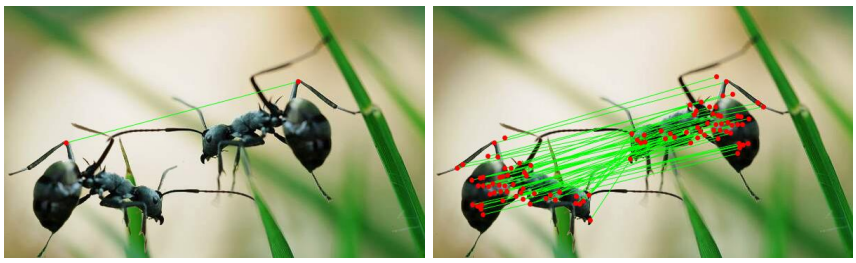
3.1 Analysis on SIFT Descriptor in the Case of Reflection

A SIFT descriptor consists of magnitudes of all the orientations histogram entries in a 4×4 array with 8 orientation bins in each around the corresponding key point. As shown in Figure 2, Figure 2(a) is a key point with its interest region in the original image, and Figure 2(b) is Figure 2(a) in the horizontally reflected image, both of which are after specifying dominant orientation as indicated by the arrow in the figures. Figure 2(d) shows the distribution of 8 orientations in the 14^{th} cell of Figure 2(a). Accordingly, Figure 2(c) is the corresponding version of Figure 2(b).

SIFT employs a fixed order to organize the 16 cells in the interest region. As shown in Figure 2(a), SIFT uses the column-major-order encoding strategy to obtain the key point descriptor. It thus sorts the order of 16 cells as Figure 2(e). However, the order of 16 cells is reversed after horizontal reflection as shown in Figure 2(b). As a result, the original fixed encoding strategy used in SIFT would arrange the 16 cells as Figure 2(f). Although SIFT descriptor is invariant to rotation and scale, and even tolerant to affine transformation, it does not result in the same order in the case of horizontal reflection. Besides, it is not hard to see that the order of 16 cells is the same as Figure 2(b) because of the rotation invariance. For the foregoing reasons, SIFT does not have the ability to resist reflection attack.

3.2 Descriptor Reconstruction

In this paper, we propose a universal encoding technique to generate key point descriptor FI-SIFT, which is also



(a) Detecting result of SIFT (b) Detecting result of FI-SIFT

Figure 1: Comparison of detecting results between SIFT and FI-SIFT in a copy-flip-move distorted image

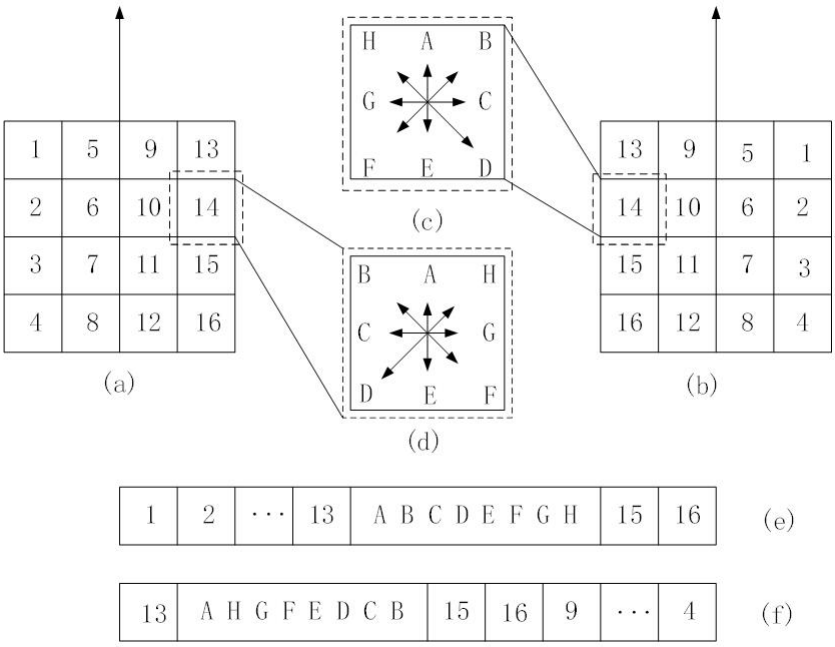


Figure 2: Illustration of the descriptor organization of SIFT in the case of horizontal reflection

invariant to reflection while preserving tolerance to rotation, scale and even affine transformation. First, we determine the location, scale and dominant orientation of key points using the classical SIFT algorithm. Next, for each key point the FI-SIFT descriptor is calculated as follow. Just as there might be multiple descriptors for the same combination of location and scale in the classical SIFT algorithm, FI-SIFT employs two different descriptors to represent the feature of each key point. To be specific, FI-SIFT adopts the anticlockwise order and clockwise order strategies to reorganize the feature descriptor respectively. As shown in Figure 3(a) and Figure 3(b), the 16 cells in the interest region are reorganized in anticlockwise order, and 8 orientation bins in each cell are rearranged into anticlockwise array. In this way, the 16 cells are ordered as Figure 3(e). Similarly, for each key point FI-SIFT reorganizes the 16 cells and 8 orientation bins in each cell in clockwise order as shown in Figure 3(c) and Figure 3(d). As a result, the 16 cells are ordered as Figure 3(f). To summarize, for each key point, FI-SIFT generates two different descriptors as shown in Figure 3(e) and Figure 3(f), where the 16 cells and 8 orientation bins are sorted in anticlockwise and clockwise order respectively.

4 The Proposed Method

In this section, we describe the proposed method in detail to detect duplicated and pasted regions in a tampered image.

4.1 FI-SIFT Features Extraction and Multiple Key Points Matching

In our method, duplicated regions are detected in the illumination domain, thus RGB images are first converted to grayscale images using standard color space conversion. Given a grayscale image, a set of SIFT key points $X = \{x_1, x_2, \cdots, x_n\}$ with their corresponding FI-SIFT descriptors $\{f_1, f_2, \cdots, f_n\}$ are extracted. Since it may happen that the same image region is cloned more than once, multiple key points matching need to be taken into

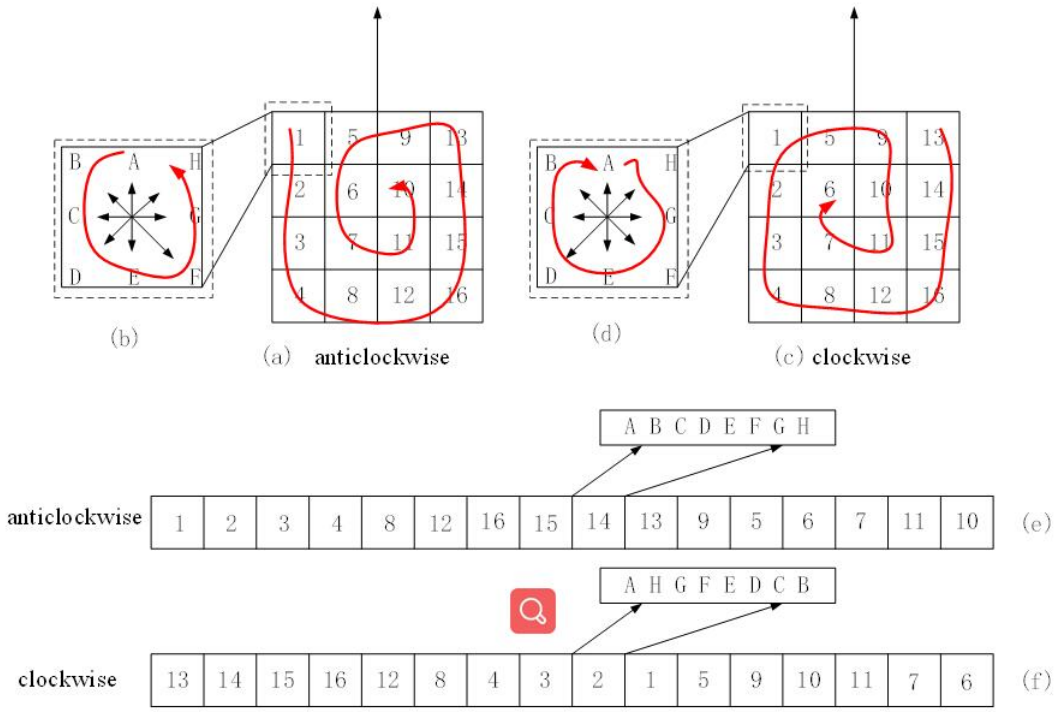


Figure 3: Illustration of the descriptor organization of FI-SIFT

account. For this reason, we adopt g2NN method [1] to implement multiple key points matching. In a high dimensional feature space such as that of FI-SIFT features, for key points that are different from one considered, Euclidean distances of their features share very high and very similar values. Instead, for two similar key points, their features show low Euclidean distances with respect to the others. In the early 2NN method [10], given a key point we need to define a similarity vector $D = \{d_1, d_2, \cdots, d_{n-1}\}$ that represents the sorted Euclidean distances with respect to the other descriptors. The key point is matched only if d_1/d_2 is lower than a preset threshold T_{2NN}. The g2NN method can be viewed as the generalization consisting of iterating the 2NN method between $R_i = d_i/d_{i+1}$ ($i = 1, 2, \cdots, n-2$) until this ratio R_i is greater than a preset threshold T_{g2NN}. If this ratio satisfies $R_k < T_{g2NN}$ $(1 \leq k < n-2)$ and $R_{k+1} \geq T_{g2NN}$, each key point in correspondence to a distance in $\{d_1, d_2, \cdots, d_k\}$ is considered as match points for the inspected key point. We can obtain the set of matched key points by iterating over key points in X.

4.2 Estimating Affine Transform Between Matched Key Points

Next, we need to estimate the possible geometric distortions between duplicated regions and pasted regions. Since almost all the image geometry transforms such as rotation, scaling and shearing can be generalized as affine transform, we model the distortion affine transform of pixel coordinates. Given two corresponding pixel location from a duplicated region and its pasted counterpart as $x = (x, y)^T$ and $\widetilde{x} = (\widetilde{x}, \widetilde{y})^T$ respectively, we can employ a 2-D affine transform to relate them, which is specified by a 2×2 matrix $T = [t_{11}t_{12}; t_{21}t_{22}]$ and a shift vector $x_0 = (x_0, y_0)^T$ as $\widetilde{x} = Tx + x_0$, more definitely

$$\begin{pmatrix} \widetilde{x} \\ \widetilde{y} \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} x_0 \\ y_0 \end{pmatrix} \tag{1}$$

We can obtain unique affine transform parameters T and x_0 by means of randomly selecting three pairs of corresponding key points which are not collinear. Since there are some imprecise matching in practice, Equation (1) may not be satisfied exactly. In order to eliminate deviation as far as possible, we optimize matched key points $(x_1, x_2, \cdots, x_n)$ and $(\widetilde{x_1}, \widetilde{x_2}, \cdots, \widetilde{x_n})$ using least squares objective function to find optimal parameter combination T and x_0 when Equation (2) is minimized.

$$L(T, x_0) = \sum_{i=1}^{N} \|\widetilde{x_i} - Tx_i - x_0\|_2^2 \tag{2}$$

According to the estimated parameters T and x_0, all the putative pairs of matched key points are classified into two groups: inliers and outliers. Specifically, a pair of matched key points $(x, \widetilde{x})$ is an inlier if $\|\widetilde{x} - Tx - x_0\|_2 \leq \beta$, otherwise, it is regarded as an outlier. To remove the impact of mismatched key points and obtain accurate transform parameters, Random Sample Consensus (RANSAC) algorithm is employed to robustly estimate the affine transform parameters, which returns with estimated parameters that generate the largest number of inliers. In our

experiment, we choose default value for N=100 and $\beta = 3$ which lead to better empirical performance.

5 Experimental Results and Discussion

In this section, we evaluate the performance of the proposed method through a comprehensive set of experiments. First, the experimental setup and evaluation metric used in the experiments are introduced. Next, the effectiveness of our method is evaluated in different situations. Then, we compare our method with two state-of-the-art methods which also are developed to improve the invariance to reflection based on SIFT.

5.1 Experimental Setup and Evaluation Metrics

At present, almost all the public datasets for copy-move forgery detection contain only simple geometrical transformation attacks, including translation, rotation, scaling, as well as the mixture of theirs, which lack the corresponding images for reflection attacks. In the recent year, a new dataset called NB-CASIA [14] was created to evaluate the performance of detection methods against reflection attacks. This dataset is composed of 510 images: 255 are original images and 255 are forged images, which the original images are taken from the CASIA v2.0 dataset [9]. The resolution of the images vary from 240 160 to 900 600. The forged images in NB-CASIA consist of translation, rotation, scaling, reflection and the mixture with different parameters as follow.

1) Translation: The duplicated region is translated to the target location with no distortion.

2) Rotation: The duplicated region is rotated with an angle $\theta \in \{20^o, 40^o, 60^o, 120^o, 240^o\}$.

3) Scaling: The duplicated region is scaled with a scaling factor $s \in \{0.6, 0.8, 1.2, 1.4, 1.6\}$.

4) Reflection: The duplicated region is flipped horizontally or vertically.

5) Mixture of attacks: The duplicated region is distorted with a mixture of attacks.

Our experiments were implemented using MATLAB R2015a on an Intel Core i7 3.4GHz processor with 8GB memory. The detection performance was measured in terms of F-score by the image-level, which is defined as

$$F = \frac{2TP}{2TP + FN + FP} \tag{3}$$

where true positive (TP), false negative (FN) and false positive (FP) represent the number of detected forged images, undetected forged images and wrongly detected original images, respectively.

5.2 Effectiveness Test and Comparisons

In the following experiment, we employed NB-CASIA dataset to test the effectiveness of our algorithm. All the forged images in this experiment were without any post-processing operation. Examples of detected results were illustrated in Figure 4. It was noted that the proposed method output detection result maps with color lines connecting all the matching points to identify the duplicated region and forgery region. Although the forged region cannot be localized precisely to pixel level, we can easily identify the tampered region by color lines, which is sufficient for practical detection requirements. Figure 4(a) shows the authentic image. Figures 4(b), 4(c) and 4(d) give the detected results of rotation, scaling and horizontal reflection respectively, which indicate that our method can expose copy-move forgeries effectively in the case of geometric transformations attacks. It is not hard to see that our method can detect stable results by sufficient matching of key points, especially for horizontal reflection attack, which surpasses the classical SIFT algorithm.

Next, we present the analysis of the performance of our method in detecting forged images. The results were compared with two promising methods: Amerini *et al.* [1] and Warif *et al.* [14]. Table 1 shows the overall performance of all the forgery detection methods which were implemented and applied to the NB-CASIA dataset. The input parameters required by the two methods were set as the papers gave. TP, FP and FN values were used to calculate the F-score for each method. As shown in Table 1, our method achieved the best performance compared to the other two methods, which indicated that our method is effective in detecting common transformation attacks, including rotation, scaling, reflections and their mixture. Experimental results show that wrongly detected original images almost have intrinsically similar areas and undetected forged images all have highly uniform region resulting in unreliable feature points.

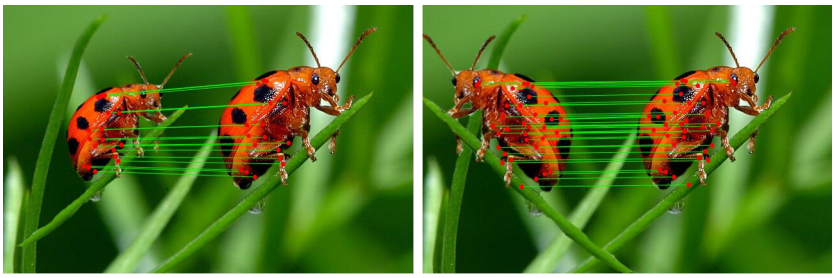
Table 1: The F-score with TP, FP, FN for each method using the NB-CASIA dataset

Methods	TP	FP	FN	F-score
Amerini *et al.* [1]	215	9	40	0.898
Warif *et al.* [14]	237	9	18	0.946
Our method	242	7	13	0.960

5.3 Robustness Test

Based on the previous analysis that showed the effectiveness of our method in terms of reflection attack, in this section we further explore the robustness of the proposed method especially in the case of reflection attack. Thus, we selected an original image at random from NB-CASIA dataset to test the robustness. First, the bird in the image was selected as target area. Then, the target area was

(a) Authentic image (b) Detected result of rotation



(c) Detected result of scaling (d) Detected result of horizontal reflection

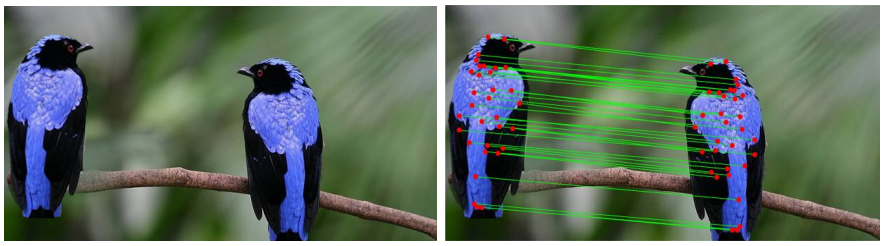
Figure 4: Examples of detected results using our method

copied, flipped horizontally and vertically respectively to create two forged images. The forged images and detected results for horizontal reflection and vertical reflection are shown in Figures 5(a) and 5(b), which indicate that our method performs well in the case of simple reflection.

Next, we created a forged image in the case of vertical reflection with occlusion, where it was actually quite common. The forged image and detected result are shown in Figure 5(c). In view of this kind of situation, the proposed method remains valid. Besides, in practical situations rotation and scaling might be used in combination with reflection attacks, which is a direct challenge to most existing techniques. On account of this, we made the corresponding experiments. Figure 5(d) showed the forged image and detected result, which was created by horizontal reflection and 15 degrees rotation. And Figure 5(e) showed the forged image and detected result, which was generated by horizontal reflection and 70% scaling. Experimental results illustrate that our method is robust enough against combined attacks of geometric transformation and reflection. In the end, we would create a sophisticated forged image involved combined attacks of rotation, scaling and reflection. We copied the bird, flipped it horizontally, scaled it to 75%, rotated it by 17 degrees clockwise, and then pasted it to the left side of the original image. In a similar way, the other duplicate was flipped vertically, scaled to 50%, and then pasted to the right side of the original image. The forged image and the corresponding result detected using our method are shown in Figure 5(f), which demonstrate that our algorithm work well even when the forged image have multiple duplicated regions. The forged image in Figure 5(f) shows the specific scenario that three kinds of attacks including rotation, scaling, reflections and multiple forgery regions coexist simultaneously in an image. Due to the sophisticated scenario in the suspicious image, it is challenge to discern the forgery. To the best of our knowledge, a number of existing methods cease to be effective under the circumstances, however, the detection result of our method is satisfactory.

6 Conclusions

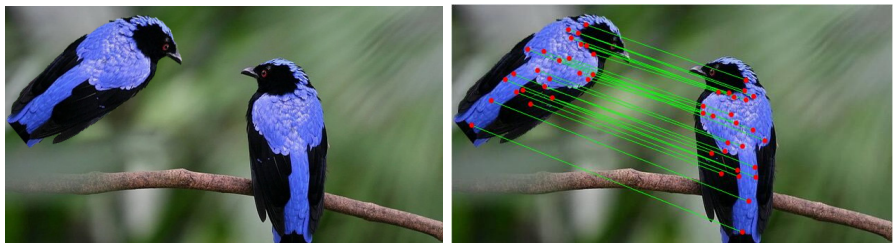
Copy-move forgery detection has been widely studied in the past ten years. However, reflection-based transformation attacks have not been highlighted by prior researchers. The purpose of this work is to achieve high robustness against reflections and any combination of reflection with other geometrical transformation attacks. Thus, we propose a novel feature descriptor called FI-SIFT based on the classical SIFT algorithm which is the core contribution of this paper, and then presented a detection scheme to resist to reflection-based attacks. FI-SIFT cover the reflection-based features by means of modifying the arrangement of feature descriptors. A series of experimental results reveal that the proposed method performs well to detect copy-move forgeries distorted by common attacks including rotation, scaling, reflections and their mixture, especially for the sophisticated scenario, such as multi-objects forgery with combination of reflections. Though having achieved promising performance in detecting sophisticated forgeries with duplicated regions under reflection-based attacks, our method relies on the detection of reliable SIFT key points. For some images with large uniform areas, the SIFT algorithm cannot find sufficient number of reliable key points. In addition, some images have intrinsically identical or similar areas that cannot be differentiated from intentionally pasted copied regions by our method. In the future work, we will con-



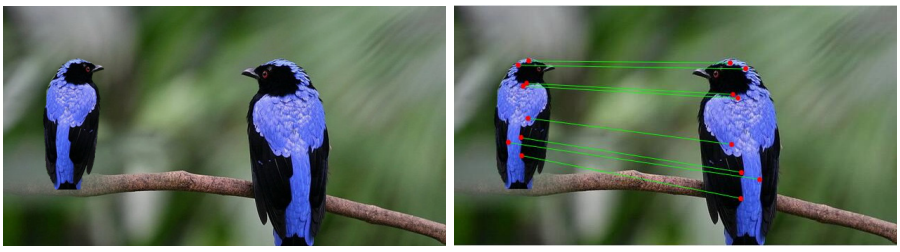
(a) Horizontal reflection

(b) Vertical reflection

(c) Vertical reflection with occlusion



(d) Horizontal reflection with rotation



(e) Horizontal reflection with scaling

(f) Multi-objects forgery with combination of reflections

Figure 5: Examples of forged images and detected results in terms of reflection attacks

sider effective approaches to improve the detection performance for such cases.

Acknowledgments

This work was supported by Natural Science Foundation of Tianjin (Grant # 15JCYBJC15500), China.

References

[1] I. Amerini, L. Ballan, R. Caldelli, *et al.*, "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, 2011.

[2] H. Bay, A. Ess, T. Tuytelaars, "SURF: Speeded up robust features," *Computer Vision and Image Understanding*, vol. 110, no. 3, pp. 346–359, 2008.

[3] X. Bi, C. M. Pun, X. C. Yuan, "Multi-level dense descriptor and hierarchical feature matching for copy-move forgery detection," *Information Sciences*, vol. 345, no. C, pp. 226-242, 2016.

[4] Y. J. Cao, T. G. Gao, L. Fan, *et al.*, "A robust detection algorithm for copy-move forgery in digital images," *Forensic Science International*, vol. 214, no. 1-3, pp. 33-43, 2012.

[5] J. Fridrich, D. Soukalm, J. Lukas, "Detection of copy-move forgery in digital images," in *Proceedings of Digital Forensic Research Workshop*, pp. 55-61, 2003.

[6] X. Guo, X.. Cao, "MIFT: A framework for feature descriptors to be reflection invariant," *Image & Vision Computing*, vol. 30, no. 8, pp. 546-556, 2012.

[7] H. L. Huang, W. Q. Guo, Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," *Proceedings of IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application*, pp. 272-276, 2008.

[8] Y. P. Huang, W. Lu, W. Sun, *et al.*, "Improved DCT-based detection of copy-move forgery in images," *Forensic Science International*, vol. 206, no. 1-3, pp. 178-184, 2011.

[9] D. Jing, W. Wei, T. Tieniu, "CASIA image tampering detection evaluation database," in *IEEE China Summit & International Conference on Signal and Information Processing*, 2013. (`file:///C:/Users/user/Downloads/06625374.pdf`)

[10] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91-110, 2004.

[11] W. Q. Luo, J. W. Huang, G. P. Qiu, "Robust detection of region-duplication forgery in digital image," in *Proceedings of International Conference on Pattern Recognition*, pp. 746-749, 2006.

[12] X. Pan, S. Lyu, "Region duplication detection using image feature matching," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 857-867, 2010.

[13] E. Silva, T. Carvalho, A. Ferreira, *et al.*, "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, 2015.

[14] N. B. A. Warif, A. W. A. Wahab, M. Y. I. Idris, *et al.*, "SIFT-Symmetry: A robust detection method for copy-move forgery with reflection attack," *Journal of Visual Communication & Image Representation*, vol. 46, pp. 219-232, 2017.

[15] B. Xu, J. W. Wang, G. J. Liu, "Image copy-move forgery detection based on SURF," in *Proceedings of International Conference on Multimedia Information Networking and Security*, pp. 889-892, 2010.

[16] M. Zandi, A. Mahmoudi-Aznaveh, A. Talebpour, "Iterative copy-move forgery detection based on a new interest point detector," *IEEE Transactions on Information Forensics & Security*, vol. 11, no. 11, pp. 2499-2512, 2011.

[17] J. Zhao, J. C. Guo, "Passive forensics for copy-move forgery using a method based on DCT and SVD," *Forensic Science International*, vol. 233, no. 1-3, pp. 158-166, 2013.

Biography

Youjian Yu is a lecturer in the department of computer science and technology, Tianjin Chengjian University. He received the M.S. degree from Communication University of China in 2013. Since 2004, he has been working in the school of computer and information engineering, Tianjin Chengjian University. His current research interests include image processing and computer vision.

Guangfu Wang is an engineer in Tianjin Surveillance Technology Company Limited. In 2011 he obtained his M.S. degree from Warwick University in computer science and application, UK. His main research interests are computer vision and deep learning.

Jie Zhao is a lecturer in the department of electronic information engineering, Tianjin Chengjian University. In 2015 he received the Ph.D. degree from Tianjin University in information and communication engineering, China. Since 2009, he has been working in the school of computer and information engineering, Tianjin Chengjian University. His current research interests include digital image forensics and computer vision.