Journal of Information Hiding and Multimedia Signal Processing ©2016 ISSN 2073-4212
Ubiquitous International Volume **7**, Number **2**, March **2016**

An Improved SIFT-Based Copy-Move Forgery Detection Method Using T-Linkage and Multi-Scale Analysis

Yi Fan, Yue-Sheng Zhu and Zhen Liu

Communication and Information Security Lab
Institute of Big Data Technologies, Shenzhen Graduate School
Peking University, China
fanyi@sz.pku.edu.cn; zhuys@pku.edu.cn; l.zhen@sz.pku.edu.cn

Received August, 2015; revised October, 2015

Abstract. *The detection of copy-move forgery is an important module in the image authentication. It aims to detect whether an image contains copy-move tampering and where the tampered regions are. To improve the detection accuracy, in this paper we propose to apply local feature matching, followed by T-Linkage and multi-scale analysis by employing the T-Linkage algorithm for robust clustering in the space of geometric transformation. We further capture coarse-to-fine information by constructing a multi-scale image representation and locating duplicated regions for each scale. We make a final decision by considering all the localization maps with a voting strategy. Experimental results show that the proposed method achieves desirable detection and localization performance on different copy-move attacks.*
Keywords: Copy-move forgery detection, SIFT, T-Linkage, Multi-scale analysis.

1. **Introduction.** With the advent of digital pictures and relative ease of digital image processing, it becomes difficult to determine whether an image is authentic. Sometimes it can be a severe problem when images are used as evidence in a court of law. Therefore it is important to detect whether an image has been tampered with. Copy-move tampering is a common type of image forgery. So far, the research on copy-move forgery detection has become a hot topic and lots of work has been done to address this issue.

Osamah *et al.* [1] and Christlein *et al.* [2] made comprehensive descriptions of the current state-of-the-art passive copy-move forgery detection methods. Generally speaking, these techniques are classified into two main categories: block-based and keypoint-based methods. Different block-based methods [3-11] have been previously proposed such as discrete cosine transform (DCT) [3],discrete wavelet transform (DWT) [4] principle component analysis (PCA) [5], singular value decomposition (SVD) [6], blur invariants [7] , zernike [8]*etc.* However, copy-move tampering always involves geometric transformations (*e.g.* rotation, scaling, *etc.*) to get a better visual effect, which makes it more difficult for the detection. It has been demonstrated that block-based methods usually result in low robustness to geometric transformations as well as significant false positives and computational complexity.

On the other hand, keypoint features such as scale invariant feature transform (SIFT) [12] and speeded up robust features(SURF)[13], have been utilized to deal with the above problems due to their low computational complexity of non-blocks and invariance to

scale, rotation and illumination. Keypoint-based methods [14-16] have been proven to work effectively for copy-move forgery detection. Particular differences of these methods lie in the postprocessing of the matched features. Amerini *et al.* [14] applied a robust feature matching procedure and hierarchical agglomerative clustering (HAC) algorithm to separate different cloned areas after SIFT feature extraction. This technique is able to precisely individuate the altered area with high reliability but is unsatisfactory in the cases where the copied patch contains pixels that are very distant among them or the pasted area is near to the original source. In [15], Amerini *et al.* presented an effective clustering procedure with J-Linkage algorithm [17], which adopts a conceptual representation of points with binary preference analysis and groups points in the space of geometric transformation. The method is demonstrated to have superior detection and localization performance to previous spatial clustering, while representing points with hard thresholding may not be feasible in practical applications. Furthermore, much finer information should be considered to achieve more accurate detection.

In this paper, we propose to use SIFT features to address copy-move detection. The main contribution lies in two folds: first, following keypoint extraction and matching, a clustering algorithm called T-Linkage [18] is applied. T-Linkage, which adopts a general conceptual representation of keypoints with soft thresholding, is proven to perform better than J-Linkage in terms of clustering accuracy and robustness to outliers. Second, to accurately detect the tampered regions in pixel level, an adapted multi-scale analysis [19] is introduced. In other words, we construct a multi-scale image representation and examine the acquired clusters with circle block features [9] to yield a localization (pixel-level detection) map for each scale. The final localization map will be obtained via a voting process. Experiments have been performed to demonstrate the effectiveness of the proposed method in terms of authenticity detection performance and of localization accuracy in the tampered patches.

The rest of this paper is organized as follows. Section 2 presents the proposed method. Section 3 gives some experimental results. Conclusion is drawn in section 4.

2. **Methodology.**

Inspired by some literature approaches that aim at dealing with hard copy-move manipulations, such as rotation, scaling and composite operations, we have come up with an approach that involves T-Linkage clustering and multi-scale analysis. Our method is composed of six steps: (i) keypoint extraction, (ii) keypoint matching, (iii) T-Linkage clustering, (iv) pyramidal decomposition, (v) multi-scale analysis, and finally (vi) voting. The pipeline of our approach is depicted in Fig. 1.

2.1. **Keypoint extraction.**

To achieve invariance to rotation and scaling, we extract keypoints by using the scale invariant feature transform (SIFT) algorithm [12]. The SIFT algorithm can be roughly summarized as the following four steps: (i) scale-space construction, (ii) keypoint extraction, (iii) canonical orientations assignment, and (iv) keypoint descriptors generation. In result, each keypoint is described as a 128-dimensional vector. Let $\boldsymbol{S} := \{\boldsymbol{s}_1, \boldsymbol{s}_2, ..., \boldsymbol{s}_n\}$ be the list of n keypoints taken from the image.

2.2. **Keypoint matching.**

SIFT keypoints from the copied and the original regions have similar descriptor vectors. Thus, keypoint matching is essential to detect if an image has been tampered with. To this end, we use the g2NN test proposed by Amerini *et al.*[14].

The g2NN test is a generalization of 2NN test which considers the ratio between the nearest neighbor and the second nearest one. For a given keypoint, $D := \{d_1, d_2, ..., d_{n-1}\}$ is defined as the sorted Euclidean distances with respect to other keypoints. The keypoint corresponding to d_1 is considered a match of the given keypoint only if the ratio d_1/d_2 is lower than a fixed threshold α (in our experiments we set this value to 0.5). A very high

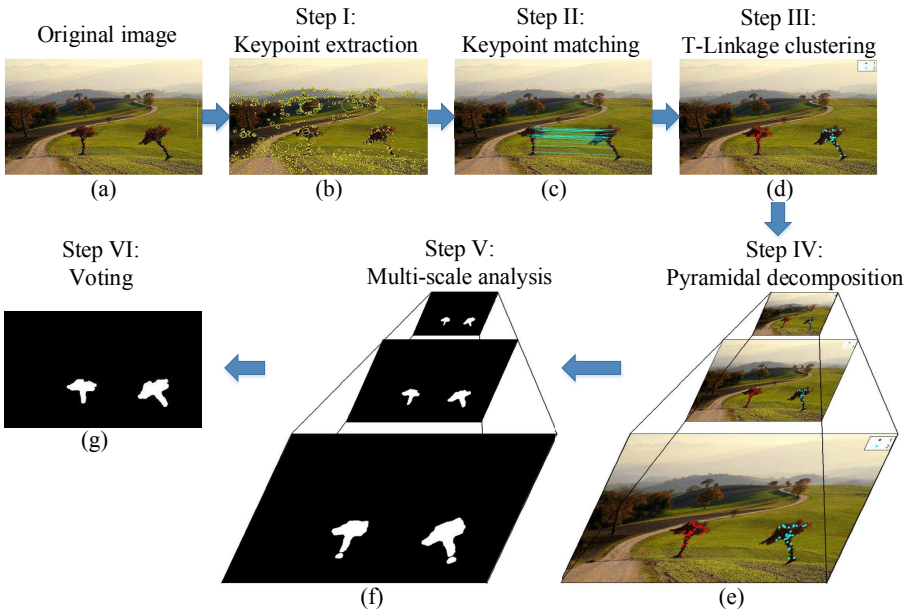

FIGURE 1. Outline of the proposed method.

ratio (*e.g.* greater than α) means two random features. The g2NN test iterates the 2NN test between d_i/d_{i+1} until this ratio is greater than α, which is able to match multiple copies. That is to say, if k is where the procedure stops, each keypoint in correspondence to a distance in $\{d_1, ..., d_{k-1}\}$ is regarded as a match for the inspected keypoint. After using the g2NN test on all the keypoints $\boldsymbol{S}$, we obtain a set of matched pairs $\boldsymbol{P} := \{\boldsymbol{p}_1, ..., \boldsymbol{p}_q\}$.

2.3. **T-Linkage clustering.** In order to group keypoints, T-Linkage algorithm [18] is applied with a continuous conceptual representation of points. This method starts with randomly selecting matched pairs to generate m affine transformation hypotheses. Thereafter, for each matched pair, a preference function(PF) is defined indicating which transformation the pair prefers and how much it prefers. The PF ϕ is described as follows:

$$\phi(\mathbf{h}) = \begin{cases} e^{-d(\mathbf{x},\mathbf{h})/\tau} & \text{if } d(\mathbf{x},\mathbf{h}) < 5\tau \\ 0 & \text{if } d(\mathbf{x},\mathbf{h}) \geq 5\tau \end{cases} \tag{1}$$

where $\xi = 5\tau$ is an inlier threshold indicating whether a point votes for the m hypotheses $\boldsymbol{H} = \{\boldsymbol{h}_j\}_{j=1,...,m}$; ϕ is set to zero when the residual is no smaller than ξ and takes values from (0,1] otherwise. Consequently, the PF of each point can be figured as an m-dimensional vector.

Prior to hierarchical agglomerative clustering (HAC), a conceptual representation of clusters and an appropriate similarity measure are defined. The preference function of a subset of data points $\boldsymbol{S}$ is a vector $\boldsymbol{p} \in [0,1]^m$ with its i-th component defined in (2), where $\boldsymbol{q}_{\mathbf{x}}$ denotes the preference function of $\mathbf{x}$. And the similarity measure between clusters is provided by the *Tanimoto distance* [20] in (3).

$$(\mathbf{p})_i = \min_{\mathbf{x} \in \boldsymbol{S}} (\mathbf{q}_{\mathbf{x}})_i \tag{2}$$

$$d_T(\mathbf{p},\mathbf{q}) = 1 - \frac{< \mathbf{p},\mathbf{q} >}{||\mathbf{p}||^2 + ||\mathbf{q}||^2 - < \mathbf{p},\mathbf{q} >} \tag{3}$$

The clusters that contain less than N matched pairs are discarded in order to remove possible outliers; this aspect has been further investigated in the experimental section in which different detection results are given changing this N value. Finally, if there is at

least one (more for multiple clones) inliers cluster, the image is considered as forged and vice versa.

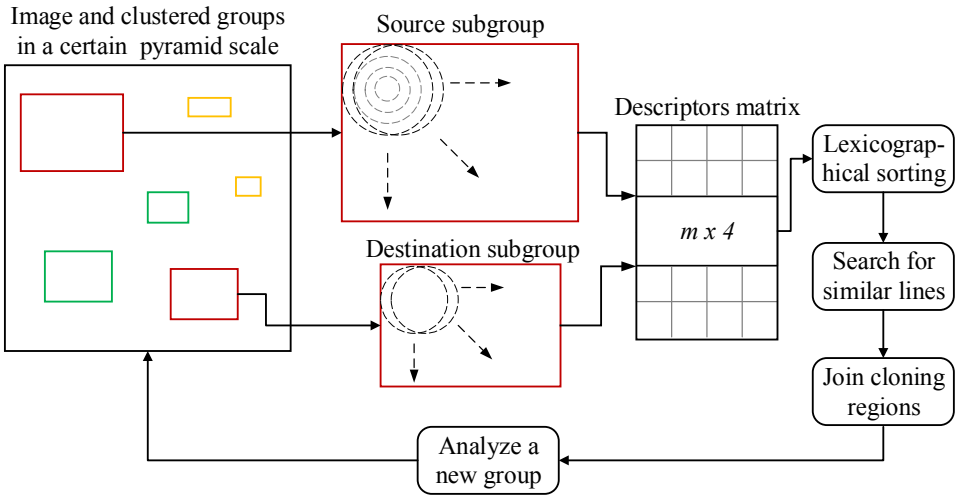

FIGURE 2. Overview of multi-scale analysis.

2.4. **Pyramidal decomposition.** In this step, we construct a multi-scale space. The bottom of the pyramid is the original image, the second-last level is an image with size of 25% of the original size and so further. In order to maintain semantic consistency with the image, the clustered groups found in section 2.3 also need to be downscaled proportionally. For instance, from the bottom of the pyramid to the second-last, the image has its height and width decreased by a factor of 0.5. The factor will be used to adjust the groups accordingly. Analogously, the resizing factor is 0.25 for the next level, and so on. This step guarantees equivalent information of the inspected regions (groups) between two neighboring levels. In the next step, all images and the corresponding groups are individually analyzed.

2.5. **Multi-scale analysis.** In order to achieve better detection in pixel level, multi-scale analysis is applied to capture coarse-to-fine information. For each scale in the pyramid, our analysis procedure is a little different from the reference approach [19]. We convert the image to grayscale to get a lower dimensional descriptor of each pixel block. The whole procedure is illustrated as follows:

- We slide a circular window through the corresponding groups one by one. The mean of the four concentric circles inside the window is adopted to make a four dimensional descriptor analogous to what is proposed by Wang *et al.* [9]. It is to be noted that the matched regions (source and destination subgroups) will be analyzed individually.
- The descriptors of each subgroup will be stored in a matrix and are lexicographically sorted.
- Search for similar descriptors in the sorted matrix. Two blocks are regarded as duplicated only if they belong to distinct subgroups (source and destination).
- By using a minimum bounding rectangle (MDR) algorithm to join the cloning candidate regions from a subgroup, a localization map at a given pyramid scale is acquired.

A detailed overview of multi-scale analysis is depicted in Fig. 2. All the localization maps are generated after processing all the images in the pyramid.

2.6. **Voting.** Voting is a good tradeoff to balance the correct and incorrect detections with regard to the threshold α mentioned in section 2.2. If we increase the threshold in order to effectively detect cloned regions, false positives may also increase. Therefore, a voting process is proposed by combining all the localization maps. It is worth mentioning that the small maps have to be resized to match the size of the larger one. It considers as duplicated blocks only those classified as such in the majority of the maps. Finally, all the blocks constitute the final localization map.

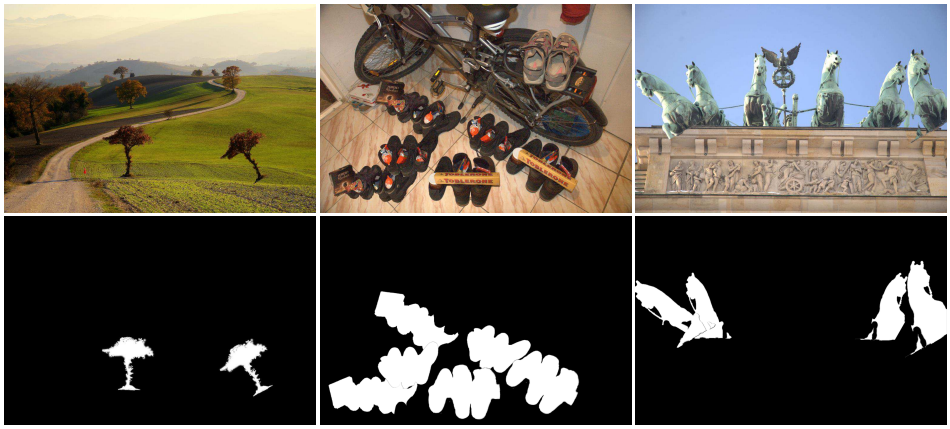

FIGURE 3. Example images of MICC-F600 dataset.

3. **Experiments.** In this section, We evaluate the performance of the proposed method not only from the view of detecting whether the image is forged (authenticity detection) but also for exploring the real intention of the forger and for further recovery (patch localization).

3.1. **Dataset.** MICC-F600 [21] is a novel dataset, which is composed of 600 high resolution images (ranging from 800*533 to 3888*2592 pixels) containing realistic and challenging copy-move attacks as shown in Fig. 3. Among these 600 images, 440 are original and 160 are tampered. Every tampered image has its own reference map (groundtruth shown in the second row of Fig. 3) indicating the original and cloned regions in white color.

3.2. **Evaluation metrics.** Authenticity detection performance is measured in terms of true positive rate (TPR) and false positive rate (FPR). TPR indicates the fraction of tampered images correctly identified as such and FPR indicates the fraction of original images that are not correctly classified. For patch localization performance, we choose the following three metrics:

- True positive rate (TPR): indicates the percentage of cloned patches (source and destination) that are correctly located.
- False positive rate (FPR): indicates the percentage of normal (non-cloned) patches that are incorrectly detected.
- Accuracy (ACC): represents the comprehensive quality of TPR and TNR (true negative rate, TNR=1-FPR), which indicates the percentage of correctly classified non-cloned patches.

3.3. **Parameter selection.**

3.3.1. *T-Linkage clustering.* As is mentioned in section 2.3, we need to determine an appropriate setting for the cutoff threshold in the preference function. To address this issue, the following experiment has been established applying a four-fold cross-validation process: from the database of 600 images (MICC-F600), 450 (120 tampered and 330 original), which is 3/4 of the image set, have been randomly chosen to perform a training to find the best threshold for T-Linkage; the remaining 150 images (1/4 of the whole set) have been used in a successive testing phase to evaluate the authenticity detection performance of the proposed technique. The experiment is repeated four times, by cyclically exchanging the four image subsets belonging to the training (3 subsets) and to the testing set (1 subset), and the results have been averaged. It should be noted that we set N (the least number of matched pairs to form an inliers cluster) to 9 in this experiment.

Table 1. Training phase: TPR and FPR with respect to ξ

ξ	0.01	0.02	0.03	**0.04**	0.05	0.06	0.07	0.08	0.09	0.10
TPR(%)	84.29	84.64	85.46	**85.73**	85.76	85.89	86.02	86.15	86.29	86.58
FPR(%)	2.93	3.04	3.54	**3.86**	4.15	4.49	5.50	5.98	6.30	7.80

Table 2. Testing phase: authenticity detection results

ξ	TPR(%)	FPR(%)
0.04	86.45	4.50

In Table 1, the TPR and FPR acquired during the training phase are reported with respect to the threshold ξ, which varies in the interval [0.01, 0.10] with steps of 0.01. The goal is to minimize the FPR while maintaining a very high TPR. It can be seen that TPR is completely very high, while FPR is relatively variable. The optimal threshold ξ has been chosen as 0.04 for the minimum Euclidean distance from the ideal performance (TPR = 100% and FPR = 0%). Finally, the testing phase has been launched for the best metrics using $\xi = 0.04$. The final detection result is presented in Table 2, which reveals that the proposed method performs satisfactorily, providing a low FPR while keeping a competitive TPR. Therefore, $\xi = 0.04$ will be used in the following experiments.

3.3.2. *Multi-scale analysis.* In order to select appropriate parameters for multi-scale analysis, we have created a small set of images originating from the benchmark database constructed by Christlein *et al.* [2]. We use the base images and copied snippets to create some images that include rotation, resizing and combination of these operations. By a visual analysis of the final localization maps, the following settings of parameters are determined. Both spatial and similarity distance are calculated as Euclidean norm.

- sliding window size: 9*9 pixels (radius equal to 4 pixels);
- number of decomposition steps: 2 steps (in this case the pyramid has 3 levels with the original image at the bottom);
- number of neighboring lines to be compared in the sorted matrix of descriptors: 5 lines (a given descriptor only compares to 5 subsequent lines);
- minimum spatial distance between pixel blocks to be compared: 30 pixels (if lower, the inspected group is discarded);
- minimum similarity distance between descriptors: 0.05 (if lower, the inspected group is discarded);
- minimum number of pixel block matches in a group: 3 matches (if less, the group is discarded).

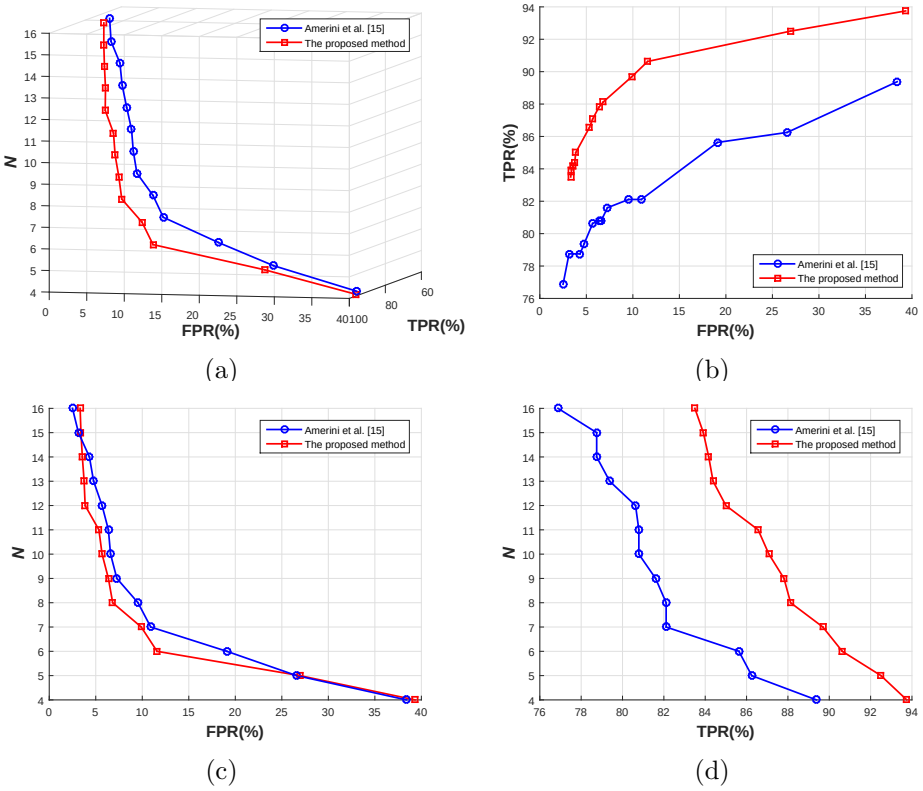

FIGURE 4. ROC curve of TPR vs FPR varying N. (a) 3D view; (b) 2D view from the angle of N; (c) 2D view from the angle of TPR; (c) 2D view from the angle of FPR.

3.4. **Quantitative experiments on authenticity detection performance.** To assess the performance of authenticity detection, experiments on MICC-F600 dataset are carried out in comparison with the reference technique described by Amerini *et al.* [15]. The main difference lies in the clustering approach: J-Linkage is applied in [15], while the proposed method adopts T-Linkage. T-Linkage is a continuous generalization of J-Linkage since J-Linkage depicts the point preferences only in $\{0, 1\}$, while T-linkage expresses them more accurately in the whole closed interval $[0, 1]$, which integrates more specific information on residuals between point pairs and transformation hypotheses. Therefore T-Linkage achieves less misclassification error and more robustness to outliers than J-Linkage for multi-model fitting, which has been demonstrated by Magri *et al.* [18]. The following experimental results verify that the proposed method outperforms the method in [15].

Fig. 4 shows the averaged detection results obtained by varying the parameter N within the interval [4,...,16] compared with the method described in [15]. The ROC curve reveals that the detection performance has been greatly improved. It is to be noted that when $N = 4$, it achieves a good TPR (93.75%) but it presents a high FPR (39.32%). However, this effect is reduced as N increases which means more points give consensus to the transformations. For example, when $N = 7$ we achieve good performance with a still high TPR (89.69%) and a low FPR (9.89%). The ideal result is the most upper left point: TPR = 100% and FPR = 0%. Considering the minimum Euclidean distance from the ideal point, $N = 8$ yields the best result. Table 3 reports the detailed results of our method and the procedure described in [15]. Results are reported for three values of the parameter N (7, 8 and 9). As for $N = 8$, the proposed technique achieves superior

TABLE 3. Comparative results between Amerini *et al.* [15] and our method on authenticity detection

(%)	N=7		N=8		N=9	
	Ours	[15]	Ours	[15]	Ours	[15]
TPR	89.69	82.11	**88.13**	82.11	87.81	81.6
FPR	9.89	10.91	**6.82**	9.54	6.36	7.27

TABLE 4. Comparative results between several state-of-the-art methods and our method on copy-move patch localization

(%)	Avg.ACC	Std.ACC	Avg.TPR	Std.TPR	Avg.FPR	Std.FPR
Ours	**89.64**	**14.01**	**80.34**	**28.12**	**1.06**	**1.88**
Amerini *et al.* [15]	87.92	21.98	76.82	31.42	0.98	1.87
Silva *et al.* [19]	85.35	13.14	71.92	26.69	1.22	1.92
Bashar *et al.* [4]	65.99	18.05	32.10	33.85	0.12	0.94
Ryu *et al.* [8]	64.54	23.39	34.31	44.25	5.24	7.72
Fridrich *et al.* [3]	64.16	16.85	28.35	31.48	0.03	0.12
Wang *et al.* [9]	61.62	16.55	23.32	32.08	0.08	0.61
Kang *et al.* [6]	58.35	16.35	16.72	31.67	0.03	0.10
Mahdian *et al.* [7]	57.27	15.13	14.56	28.21	0.03	0.14
Popescu *et al.* [5]	57.18	14.93	14.38	27.77	0.03	0.16

performances: 6.02% of improvement for TPR and 2.72% of reduction for FPR. Therefore, N is set to 8 for the following localization.

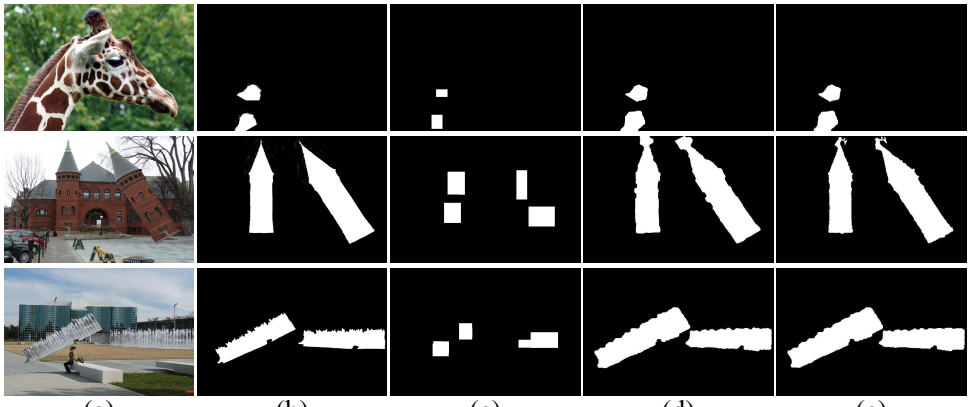

FIGURE 5. Comparative examples for patch localization. (a) shows three tampered images, (b) reports the groundtruth maps, (c) presents the result of [19], (d) displays the result of [15], and (e) indicates our result.

3.5. **Quantitative experiments on patch localization performance.** To assess the performance of patch localization, experiments are carried out in comparison with other relevant methods: one is described by Amerini *et al.* [15], who applied zero mean normalized cross-correlation (ZNCC) algorithm to locate the duplicated regions based on SIFT descriptors; one is illustrated by Silva *et al.* [19], who analogously adopted multi-scale analysis but with different matching and clustering strategies based on SURF descriptors; the rest are several state-of-the-art block-based methods [3-9]

For each localization map, we compared it to the respective reference map at the pixel level and calculated the TPR, FPR and ACC metrics. Table 4 presents the averaged results implemented on all the detected forged images after T-Linkage clustering. As shown in Table 4, our approach has achieved the highest ACC, which indicates that the proposed method is good to detect and locate copy-move forgeries containing different operations. The standard deviation in ACC is a little higher than the method proposed by Silva *et al.* [19] but much lower than the rest methods, which means our method has favorable robustness to challenging images. As for the competitive methods proposed by Silva *et al.* [19] and Amerini *et al.* [15], we present some comparative localization examples in Fig. 5.

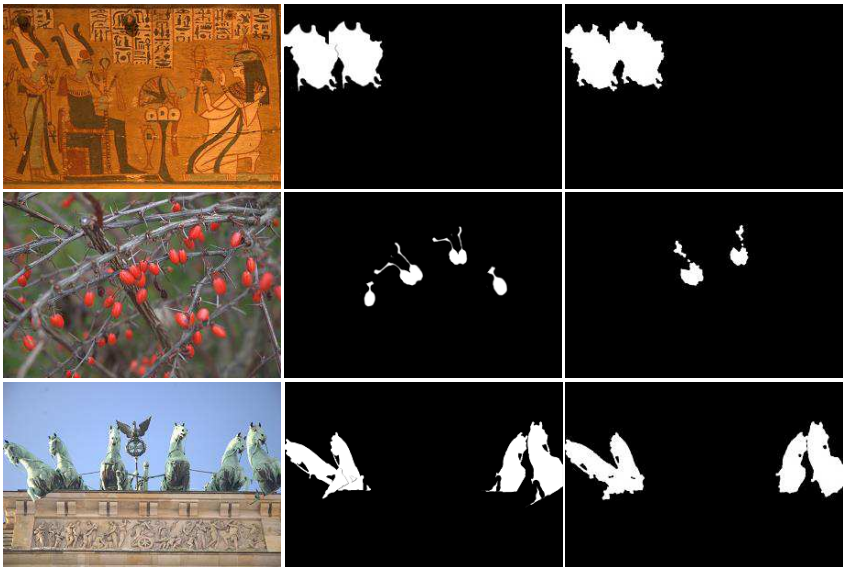

FIGURE 6. Qualitative results in different copy-move attacks. (a) shows three tampered images, (b) reports the groundtruth maps, and (c) presents the binary localization results.

3.6. **Qualitative experiments on patch localization performance.** In this experiment, we have qualitatively evaluated the proposed method with images containing some challenging operations: (i) simple cloning, (ii) rotation, (iii) scaling, and (iv) composite operations. Fig. 6 depicts the qualitative results. We can see that the proposed method performs well in most cases. But it fails when detecting very small tampered regions, which may be caused by two parameters, *i.e.* the minimum number of matched pairs in an inliers cluster and the minimum number of pixel block matches in a group. The parameters can be adjusted with regard to different needs or certain circumstances.

4. **Conclusions.** In this paper, our method introduces and combines some well-established concepts to address the copy-move forgery problem. Keypoint extraction and matching are fundamental steps to spot out the cloned fields. In the T-linkage clustering step, we apply a robust clustering strategy to group keypoints in the geometric transformation domain with soft thresholding. Here we can decide whether the image is tampered or not. Then an adapted multi-scale analysis explores coarse-to-fine information within these clusters to detect cloned regions in pixel level. This idea combines with a voting step to produce the final localization map. We carried out parameter tuning and comparison to validate our approach. Experimental results demonstrate that the proposed method has good performance in terms of both authenticity detection and patch localization tasks.

Acknowledgment. This work was supported by Shenzhen Engineering Laboratory of Broadband Wireless Network Security, and the Science and Technology Development Fund of Macao SARFDCT056/2012/A2 and UM Multi-year Research Grant MYRG144(Y1-L2)-FST11-ZLM.

REFERENCES

[1] O. M. Al-Qershi and B. E. Khoo, Passive detection of copy-move forgery in digital images: State-of-the-art, *Forensic science international*, vol. 231, no. 1, pp. 284–295, 2013.

[2] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, An evaluation of popular copy-move forgery detection approaches, *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 6, pp. 1841–1854, 2012.

[3] A. J. Fridrich, B. D. Soukal, and A. J. Lukkas, Detection of copy-move forgery in digital images, *in Proceedings of Digital Forensic Research Workshop*, 2003.

[4] M. Bashar, K. Noda, N. Ohnishi, and K. Mori, Exploring duplicated regions in natural images, 2010.

[5] A. C. Popescu and H. Farid, Exposing digital forgeries by detecting duplicated image regions, *Dept. Comput. Sci., Dartmouth College, Tech. Rep.* TR2004-515, 2004.

[6] X. Kang and S. Wei, Identifying tampered regions using singular value decomposi- tion in digital image forensics, *International Conference on Computer Science and Software Engineering*, vol. 3, pp. 926–930, 2008.

[7] 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, 2007.

[8] S.-J. Ryu, M. Kirchner, M.-J. Lee, and H.-K. Lee, Rotation invariant localization of duplicated image regions based on zernike moments, *IEEE Trans. on In- formation Forensics and Security*, vol. 8, no. 8, pp. 1355–1370, 2013.

[9] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, Detection of image region duplica- tion forgery using model with circle block, *International Conference on Multimedia Information Networking and Security*, vol. 1, pp. 25–29, 2009.

[10] L. Li, S. Li, H. Zhu, S.-C. Chu, J. F. Roddick, and J.-S. Pan, An e cient scheme for detecting copy-move forged images by local binary patterns, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 1, pp. 46–56, 2013.

[11] L. Li, S. Li, H. Zhu, and X.Wu, Detecting copy-move forgery under ane transforms for image forensics, *Computers Electrical Engineering*, vol. 40, no. 6, pp. 1951-1962, 2014.

[12] D. G. Lowe, Distinctive image features from scale-invariant keypoints, *Interna- tional journal of computer vision*, vol. 60, no. 2, pp. 91–110, 2004.

[13] H. Bay, T. Tuytelaars, and L. Van Gool,Surf: Speeded up robust features, *in Proceedings of European Conference on Computer Vision*, pp. 404–417, 2006.

[14] 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 Trans. on Information Forensics and Security*, vol. 6, no. 3, pp. 1099–1110, 2011.

[15] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, L. Del Tongo, and G. Serra, Copy-move forgery detection and localization by means of robust clustering with J-Linkage, *Signal Processing: Image Communication*, vol. 28, no. 6, pp. 659–669, 2013.

[16] B. Shivakumar and S. Baboo, Detection of region duplication forgery in digital images using SURF, *International Journal of Computer Science Issues*, vol. 8, no. 4, 2011.

[17] R. Toldo and A. Fusiello,Robust multiple structures estimation with J-Linkage, in Proceedings of European Conference on Computer Vision, pp. 537–547, 2008.

[18] L. Magri and A. Fusiello, T-linkage: a continuous relaxation of J-Linkage for multi-modeleing, *Conference on Computer Vision and Pattern Recognition*, pp. 3954–3961, 2013.

[19] 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 pro- cesses, *Journal of Visual Communication and Image Representation*, vol. 29, pp. 16–32, 2015.

[20] T. Tanimoto, IBM Internal report 17th, 1957.

[21] G. Serra, MICC-F600 dataset, 2012. http://giuseppeserra.com/content/sift-based forensic-method-copy-move-detection.