Copy-move Forgery Detection in the Presence of Similar but Genuine Objects

Ye Zhu[1, 2], Tian-Tsong Ng[2], Bihan Wen[3], Xuanjing Shen[1], Bin Li[4]

[1]College of Computer Science and Technology, Jilin University, China

[2]Institute for Infocomm Research, A*STAR, Singapore

[3]Electrical and Computer Engineering and CSL, University of Illinois at Urbana-Champaign, USA

[4]Shenzhen Key Laboratory of media information content security, Shenzhen University, China

[1]zhuye13@mails.jlu.edu.cn; xjshen@jlu.edu.cn, [2]ttng@i2r.a-star.edu.sg, [3]bwen3@illinois.edu, [4]libin@szu.edu.cn

***Abstract*— Images often contain *Similar but Genuine Objects* (SGO), such as two beverage bottles, similar windows, *etc*. This poses a natural but unexplored challenge to existing copy-move forgery detection methods with an assumption that similar regions are always manipulated for forgery purpose. In this work, we investigate the limitations of the existing CMFD methods under the SGO setting, and propose a new one with performance improvement. Our method consists of the following key steps: first, pyramid scale space and orientation assignment are used for feature extraction to ensure scaling and rotation invariance; second, combined features are applied for effective texture description; third, similar features between two points are matched through RANSAC to reduce false matches; last, tampered regions are located and correlation coefficient are computed on those regions. The experimental results indicate that the proposed algorithm is effective in detecting SGO and copy-move forgery, and compares favorably to existing methods. Furthermore, our method exhibits robustness under geometric transformation and certain forms of post-processing.**

Keywords-Image copy-move forgery; similar but genuine objects; combined feature extraction

I. Introduction

Copy-move image forgery which copies one part of the image, and paste it into another part of the same image is one of the most common form of image tampering. Various Copy-Move Forgery Detection (CMFD) methods have been proposed, and they can be roughly categorized as block-based or key-point-based matching methods. The first block-based CMFD algorithm by Fridrich [3] is based on lexicographical search in DCT (Discrete Cosine Transform) space. Several improved DCT-based methods were subsequently proposed [4, 5]. Meanwhile, Muhammad et al. [6] proposed a method based on Dyadic Wavelet Transform (DyWT), which made use of both approximation and detail wavelet subbands. Some algorithms attempt to improve computational efficiency of the DCT methods through dimensional reduction using Principal Component Analysis (PCA) [7]. To make CMFD methods robust to geometric transformation block matching through Fourier-Mellin Transform (FMT) [8], invariant moment [9, 10], and Local Binary Patterns (LBP) [11] were proposed.

On the category of key-points based methods, Huang et al. [12] proposed CMFD algorithm using Scale Invariant Feature Transform (SIFT) features. Subsequently, a few improved SIFT-based methods are proposed [1, 13]. Xu et al. [2] and Shivakumar et al. [14] used Speeded-Up Robust Feature (SURF) instead of SIFT feature to improve computational efficiency. Other methods based on DAISY descriptor [15] and scaled ORB[16] are recently proposed for better keypoint matching.

The conventional CMFD approaches are based on the simple assumption that the similar regions in the image are always made by copy-move forgery [1-16]. On the other hand, recent study introduced the concept of the Similar but Genuine Objects (SGO), which turned out to be commonly observed in realistic scenes[17]. It challenged the conventional CMFD methods, as their forgery detection accuracies are observed to degrade when tested on the dataset with SGOs. In this work, we proposed a novel CMFD method using *Scaled Harris Feature Descriptors* (SHFD), which demonstrates robust performance even under the scenarios containing SGOs.

The key intuitions of our method are as follows. (1) The traditional copy-move forgery detection algorithms locate the tampered regions by matching feature extracted in a small local block or patch. This results in reduced ability in distinguishing true copy-move regions, from SGO regions, without explicit understanding on global transformation. It is not surprising that SGO are often mistaken as tampered region in existing methods. To address this issue, our method evaluates matching based on geometric transformation on entire region of interest. We assume that true copy-move image regions have a restricted form of linear geometric transformation such as rotation and scaling from the source regions, whereas the geometric transformation between SGO regions is in general nonlinear, which is higher degree of freedom. (2) Apart from geometric transformation matrix, larger pixel value difference between the target and source regions is another telltale sign for SGO in contrast to true copy-move regions. Therefore, we also compute the correlation coefficient between source regions (convex hull of match feature points at the source object) and their corresponding target regions (obtained by transforming the source region geometrically) pixel-wise to help distinguishing SGO regions from true copy-move regions.

II. Proposed Method

In this section, we present our proposed SHFD method, which consists of five main steps: Scaled Harris point extraction (Sec. *A*), Orientation assignment (Sec. B), features extraction (Sec. *C*), feature matching (Sec. *D*) and Tampered regions location and correlation coefficient computation (Sec. *E*), as is shown in Fig.1.

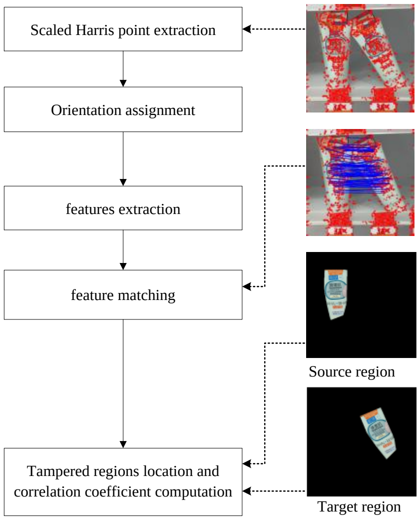


Fig. 1. The framework of proposed method.

A. Scaled Harris Point Extraction

Detecting locations with similar local image appearance is challenging as feature representation may not be scale-invariant. This problem can be overcome by identifying stable features in scale space [17]. A pyramid scale space is a multi-resolution representation of an image which is useful for multi-resolution analysis that can lead to scale invariance property.

Harris point [18] is a classical way to extract corner points. To make Harris point scale-invariant, we compute Harris points in scale-space image pyramid. Images in the scale-space image pyramid are generated by Gaussian smoothing and sub-sampling. We first generate a 4-level image pyramid by successively subsample an image in 1.25:1. Subsequently, we progressively Gaussian kernel smooth each image in the 4-level pyramid to generate a set of 4 images in each level, recorded as $L(x, y)$.

Harris points are computed using the eigenvalues, λ_1 and λ_2, of the second moment $M(x, y)$ of an image as:

$$M(x,y)=\begin{bmatrix} I_x(x,y)^2 & I_x(x,y)I_y(x,y) \\ I_x(x,y)I_y(x,y) & I_y(x,y)^2 \end{bmatrix} \quad (1)$$

where $I_x(x,y)$ and $I_y(x,y)$ respectively represent the directional derivative image in the x and y direction at (x,y) location. If $\lambda_1 \approx \lambda_2$ and $\lambda_1\lambda_2 \gg 0$, a point (x,y) is considered as a corner point, and its corner response can be measured by the following:

$$CR = \det(M) - k \bullet \mathrm{tr}(M)^2 \quad (2)$$

where $\det(M)=\lambda_1\lambda_2=I_x^2I_y^2-(I_xI_y)^2$, $\mathrm{tr}(M)=\lambda_1+\lambda_2=I_x^2+I_y^2$, and k is the weight value. Corner response is compared to a threshold value T for Harris point detection. In our case, the scaled Harris key points are extracted on every image in the scale-space image pyramid.

B. Orientation assignment

To achieve rotation invariance, we rotate each key point based on its dominant orientation. For that, we compute the gradient magnitude, $m(x,y)$, and orientation, $\theta(x,y)$ on each scale-space image by using pixel differences as shown in the following equations:

$$m(x,y)=\sqrt{\Delta L_x{}^2+\Delta L_y{}^2} \quad (3)$$

$$\theta(x,y)=\tan^{-1}(\Delta L_y/\Delta L_x) \quad (4)$$

where $\Delta L_x=L(x+1, y)-L(x-1, y)$, $\Delta L_y=L(x, y+1)-L(x,y-1)$. We then derive a histogram of gradient with 10 bins from the neighborhood of a key point. The peak of the histogram gives us the dominant orientation, and we rotate a key point region at the original coordinate frame (x,y) as follows:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} \quad (5)$$

where $[x', y']^{\mathrm{T}}$ are the coordinates of rotated region, and θ is the dominant orientation of key point (x, y).

C. Feature descriptor extraction

Accurate feature description is important for capturing the subtle image details for distinguishing SGO from true copy-move. Local Binary Patterns (LBP) [20] is an effective texture descriptor. Besides having low computational complexity, LBP is invariant to monotonic grayscale changes.

We compute LBP of various configurations in a 4×4 neighborhood denoted by M. Uniform LBP ($LBP_{P,R}^{u2}$) and the rotation invariant uniform LBP ($LBP_{P,R}^{riu2}$) are computed different P and R settings, where P is the number of pixels in neighborhood on a circle of radius R. For robust representation against noise, we also perform DCT transform on the LBP coefficients on M and extract the top four singular values through singular value decomposition. The final 93-dimensional feature vector is a combination of 59-dimensional $LBP_{P,R}^{u2}$ (P=8, R=1) coefficients, 14-dimensional $LBP_{P,R}^{riu2}$ (P=16, R=2) coefficients, 16-dimensional DCT coefficients and 4-dimensional the singular values.

D. Feature matching

We upscale the Harris point (x,y) at each scale-space image to the original image coordinate (X,Y) for feature matching. If Euclidean distances of feature vector at location i and j are less than the threshold ε, the two points form a candidate matching pair. This step gives us a set of candidate matching pairs. To remove false matches from the set we perform match validation using RANdom Sample Consensus (RANSAC) [21].

E. Tampered regions localization and correlation coefficient computation

Even if SGO may not strictly comply with linear geometric transformation, some matched points can still be found for SGO regions. Therefore, simply relying on the presence of matched points as evidence for true copy-move is not entirely reliable, as shown in Fig.2.

To address this problem, we compute the correlation coefficient between source region and target region after rectification. The source region is defined by the convex hull of the source feature points, and the target region is obtained through mapping the source region through the transformation matrix estimated in the previous step. The correlation coefficient is computed using all pixels in the source and target region.

Fig. 2. Exemplar point matching results for realistic image with SGO (left) and tampered image (right).

III. EXPERIMENT

A. Database

We evaluate the proposed SHFD algorithm, as well as the state-of-the-art SIFT-based method [1] and SORB method [16] over COVERAGE database [17]. COVERAGE database consists of multiple pairs of real and forgery image. The real images contain SGO, while the corresponding forgery images are intended to mimic the real counterpart through copy-move operation with 6 different tampering conditions which include pure translation (naïve), rotation, scaling, illumination changes, freeform distortion and combined conditions.

B. Parameters and Metrics

Our method has a few input parameters where are set as follows: $T = 0.02max(CR)$ (threshold for the corner response) and $k = 0.05$ (weight in corner response).

To evaluate the performance of CMFD on images with SGO, true positive rate (*TPR*) and false positive rate (*FPR*) are used as evaluation metrics. TPR and FPR are defined as follows:

$$TPR = \frac{\text{\# image detected as forgery being forgery}}{\text{\# forgery images}} \tag{8}$$

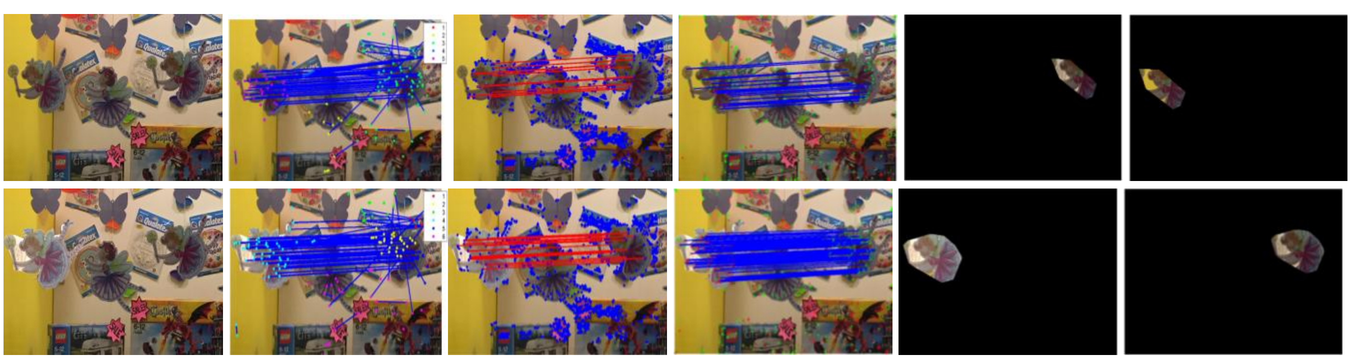
$$FPR = \frac{\text{\# image detected as forgery being origin}}{\text{\# origin images}} \tag{9}$$

C. Numerical Results

In this part, we compare empirical performance for the proposed SHFD algorithm versus other competitive CMFD methods, including SIFT-based method [1], and SORB-based method [16]. We present and analyze the numerical results along with different tampering factors and post-processing factors.

1) Performance on tampering factors discussion

To make traces of forgery less perceivable, various types of post-processing operations or tampering factors, such as illumination change, are applied in the forged image. We now analyze how the performance of CMFD methods including ours is affected by different tampering factors. We evaluate TPR and FPR values by applying SHFD algorithm to 100 images from COVERAGE. Fig. 3 illustrates example results for copy-move forgery detection for SIFT-based method [1], SORB-based method [16], and our method. In Fig.3, we can see that the methods based on SIFT and SORB are unable to differentiate SGO from true copy-move. Furthermore, our method produces relatively cleaner set of matched points, which leads a clean convex hull region for subsequent computation for correlation coefficient. As expected, the correlation coefficient for the real image with SGO is 0.78 which is lower than that for the fake image with copy-move which is 0.91.



(1) Input test image (2) SIFT-based [1] (3) SORB-based [16] (4) Our method (5) Source region (6) Target region

Fig. 3. Exemplar results for copy-move detection. (Top row) Result of real images with the presence of SGO. (Bottom row) Results for fake images produced through copy-move.

The left-side plot in Fig.4 illustrates ROC curves of our method subject to different tampering factors. Empirically, our method performs relatively well on detecting copy-move images with naive, rotation, scaling and free-form distortion tampering, as compared to the more challenging form of tampering which are illumination change and combined conditions. Finding ways to address those challenging tampering conditions will be our future work.

To compare our method to the state-of-the-art SIFT and Scaled ORB methods, we show the ROC curves for all methods evaluated COVERAGE database in the right-side plot of Fig.4. We can see that our method outperforming the competing methods across all FPR, and the margin of improvement is rather significant at the low FPR region.

2) Post-processing experiments

It is important to study the robustness of copy-move detection methods by assessing how their performance degrades under post-processing operations such as noise corruption, blurring, and JPEG compression. We simulate the post-processing effect on the image from COVERAGE database with operations including Gaussian blurring (window size = 3, and standard deviation = [0.5, 1, 2]), Gaussian noise corruption (mean = 0, and variance = [1, 3, 5]) and JPEG compression with quality factor of [80, 60, 40]. The corresponding ROC curves are plotted in Fig.5 for image blurring, noise corruption and JPEG compression respectively. We observe that our method is robust over all post-processing tests. However, the performance curve for SORB method is rather sensitive to image blurring and JPEG compression.

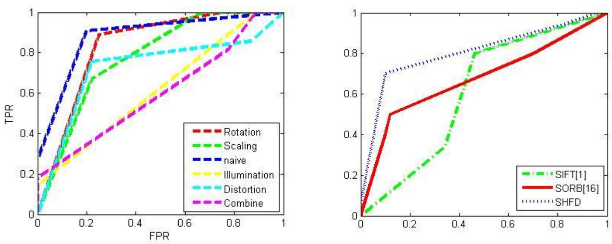


Fig. 4. ROC curves for our SHFD method evaluated under various tampering factors (left). ROC curves for various copy-move detection methods (right). Both are evaluated on COVERAGE database.

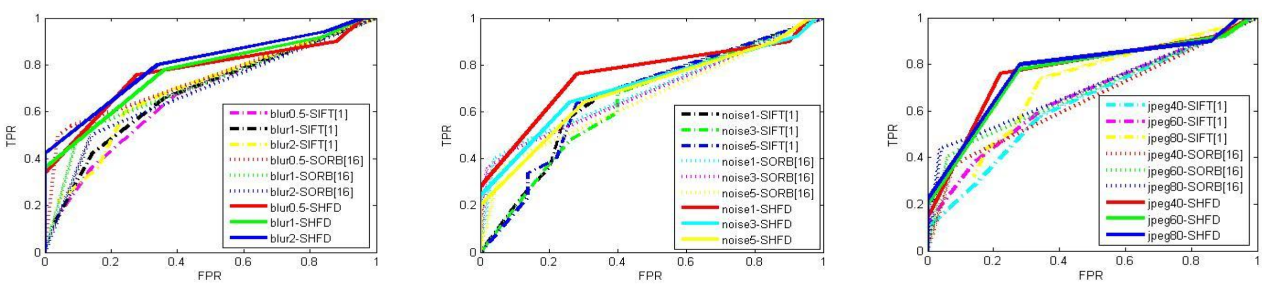


Fig. 5. From left to right: ROC curves varying with respect to blurring, noise and jpeg compression

IV. Conclusions

The main goal of this paper is to revisit copy-move forgery detection in the presence of SGO. SGO is not uncommon in real images. Ignoring SGO tends to inflate the performance of previous evaluation of copy-move detection methods. In this paper, we address this issue and present a set of more down-to-earth performance for copy-move detection. A key lesson for our work is that copy-move detection remains a work in progress, in contrast to the impression created by some previous works that copy-move detection is a solved problem. With better understanding on SGO, we propose a SHFD method that makes copy-move detection more prepared for the presence of SGO. Our method outperforms the current state-of-the-art copy-move detection methods by a significant margin. Our evaluation is comprehensive in the sense that it covers test under different tampering conditions and post-processing operations. Our SHFD is robust against post-processing operations including image blurring, JPEG compression, and addition of Gaussian noise. As future work, we like to make our method robust to challenging tampering conditions such as illumination changes, and combined tampering conditions.

References

[1] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, and G. Serra, "A sift-based forensic method for copy–move attack detection and transformation recovery," IEEE Transactions on Information Forensics and Security, 2011.

[2] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on surf," IEEE Multimedia Information Nethowrking and Security, 2010.

[3] A.J. Fridrich, B.D. Soukal, and A.J. Lukáˇ s, "Detection of copy move forgery in digital images," in Digital Forensic Research Workshop, 2003.

[4] X. Wang, X. Zhang, Z. Li, and S. Wang, "A dwt-dct based passive forensics method for copy-move attacks," IEEE Multimedia Information Nethowrking and Security, 2011.

[5] J. Hu, H. Zhang, Q. Gao, and H. Huang, "An improved lexicographical sort algorithm of copy-move forgery detection," in ICNDC, 2011.

[6] G. Muhammad, M. Hussain, and G. Bebis, "Passive copy move image forgery detection using undecimated dyadic wavelet transform," Digital Investigation, 2012.

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

[8] W. Li and N. Yu, "Rotation robust detection of copy-move forgery," in IEEE ICIP, 2010

[9] G. Liu, J. Wang, S. Lian, and Z. Wang, “A passive image authentication scheme for detecting region-duplication forgery with rotation,” Journal of Network and Computer Applications, 2011.

[10] S.J. Ryu, M.J. Lee, and H.K. Lee, “Detection of copy-rotate-move forgery using zernike moments,” in Information Hiding. Springer, 2010

[11] R. Davarzani, K. Yaghmaie, S. Mozaffari, and M. Tapak, “Copy-move forgery detection using multiresolution local binary patterns,” Forensic science international, 2013.

[12] H. Huang, W. Guo, and Y. Zhang, “Detection of copy-move forgery in digital images using sift algorithm,” IEEE PACIIA, 2008

[13] X. Pan and S. Lyu, “Detecting image region duplication using sift features,” in IEEE ICASSP, 2010

[14] B.L. Shivakumar and B.S. Santhosh, “Detection of region duplication forgery in digital images using surf,” IJCSI International Journal of Computer Science Issues, 2011.

[15] J.M. Guo, Y.F. Liu, and Z.J. Wu, “Duplication forgery detection using improved daisy descriptor,” Expert Systems with Applications, 2013.

[16] Y. Zhu, X. Shen, H. Chen, “Copy-move forgery detection based on scaled ORB,” Multimedia Tools and Applications, 2016.

[17] B. Wen, Y. Zhu, R. Subramanian, T.T. Ng, X. Shen, and S. Winkler, “Coverage - a novel database for copy-move forgery detection,” in IEEE ICIP, 2016, 161-165.

[18] A.P. Witkin, “Scale-space filtering: A new approach to multi-scale description,” in IEEE ICASSP, 1984.

[19] C. Harris and M. Stephens, “A combined corner and edge detector.,” in Alvey vision conference. 1988, vol. 15, p. 50, Manchester, UK.

[20] T. Ojala, M. Pietikainen, and T. Maenpaa, “Multires-olution gray-scale and rotation invariant texture classification with local binary patterns,” IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002.

[21] M.A. Fischler and R.C. Bolles, “Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography,” Communications of the ACM, 1981.

AUTHORS’ BACKGROUND

Your Name	Title*	Research Field	Personal website
Ye Zhu	Phd candidate	Image forgery detection	

*This form helps us to understand your paper better, the form itself will not be published.

*Title can be chosen from: master student, Phd candidate, assistant professor, lecture, senior lecture, associate professor, full professor