Over-Segmentation Based Image Forgery Detection

Xiu-Li Bi, Chi-Man Pun, and Xiao-Chen Yuan

Department of Computer and Information Science
University of Macau, Macau SAR, China
Email: cmpun@umac.mo

***Abstract*—This paper proposes an adaptive over-segmentation meth-od for image copy-move forgery detection. Firstly, the Adaptive Over-Segmentation algorithm is proposed to adaptively segment the host image into non-overlapping and irregular blocks. Then the feature points are extracted and matched with each other to locate the labeled feature points which can approximately indicate the suspected forgery regions. Finally the labeled feature points are processed and the morphological operation is applied to generate the detected forgery regions. Experimental results indicate the good performance of the proposed copy-move forgery detection.**

Keywords—Copy-Move Forgery Detection, Adaptive Over-Segmentation, Non-Overlapping and Irregular Blocks

I. INTRODUCTION

Nowadays, digital image forgery has been becoming increasingly easy to perform. Of the existing kinds of image forgery, a common manipulation with digital image is copy-move forgery, which is to paste one or several copied region(s) of an image into another part(s) of the same image. In the past years, lots of forgery detection methods have been proposed for copy-move forgery detection.

Fridrich et al. [1]proposed the forgery detection method where the input image was divided into over-lapped rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of blocks were matched to find the tampered regions.Luo et al. [2]used the RGB color components and direction information as block feature. Li et al. [3]used Discrete Wavelet Transform (DWT) and Singular Values Decomposition (SVD) to extract image features. Mahdian and Saic[4]calculated the 24 Blur-invariant moments as feature.Bayram et al. [5]used the Fourier-Mellin Transform (FMT) to obtain feature. In [6], Wang et al. used the mean intensities of circles with different radii around the block center to represent block feature. Ryu et al. [7]used Zernike moments as block feature. Bravo-Solorio and Nandi [8] used the information entropy as block feature. In [9, 10], the Scale Invariant Feature Transform (SIFT) [20] was applied to the host images to extract feature points, which are then matched to each other.

The above-mentioned existing schemes can be divided in to two categories: the block-based forgery detection methods which are to divide the input images into overlapping and regular image blocks, and then obtain the tampered regions by matching blocks of image pixels or transform coefficients; and the keypoint-based forgery detection methods, which extract the image keypointsand matchthem to identify the duplicated regions.Although these schemes are effective in forgery detection, they have three main drawbacks: 1) the host image is divided into over-lapped blocks, which will cause the computation complexity expensive; 2) the methods cannot deal with significant geometrical transformation of the forgery regions; 3) the host image is divided into regular blocks, which will cause low*recall* rate. Although the existing keypoint based forgery detection methods can somewhat reduce the computation complexity and can be robust against some attacks, the *recall* results were still poor.

To overcome the shortcomings of the existing methods, we propose a novel copy-move forgery detection scheme using adaptive over-segmentation in this paper. The Adaptive Over-Segmentation algorithm is proposed to adaptivelysegment the host image into non-overlapping and irregular blocks. Then the feature points are extracted from each block and matched with each other to locate the labeled feature points which can approximately indicate the suspected forgery regions. Finally the labeled feature points are processed and the morphological operation is applied to generate the detected forgery regions.In the following sections, Section2 shows the framework of the proposed copy-move forgery detection scheme and explains each step in detail. In Section 3, a series of experiments are conducted to demonstrate the effectiveness of our proposed scheme. And finally the conclusions are drawn in Section 4.

II. IMAGE FORGERY DETECTION USING ADAPTIVE OVER-SEGMENTATION

This section describes the proposed image forgery detection using adaptive over-segmentation in details. Fig. 1 shows the framework of the proposed scheme for image forgery detection. Firstly, the adaptive over-segmentation method is proposed to segment the host image into non-overlapping and irregular blocks. ThenSIFTis applied into each block to extract feature points as block features which are matched with each other to locate thepoints which can approximately indicate the suspected forgery regions. Finally the forgery regions are

detected according to the matched feature points.In order to divide the host image into non-overlapping regions of irregular shape, we employ the SLIC algorithm [11]to segment the host image into meaningful superpixels. As a non-overlapping segmentation method, SLIC can decrease the computational expenses comparing with the overlapping blocking; furthermore, in most of the cases, the irregular and meaningful regions can represent the forgery region better than the regular blocks. However, the initial size of the superpixels in SLIC is hard to decide. When the initial size is too small, it will cause large computation expenses; otherwise, when it is too large, it will cause the forgery detection results not accurate enough. At present, there is no such a good method to determine the initial size in superpixel segmentation algorithms. Therefore, in this paper, we proposed the Adaptive Over-Segmentation method which can determine the initial size adaptively based on the texture of the host image and thus can divide the host image into irregular and non-overlapping blocks. In the proposed Adaptive Over-Segmentation method,firstly, the Discrete Wavelet Transform (DWT)is employed into the host image to generate the low frequency and high frequency sub-bands. Then the initial size of the superpixels is calculated with the adaptive block size computation. Finally, with the calculated initial size, the SLIC segmentation algorithmis employed to segment the host image into irregular and non-overlapping image blocks.

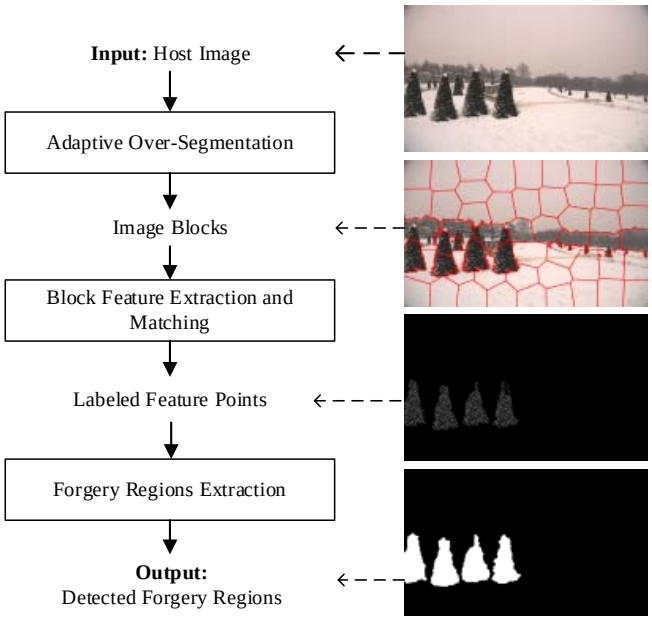

Fig. 1Framework of the proposed copy-move forgery detection scheme

III. EXPERIMENTS AND DISCUSSIONS

In this section, a series of experiments are conducted to evaluate the effectiveness and robustness of the proposed copy-move forgery detection scheme. In the following experiments, the image dataset in [12] is used to test the proposed scheme. The dataset is formed based on 48 high-resolution uncompressed PNG true color images.In the dataset, the copied regions are of categories of living, nature, man-made and even mixed, and they range from overly smooth to highly texture; the copy-move forgeries are created by copying, scaling and rotating semantically meaningful image regions.Fig. 2 shows the copy-move forgery detection results of the proposed scheme. In Fig. 2, the first column showsthe forged images selected from the dataset; the second column shows the corresponding ground truth forged regions; and the third columnshows the detected forgery regions. It can be easily seen that the proposed scheme can detect the forged regions very well.

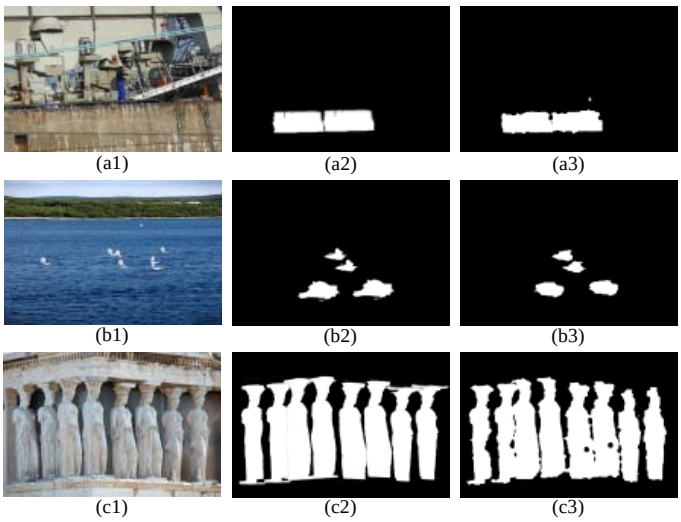

Fig. 2The copy-move forgery detection results. The first column: host images from the dataset; the second column: the corresponding ground truth forgery regions; the third column: the detected forgery regions.

In order to evaluate the performance of the proposed scheme, the *precision* and *recall*are calculated using (1).We also give the *F*score, which is defined in (2), as a measure which combines the *precision* and *recall* in a single value.

$$precision = \frac{\left|R \cap R^{'}\right|}{\left|R\right|}, \qquad recall = \frac{\left|R \cap R^{'}\right|}{\left|R^{'}\right|} \tag{1}$$

Where R means the set of forgery regions detected by the proposed scheme for the dataset; and $R^{'}$ means the set of all forgery regions for the dataset.

$$F = 2 \times \frac{precision \times recall}{precison + recall} \tag{2}$$

We evaluate the proposed scheme underdifferent conditions. Table 1 shows the results at both image level and pixel level, under plain copy-move, which means the one to one copy-move. Fig. 3 shows the F scores when the copied regions are attacked by various attacks: (a) down-Sampling, the host

images are scaled down from 90% to 10% in step of 20%;(b) scaling,the copied regions are scaled with the scale factor varies from 91% to 109%, in step of 2%;(c) rotation, the copied regions are rotated with the rotation angle varies from 2º to 10º, in step of 2º; and (d) JPEG compression,the forgery images are JPEG compressed with the qualify factor varies from 100 to 20, in step of -10. It can be easily seen that in most of the cases, the proposed scheme performs much better than the existing state-of-the-art forgery detection methods.

Table 1 Copy-move forgery detection results under plain copy-move

	Methods	*Precision* (%)	*Recall* (%)	*F* (%)
Image Level	Wang [6, 13]	92.31	100	96.00
	SIFT[9, 14]	88.37	79.17	83.52
	Proposed	**95**	**100**	**97.6**
Pixel Level	Wang [6, 13]	98.69	85.44	90.92
	SIFT[9, 14]	60.80	71.48	63.10
	Proposed	**97.2**	**83.3**	**89.7**

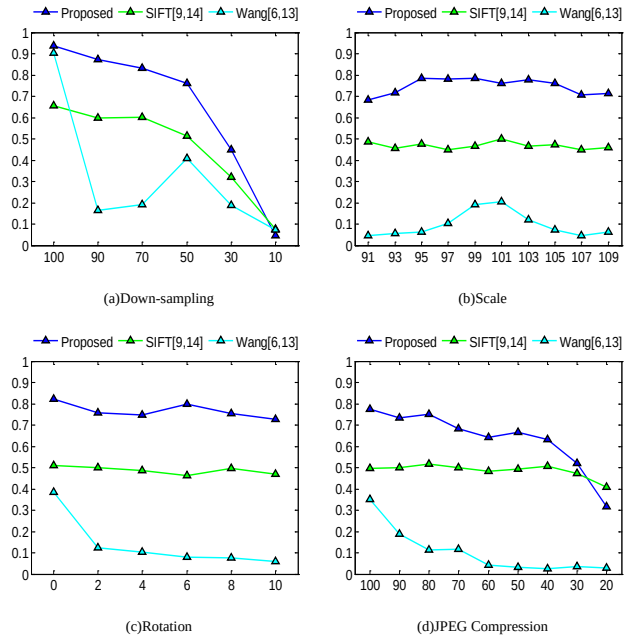

Fig. 3*F* scores under various attacks at pixel level (a) Down-sampling; (b) Scale; (c) Rotation; and (d) JPEG Compression.

IV. CONCLUSIONS

In this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation. The proposed Adaptive Over-Segmentation algorithm can adaptively segment the host image into non-overlapping and irregular blocks. In each block, the feature points are extracted and matched to indicate the suspected forgery regions. The Forgery Region Extraction algorithm is proposed to process the suspected feature points, thus generating the detected forgery regions.Experimental results show that the proposed scheme can achieve good performance under various challenging conditions such geometric transforms, and JPEG compression. Future work may focus on applying the proposed adaptive over-segmentation method into other kind of forgery such as splicing or other kind of media such as video and audio. Another future direction is to embed the forgery detection method with some watermarking algorithms [15-20] for possible improvement in multimedia security.

ACKNOWLEDGMENT

This research was supported in part by the Research Committee of the University of Macau (MYRG2015-00011-FST, MYRG2015-00012-FST) and the Science and Technology Development Fund of Macau SAR (008/2013/A1, 093-2014-A2).

REFERENCES

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

[2] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, 2006, pp. 746-749.

[3] G. Li, Q. Wu, D. Tu, and S. Sun, "A sorted neighborhood approach for detecting duplicated regions in image forgeries based on DWT and SVD," in *Multimedia and Expo, 2007 IEEE International Conference on*, 2007, pp. 1750-1753.

[4] B. Mahdian and S. Saic, "Detection of copy–move forgery using a method based on blur moment invariants," *Forensic science international*, vol. 171, pp. 180-189, 2007.

[5] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, 2009, pp. 1053-1056.

[6] J. Wang, G. Liu, H. Li, Y. Dai, and Z. Wang, "Detection of image region duplication forgery using model with circle block," in *Multimedia Information Networking and Security, 2009. MINES'09. International Conference on*, 2009, pp. 25-29.

[7] S. J. Ryu, M. Kirchner, M. J. Lee, and H. K. Lee, "Rotation Invariant Localization of Duplicated Image Regions Based on Zernike Moments," *IEEE Transactions on Information Forensics and Security*, vol. 8, pp. 1355-1370, Aug 2013.

[8] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affected by reflection, rotation and scaling," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*, 2011, pp. 1880-1883.

[9] X. Y. Pan and S. Lyu, "Region Duplication Detection Using Image Feature Matching," *Ieee Transactions on Information Forensics and Security*, vol. 5, pp. 857-867, Dec 2010.

[10] P. Kakar and N. Sudha, "Exposing Postprocessed Copy–Paste Forgeries Through Transform-Invariant Features,"

Information Forensics and Security, IEEE Transactions on, vol. 7, pp. 1018-1028, 2012.

[11] R. Achanta, A. Shaji, K. Smith, A. Lucchi, P. Fua, and S. Susstrunk, "SLIC superpixels compared to state-of-the-art superpixel methods," *IEEE Trans Pattern Anal Mach Intell*, vol. 34, pp. 2274-82, Nov 2012.

[12] V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 1841-1854, Dec 2012.

[13] J. Wang, G. Liu, Z. Zhang, Y. Dai, and Z. Wang, "Fast and robust forensics for image region-duplication forgery," *Acta Automatica Sinica*, vol. 35, pp. 1488-1495, 2009.

[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," *Information Forensics and Security, IEEE Transactions on*, vol. 6, pp. 1099-1110, 2011.

[15] C.-M. Pun and K.-C. Choi, "Generalized integer transform based reversible watermarking algorithm using efficient location map encoding and adaptive thresholding," Computing, 96(10), pp.951-973, 2014.

[16] B. Liu, C.-M. Pun and X.-C. Yuan, "Digital Image Forgery Detection Using JPEG Features and Local Noise Discrepancies," The Scientific World Journal, Volume 2014 (2014), Article ID 230425, 12 pages, 2014.

[17] C.-M. Pun and X.-C. Yuan, "Robust Segments Detector for De-Synchronization Resilient Audio Watermarking," IEEE Transactions on Audio, Speech, and Language Processing, 21(11), pp. 2412 – 2424, 2013.

[18] X.-C. Yuan, C.-M. Pun and C. L. Philip Chen, "Geometric invariant watermarking by local Zernike moments of binary image patches," Signal Processing, 93(7), pp. 2087–2095, 2013.

[19] X.-C. Yuan and C.-M. Pun," Geometrically Invariant Image Watermarking Based on Feature Extraction and Zernike Transform," International Journal of Security and Its Applications, 6(2), pp.217-222, 2012.

[20] X.-C. Yuan and C.-M. Pun , "A Geometric Invariant Digital Image Watermarking Based on Robust Feature Detector and Local Zernike Moments," Proceedings of the 9th International Conference Computer Graphics, Imaging and Visualization, Hsinchu, 2012.