International Journal For Technological Research In Engineering
Volume 4, Issue 4, December-2016 *ISSN (Online): 2347 - 4718*

IMAGE FORGERY DETECTION USING ADAPTIVE OVER SEGMENTATION AND FEATURE POINT MATCHING

Regin V. Roy
PG Student, Communication Engineering, Department. of ECE
Mount Zion College of Engineering Kadammanitta, Kerala, India

Abstract: ***A novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching is proposed in this paper. The proposed scheme integrates both block-based and keypoint-based forgery detection methods. First, the proposed Adaptive Over-Segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. Then, the feature points are extracted from each block as block features, and the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. To detect the forgery regions more accurately, we propose the Forgery Region Extraction algorithm, which replaces the feature points with small superpixels as feature blocks and then merges the neighboring blocks that have similar local color features into the feature blocks to generate the merged regions; finally, it applies the morphological operation to the merged regions to generate the detected forgery regions. The experimental results indicate that the proposed copy-move forgery detection scheme can achieve much better detection results even under various challenging conditions compared with the existing state-of-the-art copymove forgery detection methods.***

Index Terms: Copy-Move Forgery Detection, Adaptive Over-Segmentation, Local Color Feature, Forgery Region Extraction

I. INTRODUCTION

WITH the development of computer technology and image processing software, digital image forgery has been increasingly easy to perform. However, digital images are a popular source of information, and the reliability of digital images is thus becoming an important issue. In recent years, more and more researchers have begun to focus on the problem of digital image tampering. Of the existing types of image tampering, a common manipulation of a digital image is copy-move forgery which is to paste one or several copied regions of an image into other parts of the same image. During the copy and move operations, some image processing methods such as rotation, scaling, blurring, compression, and noise addition are occasionally applied to make convincing forgeries. Because the copy and move parts are copied from the same image, the noise component, color character and other important properties are compatible with the remainder of the image; some of the forgery detection methods that are based on the related image properties are not applicable in this case. In previous years, many forgery detection methods have been proposed for copy-move forgery detection. According to the existing methods, the copy-move forgery the detection methods can be categorized into two main categories: block-based algorithms and feature keypoint-based algorithms. As an alternative to the block-based methods, keypoint-based forgery detection methods were proposed, where image keypoints are extracted and matched over the whole image to resist some image transformations while identifying duplicated regions. In the Scale-Invariant Feature Transform (SIFT) was applied to the host images to extract feature points, which were then matched to one another. When the value of the shift vector exceeded the threshold, the sets of corresponding SIFT feature points were defined as the forgery region. In the Speeded Up Robust Features (SURF) were applied to extract features instead of SIFT. However, although these methods can locate the matched keypoints, most of them cannot locate the forgery regions very well; therefore, they cannot achieve satisfactory detection results and, at the same time, a sustained high recall rate.

Most of the existing block-based forgery detection algorithms use a similar framework, and the only difference is that they apply different feature extraction methods to extract the block features. Although these algorithms are effective in forgery detection, they have three main drawbacks: 1) the host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases; 2) the methods cannot address significant geometrical transformations of the forgery regions; and 3) their recall rate is low because their blocking method is a regular shape. Although the existing keypoint-based forgery detection methods can avoid the first two problems, they can reduce the computational complexity and can successfully detect the forgery, even when some attacks exist in the host images; the recall results of the existing keypoint-based forgery methods were very poor. To address the above-mentioned problems, in this paper, we propose a novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching. The proposed scheme integrates both the traditional block-based forgery detection methods and keypoint-based forgery detection methods. Similar to block-based forgery detection methods, we propose an image-blocking method called the Adaptive Over-Segmentation algorithm to divide the host image into non-overlapping and irregular blocks adaptively. Then,similar to the keypoint-based forgery detection methods, the feature points are extracted from each image block as block features instead of being extracted from the whole host image as in the traditional keypoint-base methods. Subsequently, the block features are matched with one another to locate the

labeled feature points, which can approximately indicate the suspected forgery regions. To detect more accurate forgery regions, we proposed the Forgery Region Extraction algorithm, which replaces the feature points with small super pixels as feature blocks and, then, merges the neighboring blocks with similar local color features into feature blocks, to generate the merged regions; finally, it applies a morphological operation in to the merged regions to generate the detected forgery regions.

II. LITERATURE SURVEY

Tampering images has become extremely easy due to the easy accessibility of advanced image editing software and powerful computing hardware. Various types of forgeries can be created and in recent years, image forgery detection usingpassive techniques has become a hot area of research .One of the most common types of image forgeries is the copy–paste (or copy–move or cloning) forgery, where a region from one part of an image is copied and pasted onto another part, thereby concealing the image content in the latter region.Such concealment can be used to hide an undesired object or increase the number of objects apparently present in the image. Although a simple translation may be sufficient in many cases, additional operations are often performed in order to better hide the tampering. These include scaling, rotation, lossy compression, noise addition, blurring, among others. Hence, in order to be able to reliably detect such forgeries, a few techniques have been recently proposed which try to be robust to some of these transformations. As copy–paste forgeries become more convincing, it is necessary to devise techniques which can still detect transformed regions and expose such tampering. Our proposed technique is an attempt to do this.The key contributions of our technique are listed as follows:1) adapting the MPEG-7 image signature tools for use in thenew application of image forgery detection;2) developing an alternative feature matching approach to the one used by the MPEG-7 standard for image signature tools in order to deal with a different problem context; 3) employing matching feature constraints to improve cloned region detection via clustering; 4) evaluating our novel technique on a variety of images subjected to a significant number of postprocessing operations. Copy-move forgeries are a common type of forgery where parts of an image are replaced with other parts from the same image. The copied and pasted regions may be subjected to various image transformations in order to conceal the tampering better. Conventional techniques of detecting copy–paste forgeries usually suffer from the problems of false positives and susceptibility to many image processing operations.We have proposed a technique based on the MPEG-7 image signature tools, which have been developed for robust content-based image retrieval, in order to detect copy–move forgeries. We have modified the tools in many ways to deal with copied regions in a single image. We have used a feature matching process that utilizes the inherentconstraints in matched feature pairs to improve the detection of cloned regions. We have analyzed the performance of this technique on actual and synthesized forgeries. The results obtained by using these features display high true positive rates and extremely low false positives and are better than the state of the art, in general. As these descriptors are invariant to a lot of common image processing operations (scaling, rotation,flipping, noise addition, JPEG compression, blurring), their use in dealing with realistic copy–paste forgeries is justified.

III. PROPOSED SYSTEM

We first propose the Adaptive Over-Segmentation algorithm, which is similar to the traditional block-based forgery detection methods and can divide the host image in to blocks. In previous years, a large amount of block-based forgery detection algorithms have been proposed . Of the existing block-based forgery detection schemes, the host image was usually divided into overlapping regular blocks, with the block size being defined and fixed beforehand.Then, the forgery regions were detected by matching those blocks. In this way, the detected regions are always composed of regular blocks, which cannot represent the accurate forgery region well; as a consequence, the recall rate of the block-based methods is always very low. Moreover, when the size of the host images increases, the matching computation of the overlapping blocks will be much more expensive. To address these problems, we proposed the Adaptive Over-segmentation method, which can segment the host image in to non-overlapping regions of irregular shape as image blocks afterward, the forgery regions can be detected by matching those nonoverlapping and irregular regions.We use SLICO to segment the image. SLICO does away with this problem completely. The user no longer has to set the compactness parameter or try different values of it. SLICO adaptively chooses the compactness parameter for each superpixel differently. This generates regular shaped superpixels in both textured and non textured regions alike. The improvement comes with hardly any compromise on the computational efficiency - SLICO continues to be as fast as SLIC. In this section, we extract block features from the image blocks (IB). The traditional block-based forgery detection methods extracted features of the same length as the block features or directly used the pixels of the image block as the block features.SURF were often used as feature point extraction method.

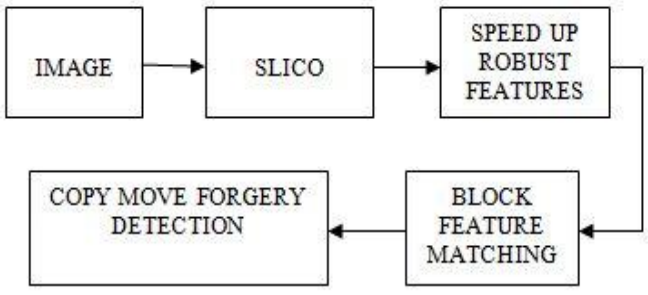

Fig.1. Block Diagram of Proposed System

First we take the the input image to identify the forgery. We use SLICO to segment the image. SLICO does away with this problem completely. The user no longer has to set the compactness parameter or try different values of it. SLICO adaptively chooses the compactness parameter for each superpixel differently. This generates regular shaped

superpixels in both textured and non textured regions alike. The improvement comes with hardly any compromise on the computational efficiency SLICO continues to be as fast as SLIC. The SURF approach describes a keypoint detector and descriptor. Keypoints are found by using a so called Fast-Hessian Detector that bases on an approximation of the Hessian matrix for a given image point. The responses to Haar wavelets are used for orientation assignment, before the keypoint descriptor is formed from the wavelet responses in a certain surrounding of the keypoint. After we have obtained the block features (BF), we must locate the matched blocks through the block features. In most of the existing block-based methods, the block matching process outputs a specific block pair only if there are many other matching pairs in the same mutual position, assuming that they have the same shift vector. When the shift vector exceeds a user-specified threshold, the matched blocks that contributed to that specific shift vector are identified as regions that might have been copied and moved. In our algorithm, because the block feature is composed of a set of feature points, we proposed a different method to locate the matched blocks. First, the number of matched feature points is calculated, and the correlation coefficient map is generated; then, the corresponding block matching threshold is calculated adaptively; with the result, the matched block pairs are located; and finally, the matched feature points in the matched block pairs are extracted and labeled to locate the position of the suspected forgery region.

Although we have extracted the labeled feature points (LFP),which are only the locations of the forgery regions, we must still locate the forgery regions. Considering that the superpixels can segment the host image very well, we proposed a method by replacing the LFP with small superpixels to obtain the suspected regions (SR), which are combinations of labeled small superpixels. Furthermore, to improve the precision and recall results, we measure the local color feature of the superpixels that are neighbors to the suspected regions (SR); if their color feature is similar to that of the suspected regions, then we merge the neighbor superpixels into the corresponding suspected regions, which generates the merged regions (MR). Finally, a close morphological operation is applied to the merged regions to generate the detected copy-move forgery regions.

IV. CONCLUSION

Digital forgery images created with copy-move operations are challenging to detect. In this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature-point matching. The Adaptive OverSegmentation algorithm is proposed to segment the host image into non-overlapping and irregular blocks adaptively according to the given host images; using this approach, for each image, we can determine an appropriate block initial size to enhance the accuracy of the forgery detection results and, at the same time, reduce the computational expenses. Then, in each block, the feature points are extracted as block features, and the Block Feature Matching algorithm is proposed, with which the block features are matched with one another to locate the labeled feature points; this procedure can approximately indicate the suspected forgery regions. Subsequently, to detect the more accurate forgery regions, we propose the Forgery Region Extraction algorithm, in which the labeled feature points are replaced with small superpixels as feature blocks, and the neighboring feature blocks with local color features that are similar to the feature blocks are merged to generate the merged regions. Next, the morphological operation is applied to the merged regions to generate the detected forgery regions.

REFERENCES

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

[2]. 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.

[3]. 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

[4]. 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.

[5]. B. Shivakumar and L. D. S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," IJCSI International Journal of Computer Science Issues, vol. 8, 2011.

[6]. 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.

[7]. 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.

[8]. X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF," in Multimedia Information Networking and Security (MINES), 2010 International Conference on, 2010, pp. 889-892.

[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]. S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using Zernike moments," in Information Hiding, 2010, pp. 51-65.

[11]. 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.

[12]. 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.

[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]. H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection," WSEAS Transactions on Signal Processing, vol. 5, pp. 188-197, 2009.

[15]. X. Kang and S. Wei, "Identifying tampered regions using singular value decomposition in digital image forensics," in Computer Science and Software Engineering, 2008 International Conference on, 2008, pp. 926-930.

[16]. H. Huang, W. Guo, and Y. Zhang, "Detection of copy-move forgery in digital images using SIFT algorithm," in Computational Intelligence and Industrial Application, 2008. PACIIA'08. Pacific-Asia Workshop on, 2008, pp. 272-276

[17]. 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.

[18]. 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

[19]. H. Bay, T. Tuytelaars, and L. Van Gool, "Surf: Speeded up robust features," in Computer Vision–ECCV 2006, ed: Springer, 2006, pp. 404-417.

[20]. 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.

