Improving Digital Image Forgery Detection Using MIFT Features and Adaptive Over Segmentation

Dhania V S[1], Harish Binu K P[2]

[1]M.Tech Student, Dept. of Computer Science & Engineering, MEA Engineering College, Perinthalmanna

[2] Assistant professor, Dept. of Computer Science & Engineering, MEA Engineering College, Perinthalmanna

---

Abstract - *A novel copy–move forgery detection method using adaptive over segmentation and feature point matching is proposed in this paper. The proposed method integrates both block-based and key point-based forgery detection methods. First, the adaptive over segmentation algorithm divides the host image into non- overlapping and irregular blocks adaptively. Then the features points are extracted using SIFT and matched with each other to locate the labeled feature points which can almost show the suspected forgery regions. To find the forgery regions more precisely, we propose the forgery region extraction algorithm, which substitutes the feature points with small super pixels as feature blocks and then merges the adjacent blocks that have similar local color features into the feature blocks to generate the merged regions. Finally, this method applies the morphological operation into the merged regions to generate the detected forgery regions. In this paper, our importance is on improving the detection and localization of duplicated regions using more powerful keypoint-based features. In this context, we have also adopted a more powerful set of keypoint-based features, called MIFT, it shares the properties of SIFT features but also are invariant to mirror reflection transformations. Experimental results show the good performance of the proposed copy-move forgery detection.*

***Key Words*:** Copy-move forgery detection, adaptive Over-segmentation, SIFT, MIFT, Matching

1. INTRODUCTION

Nowadays, digital image forgery has been becoming gradually easy to perform. Of the existing kinds of image forgery, one of the common manipulations 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, many forgery detection methods have been proposed for copy-move forgery detection.

Fridrich et al. [1] suggested the forgery detection method where the input image was segmented into over-lapped rectangular blocks, and from which the quantized Discrete Cosine Transform (DCT) coefficients of blocks were matched to find the tampered regions. Luo et al. [2] was used the RGB color components and direction information as block feature. Li et al.[3] was 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. Wang et al.[6] suggested 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 the Scale Invariant Feature Transform (SIFT)[9] was used to the input images to extract feature points, which are then matched to each other.

The above-stated existing methods can be divided in to two categories: the block-based forgery detection methods which are to segment the input images into overlapping and regular image blocks, and then obtain the forged regions by matching blocks of image pixels or their transform coefficients; and the keypoint-based forgery detection methods, which extract the image feature keypoints and match them to find the duplicated regions. Although these methods are effective in forgery detection, they have three main drawbacks: 1) the input image is divided into over-lapped regions, which will cause the computation complexity expensive; 2) the methods cannot deal with significant geometrical transformation of the forgery areas; 3) the host image is divided into regular blocks, which will cause low recall rate. And the existing keypoint based forgery detection methods can somewhat reduce the computation complexity and can be strong against some attacks, the recall results were still poor. To address the shortcomings of the existing methods, we propose a novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching in this paper. The Adaptive Over-Segmentation algorithm is proposed to adaptively divide the host image into non-overlapping and irregular blocks. Then the feature points are extracted from each block and matched with each other to find the labeled feature points which can approximately indicate the suspected forgery regions. And finally the labeled feature points are processed and the morphological operation is applied to generate the detected forgery regions.

International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 07 | July-2016 www.irjet.net p-ISSN: 2395-0072

2. PROPOSED METHOD

This section describes the proposed image forgery detection using adaptive over-segmentation [10] in details. Fig. 1 shows the framework of the proposed method for image forgery detection. Firstly, the adaptive over-segmentation method is proposed to divide the input image into non-overlapping and irregular regions. Then SIFT [9,10] is applied into each block to extract feature points as block features which are matched with each other to locate the points which can approximately specify the suspected forgery regions. Finally the forgery regions are detected according to the matched feature points.

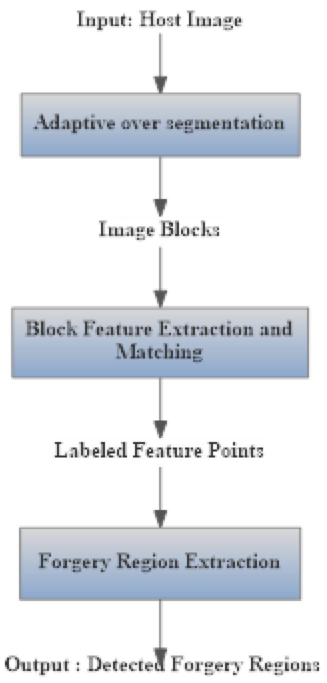

Fig -1: Framework of the proposed copy-move forgery detection scheme

2.1 Adaptive Over Segmentation

In order to segment the input image into non-overlapping regions of irregular shape, we used the SLIC algorithm to divide the host image into meaningful superpixels. As a non-overlapping segmentation method, SLIC [10] can reduce the computational expenditures comparing with the overlapping blocking; furthermore, in most of the cases, the irregular and meaningful regions can signify the forgery region better than the regular blocks. However, the initial size of the superpixels in SLIC is hard to determine. 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 define the initial size adaptively based on the texture of the host image and thus can segment the input 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 algorithm is employed to divide the input image into irregular and non-overlapping image blocks.

2.2 Block Feature Extraction-SIFT

After the host image is segmented into image blocks, block features are extracted 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. However, these features reflect mainly the content of the image blocks, leaving out the location information. Also, these features are not resistant to various image transformations. Therefore, in this project, the feature points are extracted from each image block as block features and the feature points should be robust to various distortions, such as image scaling, rotation, and JPEG compression. The feature points generated using these methods are robust against common image processing operations such as rotation, scale, blurring, and compression. Experiments have shown that the results obtained using SIFT are more constant and have better performance compared to other feature extraction methods. Hence, in this proposed scheme SIFT is used for feature point extraction. Therefore, each block feature contains irregular block information and the extracted SIFT feature points.

2.3 Block Feature Extraction-MIFT

In this study, we improve copy-move forgery detection using keypoint-based features by focusing on the issue of accurate detection and localization of duplicated regions. Exactly, we have made several contributions in this work. The SIFT algorithm is a powerful feature extraction technique, which extracts features invariant to scale, rotation, and brightness. However, SIFT descriptors are not invariant to mirror reflection. To account for this issue, previous approaches proposed extracting SIFT descriptors from horizontally and vertically reflected versions of the original image. In this paper, we have adopted MIFT [11] descriptors that are invariant to mirror reflection transformations. Since we pursuit for duplicated regions in a single image, we segment the image into smaller regions and compare the descriptors among them. The search is done outside a small window centered at the detected keypoint to avoid finding nearest neighbours of a keypoint from the same region. Once a matching candidate has been found, it is accepted as a unique matched point if the ratio of the distances from the first and second nearest neighbours is smaller than the threshold. This threshold can differ from zero to one; a threshold closer to zero yields more correct but less matches. Here, a low threshold is used since it decreases false matches.

3. EXPERIMENTAL RESULTS

In this section, a sequence of experiments is conducted to evaluate the effectiveness and robustness of the proposed copy-move forgery detection scheme. We have evaluated the performance of the proposed methodology by performing a comprehensive set of experiments with a large database of real images. Comparisons with competitive approaches show that the proposed method can find duplicated regions in copy-move image forgery more accurately, especially when the size of the duplicated regions is small.

Fig -2: (a) Original Image (b) Forged Image

Fig -3: (a) Host Image (b) Segmented Image (c) Feature Extraction using SIFT (d)Feature Matching (e)Forgery Region Extraction

Experimental results show that the proposed scheme can achieve much better detection results for copy-move forgery images under various challenging conditions, such as geometric transforms, JPEG compression, and down-sampling. But this method, however, cannot handle reflection. Mirror reflection invariant feature generalizes SIFT by producing mirror reflection invariant descriptors. We have adopted MIFT descriptors in this work to find duplicated regions with or without mirror reflection. Figure 4 shows an example using MIFT in the case of mirror reflection.

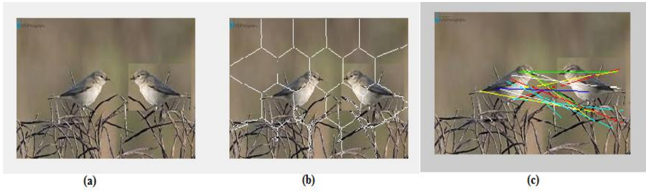

Fig -4: (a) Host Image (b) Segmented Image (c) Feature Extraction using MIFT

In the above experiments, the two characteristics precision and recall [10] are used to evaluate the performance of the proposed forgery detection scheme. Precision is the probability that the detected regions are relevant, and it is defined as the ratio of the number of correctly detected forged pixels to the number of totally detected forged pixels, as stated in [10]. Recall is the probability that the relevant regions are detected, and it is defined as the ratio of the number of correctly detected forged pixels to the number of forged pixels in the ground-truth forged image. Fig 5 shows the precision and recall rate of the method using MIFT.

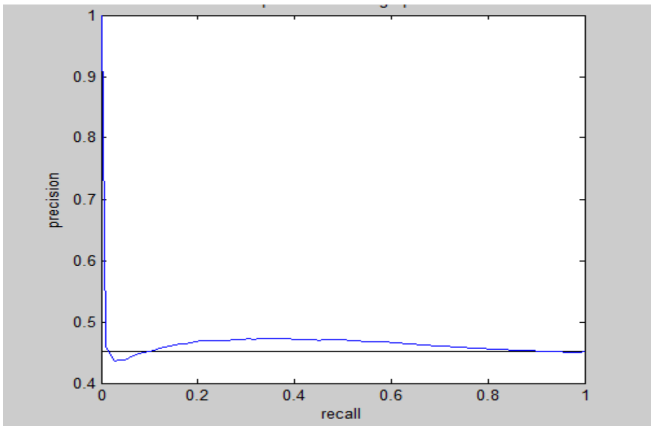

Fig -5: Precision and Recall Rate of Feature Extraction Using MIFT

3. CONCLUSIONS

In this paper, we have proposed a novel copy-move forgery detection scheme using adaptive over-segmentation and feature extraction. The proposed Adaptive Over-Segmentation algorithm can adaptively divide the input image into non-overlapping and irregular blocks. In each block, the features points are extracted using SIFT and matched to indicate the suspected forgery regions. The proposed methodology employs a new set of keypoint-based features, called MIFT, for finding similar regions in an image. We have performed comprehensive experiments using a large dataset of real images to evaluate the proposed approach. In particular, we have investigated the effect of different transformations in creating the image forgery on detection accuracy. It should be mentioned that like with similar methods employing keypoint-based features for matching, the proposed approach will not work well if the duplicated region corresponds to a flat surface where no interest points can be detected.

REFERENCES

[1] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy–move forgery in digital images," in Proc. Digit. Forensic Res. Workshop,Cleveland,OH,Aug 2003

[2] W. Luo, J. Huang, and G. Qiu, "Robust detection of region-duplication forgery in digital image," in Proc. 18th Int. Conf. Pattern Recognit. (ICPR), Aug. 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 Proc. IEEE Int. Conf. Multimedia Expo, Jul. 2007, pp. 1750–1753.

[4] B. Mahdian and S. Saic , "Detection of copy–move forgery using a method based on blur moment invariants," Forensic Sci. Int., vol. 171, nos. 2–3, pp. 180–189, 2007.

[5] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy–move forgery," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), Apr. 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 Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES), Nov. 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 Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1355–1370,Aug. 2013.

[8] S. Bravo-Solorio and A. K. Nandi, "Exposing duplicated regions affecte by reflection, rotation and scaling," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2011, pp. 1880–1883.

[9] 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. Inf. Forensics Security, vol. 6,no. 3, pp. 1099–1110, Sep. 2011.

[10] Chi-Man Pun, Xiao-Chen Yuan,, M. J. Lee, and Xiu-Li Bi, "Image Forgery Detection Using Adaptive Oversegmentation and Feature Point Matching," IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1705–1716,Aug. 2015.

[11] Maryam Jaberi, George Babis, "Accurate and robust localization of duplicated region in copy–move image forgery," Springer-Verlag Berlin Heidelberg 2013.