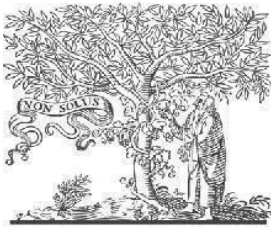


COPYRIGHT



ELSEVIER
SSRN

2024 IJEMR. Personal use of this material is permitted. Permission from IJEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper; all copy right is authenticated to Paper Authors

IJEMR Transactions, online available on 20th Dec 2024. Link

<https://ijiemr.org/downloads.php?vol=Volume-13&issue= Issue12>

DOI:10.48047/IJEMR/V13/ISSUE12/49

Title: " MEDICAL IMAGE FORGERY DETECTION FOR SMART HEALTHCARE"

Volume 13, ISSUE 12, Pages: 366 - 369

Paper Authors

Dr.K.Niranjan Reddy, Mr.Sk.Shadab, Mr.S.Pavan, Mr.M.Mahesh Naik



USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper as Per **UGC Guidelines** We Are Providing A Electronic Bar code

MEDICAL IMAGE FORGERY DETECTION FOR SMART HEALTHCARE

Dr.K.Niranjan Reddy¹, Mr.Sk.Shadab², Mr.S.Pavan³, Mr.M.Mahesh Naik⁴

¹Associate Professor and HOD, Department of ECE, CMR Institute of Technology, Medchal, Hyderabad.

^{2,3,4}Bachelor's Student, Department of ECE, CMR Institute of Technology, Medchal, Hyderabad.

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 super pixels 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 copy-move forgery detection methods.

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 [1], which is to paste one or several copied region(s) of an image into other part(s) 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 detection methods can be categorized into two main categories: block-based algorithms [1-13] and feature key point-based algorithms [14-19].

II. Literature Review

The goal in copy-move forgery detection is detecting duplicated image regions, even if they are slightly different from each other. One direct solution to this problem would be an exhaustive search, which involves comparison of the image to every cyclic-shifted version of itself. However, this approach would be computationally very expensive and would take $(MN)^2$ steps for an image of size $M \times N$. Also, this type of search might not work in the case where the copied area has undergone some modifications.

A second and more efficient approach, which was proposed by Fridrich et al. in [6], is the use of autocorrelation properties. Nevertheless, this approach is shown to be effective only when the duplicated regions were a large portion of the image. Another approach, which is the main interest of this paper, is block-matching procedure. In this approach, the image is segmented into overlapping blocks first. The task here is to detect connected image blocks that are copied and moved, instead of detecting the whole duplicated region. Note that the copied region would consist of many overlapping blocks and since each block would be moved with the same amount of shift, the distance between each duplicated block pair would be the same, as well. Therefore, the forgery decision can be made only if there are more than a certain number of similar image blocks within the same distance and these blocks are connected to each other so that they form two regions of the same shape.

Adaptive Over-Segmentation algorithm The Adaptive Over-Segmentation algorithm, which is similar to 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 into non-overlapping regions of irregular shape as image blocks afterward, the forgery regions can be detected by matching those non-overlapping and irregular regions. Segmentation method, the non-overlapping segmentation can decrease the computational expenses compared with the overlapping blocking; furthermore, in most cases, the irregular and meaningful regions can represent the forgery region better than the regular blocks. However, the initial size of the super pixels in SLIC is difficult to decide. In practical applications of copy-move forgery detection, the host images and the copy-move regions are of different sizes and have different content, and in our forgery detection method, different initial sizes of the super pixels can produce different forgery detection results; consequently, different host images should be blocked into super pixels of different initial sizes, which is highly related to the forgery detection results.

III. PROPOSED METHOD

This section describes the proposed image forgery detection using adaptive over-segmentation and feature point matching in detail. Fig. 1 shows the framework of the proposed image forgery detection scheme. First, an adaptive over-segmentation method is proposed to segment the host image into non-overlapping and irregular blocks called Image Blocks (IB). Then, we apply the Scale Invariant Feature Transform (SIFT) in each block to extract the SIFT feature points as Block Features (BF). Subsequently, the block features are matched with one another, and the feature points that are successfully matched to one another are determined to be Labeled Feature Points (LFP), which can approximately indicate the suspected forgery regions. Finally, we propose the Forgery Region Extraction method to detect the forgery region from the host

image according to the extracted LFP. In the remainder of this section, Section II-A explains the proposed Adaptive Over-Segmentation method in detail; Section II-B introduces the Feature Point Extraction using SIFT; Section II-C describes the Block Feature Matching procedures; and Section II-D presents the proposed Forgery Region Extraction method.

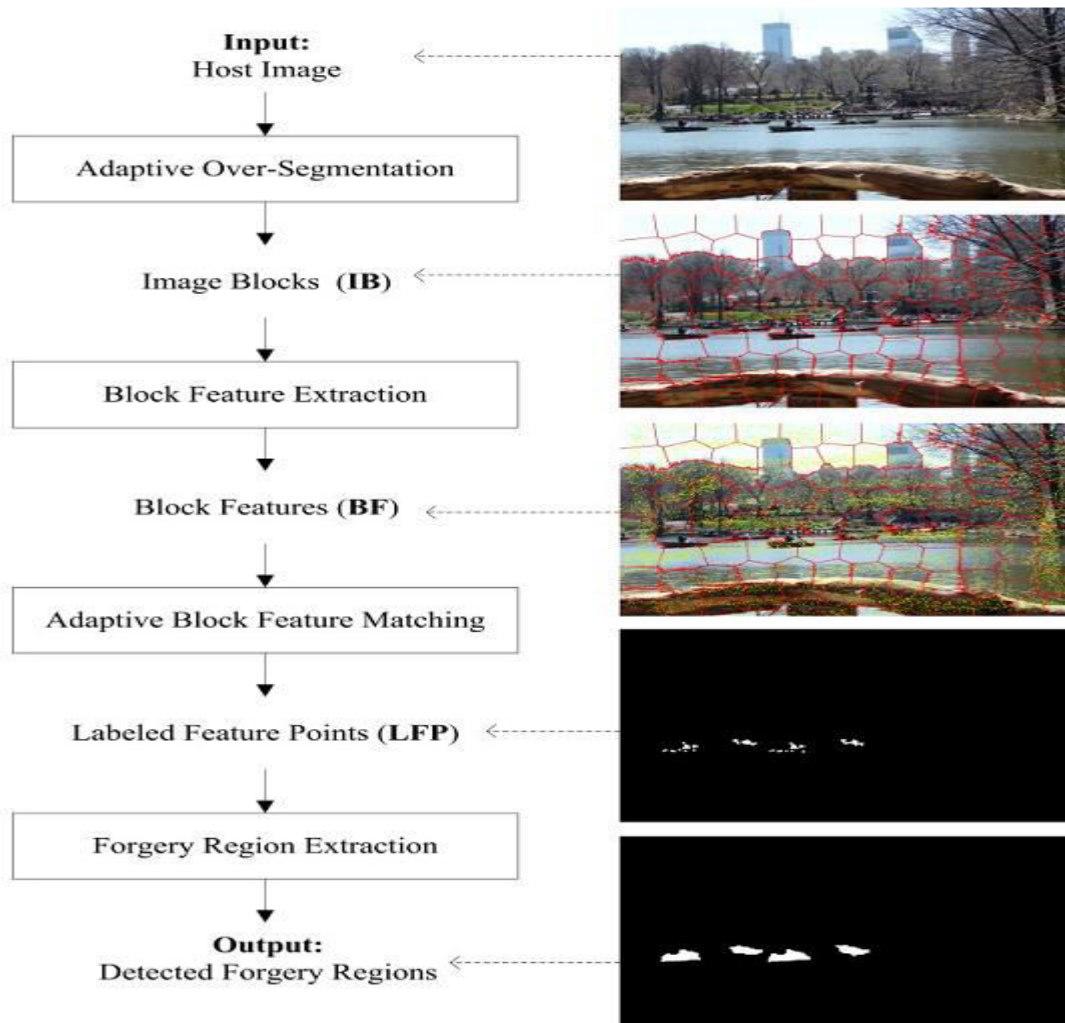


Fig. 1 Framework of the proposed copy-move forgery detection scheme

- Operating system : Windows XP/7.
- Coding Language : MATLAB
- Tool : MATLAB R 2012
- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

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 Over-Segmentation 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. We demonstrate the effectiveness of the proposed scheme with a large number of experiments. 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, compared with the existing state-of-the-art copy-move forgery detection schemes. Future work could focus on applying the proposed forgery detection scheme based on adaptive over-segmentation and feature-point matching on other types of forgery, such as splicing or other types of media, for example, video and audio

V. 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] A. C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions," Dept. Comput. Sci., Dartmouth College, Tech. Rep. TR2004-515, 2004.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] 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.