International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue 13
October 2017

Advanced Techniques for Image Forgery Detection

[1]NAVYA SRI BANDARI, [2]NAAGESHWAR RAO

[1]Pg Scholar, Department of ECE, Vaageswari College of engineering, Karimnagar

[2]Assoc.Prof, Department of ECE, Vaageswari College of engineering, Karimnagar.

ABSTRACT

Image lookalike mechanism use of numerical drawing to hide meaningful tip of your instance. The exposé of solid version be necessitated per head right of credibility and to hold integrity of your idea. Reproduction–flow twin revelation subject matter victimization sturdy up distribution and feature motive factor analogous is submitted. The schemed theory integrates both stall-based totally and key point-primarily based dual uncovering strategies. The purposed flexible extra-vivisection algorithm segments the pick out up the check drawing in the route of thru to non-traverselylapping and irregular impedes robustly. Then, the star points are extracted from every stall as intercept stars, and the clog articles are matched conjointly to discover the categorized trait points; this plan can especially factor out the suspected phony areas. To discover the imitation regions extra correctly, we recommend the work alike place extraction set of rules which replaces the spotlights point with small notable pixels as article close offs and them merges the neighboring impedes that have similar local coloration advertises in the path of via to the issue deter to generate the merged regions. Finally, it applies the morphological operation to merged areas to generate the detected lookalike areas. In reduce-paste version imposture ferreting out, schemed microcomputer idea forensic techniques capable of detecting worldwide and local assessment enhancement, figuring out the usage of histogram equalization

1. INTRODUCTION

In this era, Digital Image Forgery has been increasingly easy to perform, so the reliability of the image is thus becoming an important issue to be focus on. It does not differ very much in nature to conventional image forgery. Instead of using photograph digital image forgery deals with the digital image. By using the tool such as Adobe Photoshop, GIMP, Coral Paint fake images can be created as some of the tools are open source. Image forgery may lead to hazards. In banking system image forgery is a big threat, this result into big frauds. Nowadays detecting these types of forgeries has

become very useful to reduce these problems at present. To determine whether a digital image is original is a big challenge. To find the marks of tampering in a digital image is a challenging task. Tampering is normally done to cover objects in an image in order to either produce false proof or to make the image more pleasant for appearance. There are many cases in digital image forgery, all this cases are classified into three categories based on the process of creating fake images the group are image retouching, and image splicing, copy-move attack. Image forgery is basically a modification of image to conceal some meaningful or useful information. The common manipulations of a digital image are copy-move and cut-paste forgery.

1.1 COPY-MOVE FORGERY DETECTION

Copy-move forgery, which is to paste one or several copied region of an image into other part 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. Earlier blocked based forgery detection was used to detect forged image but this algorithm faced some drawbacks such as the host image is divided into over-lapping rectangular blocks, which would be computationally expensive as the size of the image increases and it was less efficient as it take more time to be process. To avoid such drawbacks along with the blocked based forgery, we proposed an image-blocking method called Adaptive OverSegmentation that divided the host image into non overlapping blocks adaptively with the help of two algorithm those are Simple Linear Iterative Clustering (SLIC) to segment the host image into irregular blocks and Discrete Wavelength Transform (DWT) which is employed to analyze the frequencies of the super pixel. Further the image block formed are pass to the Block Feature Extraction method where the block feature are extracted by using Scale Invariant Feature Transform (SIFT) as it possessed constant and better performance compared with the other extraction method. Further the process of Block Feature Matching is carried out which used Simple Linear Iterative Clustering (SLIC) for calculating super pixel and Discrete Wavelength Transform for finding super pixel from one block and checking other for other blocks. When the features are extracted and matched then we get to know which regions the host image has been

forged. 1.2 Cut-And Paste Image Forgery Detection Cut-and paste image forgery consists of creating a composite image by replacing a contiguous set of pixels in one image with a set of pixels corresponding to an object from a separate image. If the two images used to create the composite image were captured under different lighting environments, an image forger may need to perform contrast enhancement on so that lighting conditions match across the composite image. Failure to do this may result in a composite image which does not appear realistic. Image forgeries created in this manner can be identified by using localized contrast enhancement detection to locate, the cut-and-pasted region.

2. PROBLEM DEFINITION

In existing blocked based forgery detection faced some drawbacks such as the host image is divided into over-lapping rectangular blocks and it was computationally expensive in terms of size, so the need to overcome this problem was necessary for accurate and efficient results. Hence, proposed an image-blocking method called Adaptive OverSegmentation that divided the host image into non overlapping blocks adaptively with the help of two algorithm those are Simple Linear Iterative Clustering (SLIC) to segment the host image into irregular blocks and Discrete Wavelength Transform (DWT) which is employed to analyze the frequencies of the super pixels. Further the image block formed are pass to the Block Feature Extraction method where the block feature are extracted by using Scale Invariant Feature Transform (SIFT) as it possessed constant and better performance compared with the other extraction methods.

3.LITERATURE SURVEY

The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the tampered region can be obtained by matching blocks of image pixels or transform coefficients. Fridrich [7], proposed a forgery detection method in which the input image was divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks were matched to find the tampered regions. In [8], proposed a method for detecting copy-move forgery over images tampered by copy-move. To detect such forgeries, the given image is divided into overlapping blocks of equal size, feature for each block is then extracted and represented as a vector, all the

extracted feature vectors are then sorted using the radix sort. DWT and SIFT [2] algorithms are proposed for copy-move detection. With DWT, the low frequency information or image is obtained. With SIFT robustness is introduced, here it detect forgery of the image even it is copied, rotate scale and then pasted. In [3], survey done on various image forgery detection techniques and finally conclude the comparative study with some parameters. Also tools are mentioned to detect the forged images that travel over the network or by natural way for daily forensics, image processing, and security. Salam A.Thajeel [4], discussed digital image forensics and its types, challenges and research problems and detail analysis of the existing approaches for detect image tampering. Author also discussed block based method and key point-based method and popular techniques of two methods. Moreover, most of the methods may not address the problems. Therefore, there is a need to develop techniques that is efficient to deal with these challenges. The Speeded Up Robust Features (SURF) [6] were applied to extract features instead of SIFT. However, although these methods can locate the matched key-points, 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 [5]. A novel copy–move forgery detection scheme using adaptive over segmentation and feature point matching [1] is proposed, that integrates both block-based and key point-based forgery detection methods. Methods for detecting locally applied contrast enhancement as well as a method for identifying histogram equalization [9] are proposed. By observing that the intrinsic fingerprints of contrast enhancement operations add energy to the high frequency components of an image's pixel value histogram, we developed a global contrast enhancement detection technique. We extended this technique into a method for detecting locally applied contrast enhancement and demonstrated its usefulness for detecting cut and paste type forgeries. A novel algorithm is proposed to identify the source-enhanced composite image created by enforcing contrast adjustment on either single or both source regions [10].The two source images used for creating cut-and-paste type of forged images may have different color temperature or luminance contrast. So, in order to make the forged image more real, contrast enhancement is performed on either one or both the regions.

4.IMPLEMENTATION:

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.

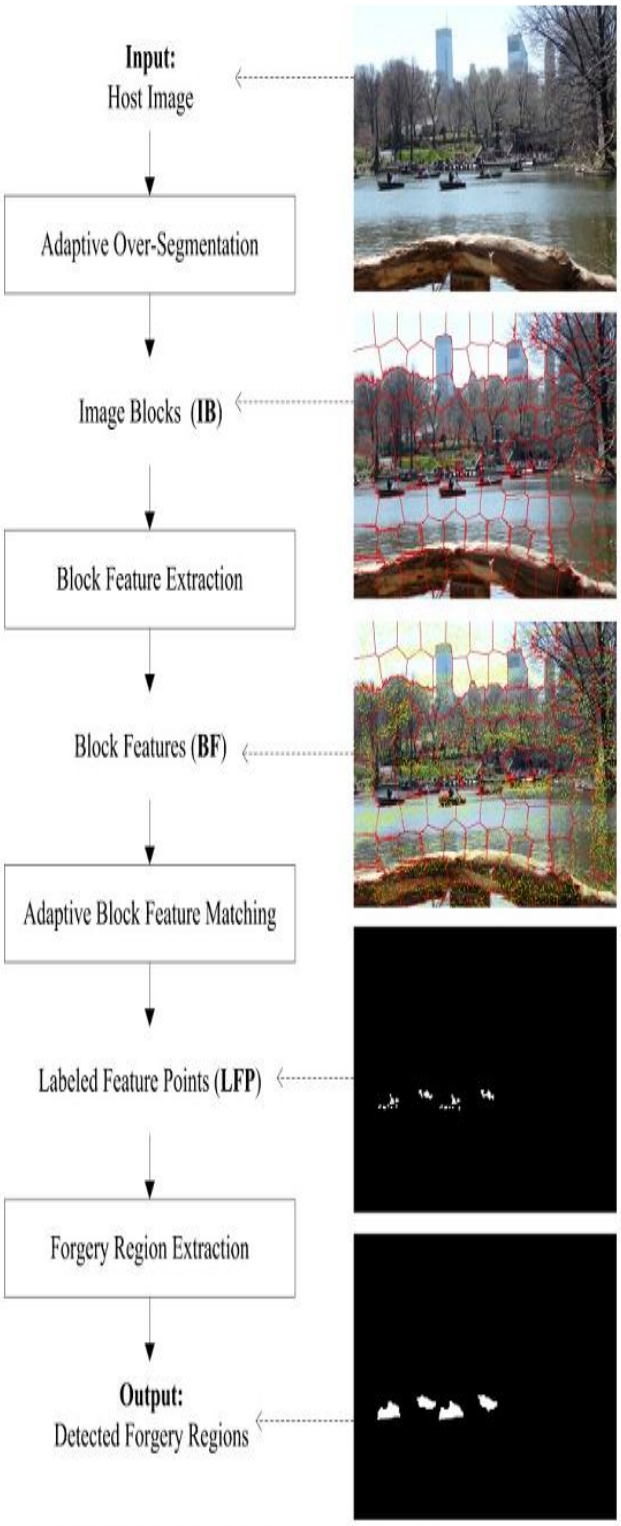
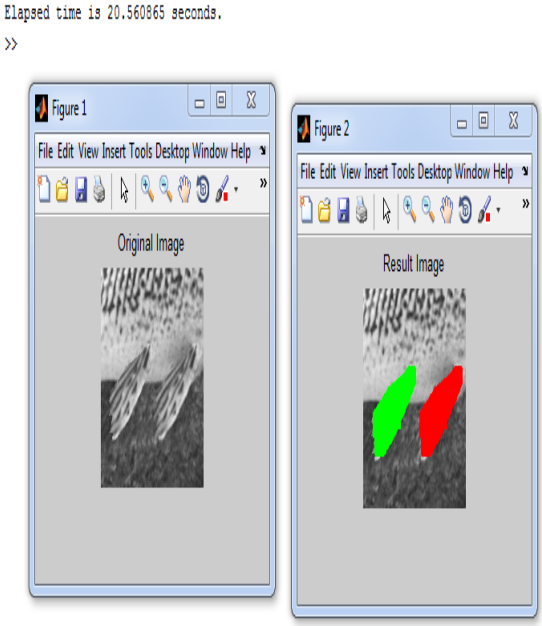


Fig. 1 Framework of the proposed copy-move forgery detection scheme

5.RESULTS:



6. 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

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.

[7] 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.

[8] 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.

[9] 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.

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