International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

Implementation of image forgery detection using adaptive over segmentation and feature point matching

P.Srilatha
Assistant professor,Dept. of ECE, SR Engineering College,Telangana, India

Abstract: The proposed scheme assimilates both block-based and keypoint-based forgery detection methods. First, the proposed Adaptive Over Segmentation algorithm segments the host image into nonoverlapping 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.

Keywords- Copy-Move Forgery Detection, Adaptive Over-Segmentation, Local Color Feature, Forgery Region Extraction

I. INTRODUCTION

We are undoubtedly living in an age where we are exposed to a remarkable array of visual imagery. While we may have historically had confidence in the integrity of this imagery, today's digital technology has begun to erode this trust. From the tabloid magazines to the fashion industry and in mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our email in-boxes, doctored photographs are appearing with a growing frequency and sophistication. Over the past five years, the field of digital forensics has emerged to help restore some trust to digital images. Here we review the state of the art in this new and exciting field. Digital watermarking has been proposed as a means by which an image can be authenticated. The drawback of this approach is that a watermark must be inserted at the time of recording, which would limit this approach to specially equipped digital cameras. In contrast to these approaches, passive techniques for image forensics operate in the absence of any watermark or signature. These techniques work on the assumption that although digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image. The set of image forensic tools can be roughly grouped into five categories: 1) pixel-based techniques that detect statistical anomalies introduced at the pixel level; 2) format-based techniques that leverage the statistical correlations introduced by a specific lossy compression scheme; 3) camera-based techniques that exploit artifacts introduced by the camera lens, sensor, or on-chip post processing.

As the use of images have been increasing day by day in our lives, with the introduction of digital technology, The forgery of digital image has become more and more simple and indiscoverable. Today's digital technology had begun to erode the integrity of images and image counterfeiting and forgeries with the move to the world of Megapixels, opens a new door to the dark-side of it. We are living in an age, where anything can be manipulated or altered with the help of modern technology. With the increasing applications of digital imaging, different types of software tools are introduced for processing images and images. They are used to make forge images to make it look real or objects can be added or deleted. For decades, images have been used to document and they have used as evidence in courts. But this process is very time consuming and requires expert knowledge so it is hard to implement than digital pictures. Today, however, powerful digital image editing software makes image modifications straightforward [1]. Today's digital technology has begun to remove trust in our knowledge, as from the magazines, to fashion world and in scientific journals, political campaigns, courts and the photo

that come in our e-mail. In all of these forged photographs are appearing with a more frequencies and sophistication. In the increase in the availability of multimedia data in digital form has come to a tremendous growth of tools to manipulate digital multimedia contents. The process of creating fake image has been tremendously simple with the introduction of new and powerful computer graphics editing software which are freely available as Photoshop, GIMP, and Corel Paint Shop.

II. RELATED WORK

Amruta Jagtap et al [1] this paper proposes a Verifying the integrity of images and detecting traces of tampering without requiring more previous data of the image content material or any embedded watermarks is an essential research subject. An attempt is made to survey the recent traits within the field of virtual image forgery detection. And a singular reproduction-circulate forgery detection scheme using adaptive over-segmentation and feature point matching. Also, it explained the scheme integrates each block-primarily based and keypoint-based forgery detection strategies. The proposed adaptive over-segmentation algorithm segments the host image into non-overlapping and irregular blocks adaptively. Then, the function factors are extracted from every block as block capabilities, and the block capabilities are matched with each other to discover the categorized function points; this manner can about indicate the suspected forgery regions. To hit upon the forgery areas extra as it should be, we suggest the forgery place extraction algorithm, which replaces the feature points with small superpixels as feature blocks after which merges the neighboring blocks that have comparable neighborhood shade capabilities into the function blocks to generate the merged regions. Finally, it applies the morphological operation to the merged areas to generate the detected forgery regions.

A. J. Fridrich et al [2] described to the existing strategies, the reproduction-pass forgery detection methods may be categorised into most important categories: block-primarily based algorithms and function keypoint-based algorithms. This paintings comes underneath block-primarily based forgery detection techniques. The current block-primarily based forgery detection techniques divide the enter images into overlapping and everyday picture blocks; then, the tapered area can be obtained via matching blocks of image pixels or remodel coefficients. And proposed a forgery detection technique wherein the input image turned into divided into over-lapping rectangular blocks, from which the quantized Discrete Cosine Transform (DCT) coefficients of the blocks had been matched to locate the tampered regions.

Sreelakshmi M. Et al [3] proposes for a Method Image functions in an image may be added up or removed, without leaving any obvious lines in the photo. Thus the method referred to as forensic detection is used to stumble on such manipulations passed off in an image by means of recovering the history of an picture. Here recovers the data of filtered JPEG image the usage of an effective linear classifier that discriminates the forensic image with its skilled data. Copy- circulate forgery is a sort of photo forgery wherein a portion of the image receives copied and pasted at every other vicinity of the same image, which can't be detected by way of bare eye. The method to hit upon such forgery is to initially phase the image the use of adaptive block segmentation and capabilities are extracted from each image blocks and examine each block to one another to discover the fit. Label the matched points to extract the cast location. The Hence forged vicinity is detected.

Musaed Alhussein et al [4] the picture tampering includes each splicing and duplicate-circulate forgery. First, the image become decomposed into 3 shade channels (one luminance and two Chroma), and every channel changed into divided into nonoverlapping blocks. Local textures within the shape of the neighborhood binary sample (LBP) had been extracted from each block. The histograms of the patterns of all the blocks had been concatenated to shape a feature vector. The characteristic vector become then fed to an ELM for category. The ELM is a effective and fast class method. The experiment turned into performed using publicly to be had databases. The experimental results confirmed that the proposed method finished excessive detection accuracy in both the databases.

III. PROPOSED SCHEME

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 blockbased 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 Oversegmentation 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.

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.

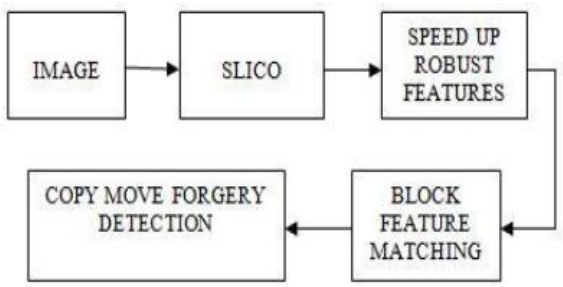

Fig.1 Block diagram of proposed system

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 blockbased 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

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

REFERENCES

[1] Amruta Jagtap, H. A. Hingoliwala, H. A. Hingoliwala, “Survey Paper on Advanced Techniques for Image Forgery Detection”, International Journal of Science and Research (IJSR), Vol 4 Issue 12, 2015.

[2] A. J. Fridrich, B. D. Soukal, and A. J. Lukáš, "Detection of copy-move forgery in digital images," 2003.

[3] Sreelakshmi. M, Amrutha M, “Forgery and Forensic Detection Using Adaptive over segmentation and DCT of JPEG Images”.

[4] Chi-Man Pun, Chen Yuan, Xiu-Li Bi,” Image Forgery Detection Using Adaptive Over-Segmentation and Feature Point Matching”.

[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 copyrotate-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 copymove forgery," in Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on, 2009, pp. 1053-1056.

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

[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 regionduplication 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.