International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey Paper on Advanced Techniques for Image Forgery Detection

Amruta Jagtap.[1], H. A. Hingoliwala[2]

[1]M.E(Computer) Department of Computer Engineering, Jaywantrao Sawant College of Engineering, Pune, India, Savitribai Phule University of Pune, Maharashtra, India -411007

[2]Professor and Head of Department of Computer Engineering, Jaywantrao Sawant College of Engineering, Pune, India, Savitribai Phule University of Pune, Maharashtra, India -411007

Abstract: ***Today manipulation of digital images has become easy due to powerful computers, advanced photo-editing software packages and high resolution capturing devices. Verifying the integrity of images and detecting traces of tampering without requiring extra prior knowledge of the image content or any embedded watermarks is an important research field. An attempt is made to survey the recent developments in the field of digital image forgery detection. This paper proposes a novel copy–move forgery detection scheme using adaptive over-segmentation and feature point matching. The proposed scheme integrates both block-based and key point-based forgery detection methods. 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.***

Keywords: Copy-move forgery detection, adaptive over-segmentation, feature point matching, forgery region extraction.

1. Introduction

Digital image play a significant role in different technologies and fields. The use of digital cameras, personal computers, and sophisticated image processing software available for modification and for manipulation of image. These tools are scalable and provides user interface features. An image can be manipulated easily through image-processing tools and use for hiding some meaningful or useful information to make forged images [1]. The basic aim of image forensics to address image integrity and authenticity. Image slicing, cloning, tempering has been done to make forged images and integrity of image is lost. These digital forged images are not recognizable and so real and authenticity is lost.

The forgeries are classified into five major categories: image retouching, Image Splicing, Copy-Move (cloning), Morphing, Enhanced [2]. The first type is image retouching, where the method is used for enhances an image or reduces certain feature of an image and enhances the image quality for capturing the reader's attention. In this method, the professional image editors change the background, fill some attractive colors, and work with hue saturation for toning and balancing. The second type is image splicing where the different elements from multiple images are juxtapose in a single image to convey an idea. Such splicing can usually be detected by searching the splicing boundary, or by considering the directions of the light incident on surfaces in the image. Inconsistencies in lighting or blurred splicing boundaries can be used to expose the above images as fake, if the light direction can be correctly estimated or if the splicing boundary can be correctly detected respectively [4]. The third type is copy-move attack and same like image splicing because in both techniques modify the image area to use other images. The some portion of base image uses in copy-move attack instead of external image as a source. The parts of base image copy and move to modified image and pastes. This method usually for hide definite particulars or to matching convinced features of an image. The blur tool is use for retouching borders and decrease the effect between original and pasted area [7]. Copy-move forgeries are usually detected by searching for matching regions in the image, although recent research has taken a more feature-based approach, concentrating on matching features rather than blocks, in order to allow form various image transformations that can be used to create more convincing forgeries. The forth type is Morphing and in this type the image and video can be exposed into unique influence , were the one object on image is turned into to another object in the other image. The morphing is used to transfer the one-person image from another person image by using seamless transition between two images [2].

A copy-move forgery denotes an image where part of its content has been copied and pasted within the same image. Typical motivations are either to hide an element in the image, or to emphasize particular objects, e.g., a crowd of demonstrators. A copy-move forgery is straightforward to create. Additionally, both the source and the target regions stem from the same image, thus properties like the color temperature, illumination conditions and noise are expected to be well-matched between the tampered region and the image. The fact that both the source and the target regions are contained in the same image is directly exploited by many CMFD algorithms.

The copy-move forgery detection methods can be categorized into two main categories: block-based algorithms and feature key point-based algorithms [2]. In both cases, preprocessing of the images is possible. For instance, most

methods operate on grayscale images, and as such require that the color channels be first merged. For feature extraction, block-based methods subdivide the image in rectangular regions. For every such region, a feature vector is computed. Similar feature vectors are subsequently matched. By contrast, key point-based methods compute their features only on image regions with high entropy, without any image subdivision. Similar features within an image are afterwards matched. A forgery shall be reported if regions of such matches cluster into larger areas. Both, key point-based and block-based methods include further filtering for removing spurious matches [2].

2. Literature Survey and Related Work

The existing block-based forgery detection methods divide the input images into overlapping and regular image blocks; then, the forgery regions were detected by matching those blocks [8]. 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.

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, those features mainly reflect the content of the image blocks, leaving out the location information. In addition, the features are not resistant to various image transformations.

Although block-based forgery detection 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 [1].

Although the existing key point-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 key point-based forgery methods were very poor.

3. Proposed System

To address the above-mentioned problems, we propose a novel copy-move forgery detection scheme using adaptive over-segmentation and feature point matching [1]. The proposed scheme integrates both the traditional block-based forgery detection methods and key point-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 key point-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 into the merged regions to generate the detected forgery regions.

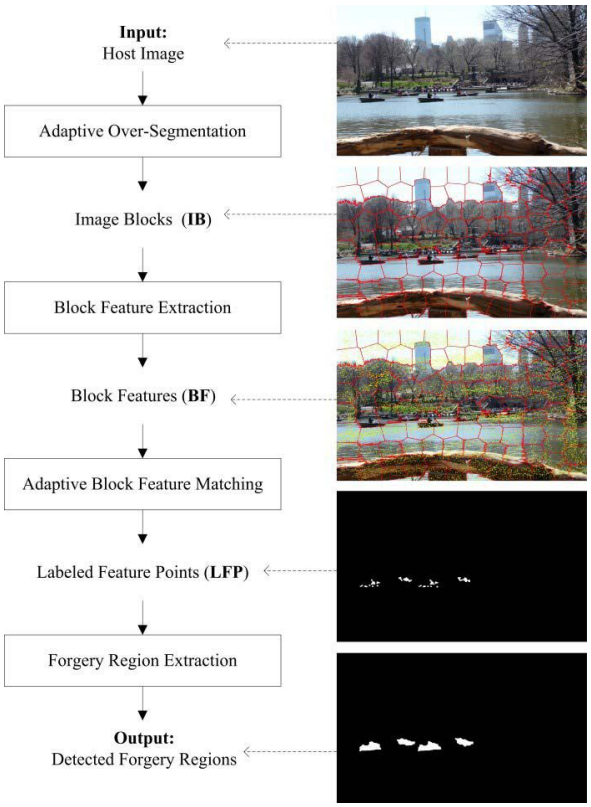

Figure 1: Framework of the proposed copy-move forgery detection scheme.

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 [4]. 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, which can approximately indicate the suspected forgery regions. Finally, to detect the more accurate forgery regions, we propose the Forgery Region Extraction algorithm, in which the labeled feature points are replaced with small super pixels 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.

4. Conclusion

In this paper, I have presented 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. Region Extraction algorithm, in which the labeled feature points are replaced with small super pixels 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] Chi-Man Pun , Xiao-Chen Yuan and Xiu-Li Bim, **"** Image Forgery Detection Using AdaptiveOver segmentation and Feature Point Matching**",** IEEE Trans. Inf. Forensics Security, Vol. 10, No. 8, August 2015.
[2] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess, and Elli Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions On Information Forensics And Security, Vol. 7, No. 6, December 2012.
[3] M. Kirchner And R. Bohme, "HIDING TRACES OF RESAMPLING IN DIGITAL IMAGES, " Information Forensics And Security, IEEE Transactions On, Vol. 3, Pp. 582-592, 2008
[4] H. Huang, W. Guo, and Y. Zhang, "Detection of copy–move forgery in digital images using SIFT algorithm," in Proc. Pacific-Asia Workshop Comput. Intell. Ind. Appl. (PACIIA), Dec. 2008, pp. 272–276.
[5] B. L. Shivakumar and S. S. Baboo, "Detection of region duplication forgery in digital images using SURF," IJCSI Int. J. Comput. Sci. Issues, vol. 8, issue 4. no. 1, pp. 199–205, 2011.
[6] H. J. Lin, C. W. Wang, and Y. T. Kao, "Fast copy–move forgery detection, " WSEAS Trans. Signal Process., vol. 5, no. 5, pp. 188–197, 2009.
[7] 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.
[8] J. Fridrich, D. Soukal, and J. Lukáš, "Detection of copy–move forgery in digital images, " in Proc. Digit. Forensic Res. Workshop, Cleveland, Aug. 2003.
[9] Z. Mohamadian And A. A. Pouyan, "Detection Of Duplication Forgery In Digital Images In Uniform And Non-Uniform Regions, " In Uksim, 2013, Pp. 455-460.
[10] N. D. Wandji, S. Xingming, And M. F. Kue, "Detection Of Copy-Move Forgery In Digital Images Based On Dct, " International Journal Of Computer Science Issues (IJCSI), Vol. 10, 2013.
[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] R. Davarzani, K. Yaghmaie, S. Mozaffari, And M. Tapak, "Copymove Forgery Detection Using Multiresolution Local Binary Patterns, " Forensic Science International, Vol. 231, Pp. 61-72, 2013.
[13] J. Zhang, Z. Feng, and Y. Su, "A new approach for detecting copymove forgery in digital images, " in Proc. Int. Conf. Communication Systems, Nov. 2008, pp. 362–366.
[14] V. Christlein, C. Riess, and E. Angelopoulou, "A study on features for the detection of copy-move forgeries, " in Proc. GI SICHERHEIT, Berlin, Germany, Oct. 2010, pp. 105–116.
[15] X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, "Image copy-move forgery detection based on SURF, " Multimedia Inf. Netw. Security, pp. 889–892, Nov. 2010.
[16] S. Ryu, M. Lee, and H. Lee, "Detection of copy-rotate-move forgery using Zernike moments, " in Proc. Information Hiding Conf., Jun. 2010, pp. 51–65.
[17] H. Lin, C. Wang, and Y. Kao, "Fast copy-move forgery detection, " WSEAS Trans. Signal Process., vol. 5, no. 5, pp. 188–197, 2009.
[18] I. Amerini et al., "A SIFT-based forensic method for copy_move attack detection and transformation recovery, " IEEE Trans. Inf. Foren. Sec., Vol. 6, no 3, pp. 1099_111, 2011.

Author Profile

Ms. Amruta P. Jagtap, is currently pursuing M.E (Computer) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. She received her B.E (Information Technology) Degree from DPCOE, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. She is currently working as Asst. Prof and I.C.T Instructor at A.E.I, Pune, Maharashtra, India -411007. Her area of interest is Information Security and Image Processing.

Prof. H. A. Hingoliwala, received M.E (Computer Science and Engineering) Degree. He received B.E (Computer Engineering) Degree. He is currently working as Head of Department Of Computer Engineering of Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His area of interest is Networking and Image processing.