Bulletin of Electrical Engineering and Informatics
Vol. 7, No. 3, September 2018, pp. 345~349
ISSN: 2302-9285, DOI: 10.11591/eei.v7i3.754

A New Copy Move Forgery Detection Technique Using Adaptive Over-segementation and Feature Point Matching

Anil Gupta
MIET, Kot Bhalwal, Jammu, India

Article Info

Article history:

Received Sep 09, 2017
Revised May 25, 2018
Accepted Jun 08, 2018

Keywords:

Copy-move image forgery
Image forgery
Image forgery detection
Tampering

ABSTRACT

With the development of Image processing editing tools and software, an image can be easily manipulated. The image manipulation detection is vital for the reason that an image can be used as legal evidence, in the field of forensics investigations, and also in numerous various other fields. The image forgery detection based on pixels aims to validate the digital image authenticity with no aforementioned information of the main image. There are several means intended for tampering a digital image, for example, copy-move or splicing, resampling a digital image (stretch, rotate, resize), removal as well as the addition of an object from your image. Copy move image forgery detection is utilized to figure out the replicated regions as well as the pasted parts, however forgery detection may possibly vary dependant on whether or not there is virtually any post-processing on the replicated part before inserting the item completely to another party. Typically, forgers utilize many operations like rotation, filtering, JPEG compression, resizing as well as the addition of noise to the main image before pasting, that make this thing challenging to recognize the copy move image forgery. Hence, forgery detector needs to be robust to any or all manipulations and also the latest editing software tools. This research paper illustrates recent issues in the techniques of forgery detection and proposes a advanced 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.

Corresponding Author:

Anil Gupta,
Department of Information Technology,
Model Institute of Engineering and Technology, Kot Balwal, Jammu, India
Email: anil.it@mietjammu.in

1. INTRODUCTION

The present day digital revolution has changed the format of accessing, manipulating and sharing information, however these developments have also given rise to different security issues. Complex digital technology and various photo-editing software like Adobe Photoshop etc. are universal and have made the task of forging images a common practice. [1]

Complex digital technology and different photo-editing software, such as Adobe Photoshop, are universal and thus have made the process of manipulating images to create forgeries a fairly common practice. As a result, trust in digital imagery has been eroded.

An example of digital forgery was seen in a Tunisian newspaper in which a photo was altered duplicating the crowd to appear large. Another example as shown in Figure 1 displays the altered photograph released by Iran showing four missiles instead of three [2]. This tampered image was also being published by various western media including The New York Times. The research in this paper attempts to address this need and provide some insight into this challenging problem.

(a) Original image (b) Forged image

Figure 1. Example of copy-move forgery

2. IMAGE TAMPERING

Image tampering is defined as "adding or removing important features from an image without leaving any obvious traces of tampering" and thus image tampering is considered as intentional manipulation of images for malicious purposes [3]. There are various techniques for counterfeiting images and these can be classified into three broad categories.

Copy-Move attack, also called Cloning, is a technique in which instead of having an external image as the source, it uses portion of the original base image as its source. Therefore, the source and the destination of the modified image originate from the same image. Photoshop Clone Stamp Tool can be used to achieve such type of forgery. Blurring is usually applied along the border of the modified region to reduce the effect of irregularities between the original and pasted region.

The second type of image tampering techniques is known as Image-Splicing, which is a technique that involves a composite of two or more images which are combined to create a fake image. Thus, by sticking together photographic images a spliced image is being obtained. [4]

And the third category of image tampering technique is known as Image-Retouching in which certain features of image are being enhanced or reduced in order to make the image more attractive. Thus, this type forgery is considered less harmful and is used mostly by the magazine editors. [5]

3. TECHNIQUES TO COUNTERATTACK FORGERY

To detect above mentioned digital forgeries in images two principle approaches are taken into account namely, **Active approach** and **Passive approach.** [6]

In active approach, during the creation of images pre-processing techniques like watermark embedding or signature generation are applied which limit the use of images in general. However, there are millions of digital images on internet which are without any digital watermark or signature. In this context *active approach* could not be used to find the authenticity of the image.

Therefore unlike the active approach, the passive approach does not need any embedded watermark or digitally generated signature. Mainly three techniques are widely used to tamper digital images namely Copy-Move, Splicing and Retouching as shown in Figure 2.

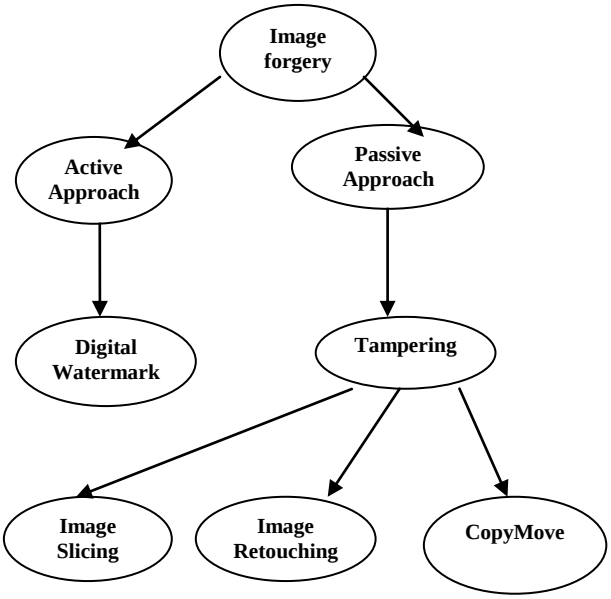

Figure 2. Image forgery techniques and their solutions

4. COPY/MOVE FORGERY DETECTION

The copy-move forgery detection methods can be categorized into two main categories: block-based algorithms and feature key point-based algorithms [7]. 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 [8].

5. PROPOSED SYSTEM

We propose a new copy-move forgery detection scheme using adaptive over-segmentation and feature point matching [9]. 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 3 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 [10]. 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. Table 1 shows literature review.

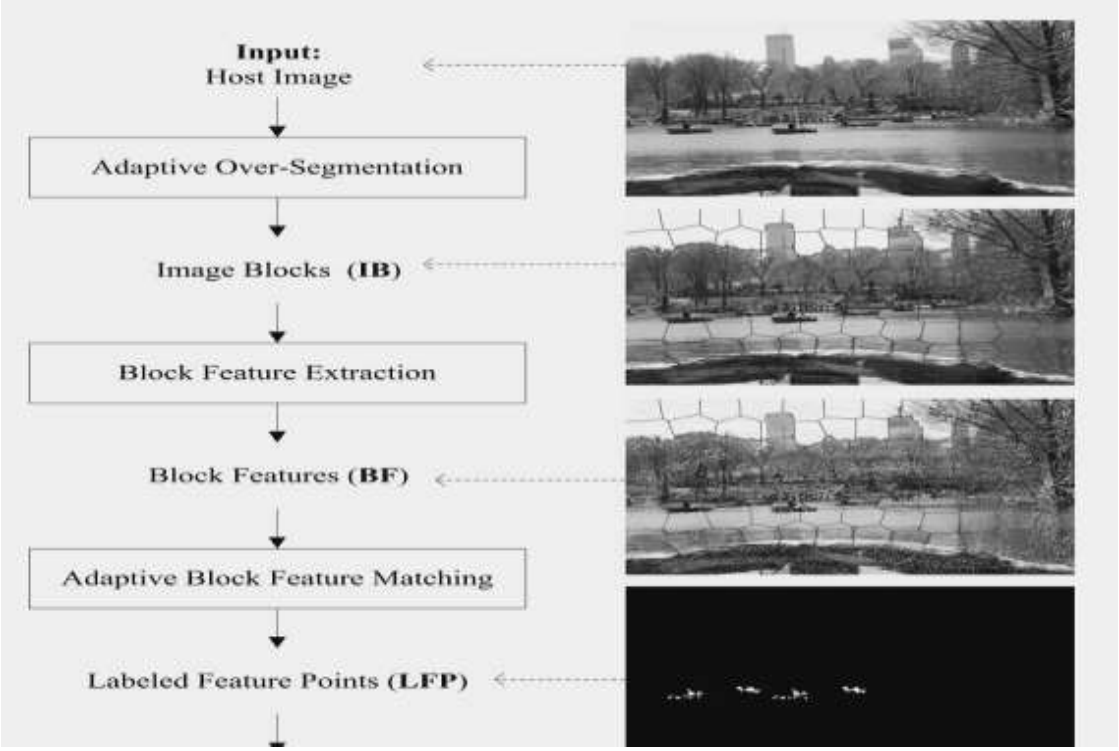

Figure 3. Framework of the proposed copy-move forgery detection scheme

Table 1. Comparision of Different Copy Move Image Forgery Techniques with the proposed method

Title	Method	Advantages	Disadvantages
Detection of Copy-Move Forgery in Digital Images [1]	Block based method. Image is divided to blocks and forged parts are detected with exact match and appropriate match	It can detect images with distortion format	Slow detection process
Exposing digital forgeries by detecting duplicated image regions [2]	Block based method. PCA applied to obtain reduced dimensional representation. Key-point based technique.	More reliable to detect noisy and lossy images	Sometimes it failed to detect difficult forgeries.
Robust Method for Detection of Copy-Move Forgery in Digital Images. [3]	Wavelet transform technique is used and computes phase correlation to detect similarity.	Lower computational complexity	Duplicated regions through angles and scaled regions cannot detect.
Segmentation-Based Image Copy-Move Forgery Detection Scheme [5]	Key-point based technique. Extracted key points from patches and matched for duplicated regions.	Segment image into semantically independent patches An accurate estimation of transform matrix is obtained by EM based algorithm [8]	Re-estimation of transform matrix is complex.
Region Duplication Detection Using Image Feature Matching [4]	Key point based method. By calculating SIFT key-points finds pixels within the duplicated regions.	Reliable than other key point techniques	Sometimes it gives vague results
A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery [6]	Key point based method. Key points are extracted and key point localization is done for detection.	Good at determine the Geometric transformation.	Not good at detection phase with respect to cloned image patch with high uniform texture
A New Copy Move Forgery Detection Technique using Adaptive over-Segementation and Feature Point Matching (Proposed Paper)	Adaptive over-segmentation and feature point matching Method	Yields better results when compared to the earlier techniques. Segments the host image into non-overlapping and irregular blocks adaptively.	No drawbacks

6. CONCLUSION

Digital forgery images created with copy-move operations are challenging to detect. In this paper, I have proposed a new 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.. 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] Jessica Fridrich, David Soukal, and Jan Lukáš, "Detection of Copy-Move Forgery in Digital Images", in *Proc. Digit. Forensic Res. Workshop*, Cleveland, OH, Aug. 2003.
[2] A.C. Popescu and H. Farid, "Exposing digital forgeries by detecting duplicated image regions", *Dept. Comput. Sci., Dartmouth College, Hanover, NH, USA, Tech. Rep.* TR2004-515, 2004
[3] Saiqa Khan, Arun Kulkarni, "Robust Method for Detection of Copy-Move Forgery in Digital Images", *International Conference on Signal and Image Processing*, 2010.
[4] L. Fitzpatrick and M. Dent, "Region Duplication Detection Using Image Feature Matching", *Ieee Transactions On Information Forensics and Security*, Vol. 5, No. 4, 2010.
[5] Jian Li, Xiaolong Li, Bin Yang and Xingming Sun, "Segmentation-Based Image Copy-Move Forgery Detection Scheme", *IEEE Transactions on Information Forensics and Security*, Volume: 10, Dec 2014.
[6] Chi-Man Pun, Xiao-Chen Yuan and Xiu-Li Bim, "Image Forgery Detection Using Adaptive Over segmentation and Feature Point Matching", *IEEE Trans. Inf. Forensics Security*, Vol. 10, No. 8, August 2015.
[7] Vincent Christlein, Christian Riess, Johannes Jordan, CorinnaRiess, 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.
[8] M. Kirchner And R. Bohme, "Hiding Traces of Resampling in Digital Images", Information Forensics And Security, *IEEE Transactions*, Vol. 3, Pp. 582-592, 2008
[9] 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.
[10] B.L. Shivakumar and S.S. Baboo, "Detection of region duplication forgery in digital images using SURF", IJCSI *Int. J. Comput. Sci. Issue*s, vol. 8, issue 4, no. 1, pp. 199–205, 2011.

BIOGRAPHY OF AUTHOR

Mr. Anil Gupta is working as a Assistant Professor with the Department of Information Technology, Model Institute of Engineering and Technology, Kot Balwal, Jammu, India. Mr. Anil Gupta has over Sixteen years of working experience. Mr. Anil Gupta has substantial academic work to his credit. As a distinguished academician he has published considerable number of research papers in various reputed national and international journals and he has also presented research papers in various national and international conferences. His has strong orientation towards Programming and specific areas of interest are Programming in C, C++, Java and MATLAB