ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Issue 4, April 2018

Copy-Move Image Forgery Detection Using Adaptive Over-Segmentation and Brute-Force Matching

Neema Antony[1], Binet Rose Devassy[2]
M.Tech Scholar, Electronics and Communication Engineering Department, Sahradya College of Engineering and Technology, Thrissur, India [1]
Asst.Professor, Electronics and Communication Engineering Department, Sahradya College of Engineering and Technology, Thrissur, India [2]

Abstract: Digital images are the most important route for exchange data, so the integrety of images are exceptionally fundamental. Digital images are generally utilized for different applications like therapeutic imaging, reporting, and advanced crime scene investigation. With the development of image editing tools and computer technology, digital images can easily forge. Copy-move forgery is one of the frequently used image forgery in digital image forensic field. This paper presents a new method to detect copy-move forgery is called adaptive over segmentation method. This method adaptively divided the input copy-move image into non-overlapping and irregular blocks. Using scale invariant feature transform(SIFT), the feature points are extracted from each blocks. After that, the feature points are matched with one another using brute force matching method. If any feature points are successfully matched with one another are determined to be labeled feature points.This step approximately illustrate the suspected forgery regions. To detect more accurate forgery regions, morphological operations are used. The proposed method is implemented on raspberry pi 3 model b using the OpenCV-Python platform.

Keywords: Copy-Move image forgery detection (CMFD), Adaptive over-segmentation, Brute-force matching, Morphological operation, OpenCV-Python, Raspberry Pi 3 model b.

I. Introduction

In the present advanced world, digital images are the major source of information. Images can be utilized as a confirmation for any occasion in the courtroom. The pictures communicated in any TV news are acknowledged as the authentication for the honesty of that news. Digital images are being utilized as a part of numerous applications ranging from military to medical diagnosis and from art piece to client photography. Digital image forensics is a rapidly increasing field of image processing area. The major problem present in image forensics is determining the specific image is authentic or not. Copy-move forgery is one type of image forgery in digital image forensic field. Due to technology development and availability of low-rate hardware and software tools, the digital images are very easy to manipulate without leaving the visible traces of manipulation and the digital image can be manipulated with a wide variety of manipulation methods, for example scaling, rotation, blurring, filtering, cropping, etc.

"Forgery" is the process of adding, changing or deleting some important features from the image. The image forgery is divided into three types namely, copy move, image splicing, image enhancement. Among this, copy move image forgery is one of the frequently used techniques. In copy-move image forgery, the copied part is pasted elsewhere in the same image to either add or hide objects. The noise, color and texture property of this type of image do not change. An example of copy-move forgery is shown in fig.1.

Copy –move forgery detection is divided into two types namely: block-based methods and key point based methods. In the existing block-based method, the input host image is divided into overlapping and regular image blocks. The forged region can be determined by matching blocks of image pixels. The commonly used block-based techniques are DCT, DWT, and SVD. But this existing block-based method has some disadvantages: 1) when the size of the image is large, the computational expense is increasing.Because the input image is divided into regular rectangular and over-lapping blocks, 2) the existing block-based methods cannot address geometrical transformations of the forgery regions, 3)their recall rate is low.Because the blocking method is a regular rectangular shape.

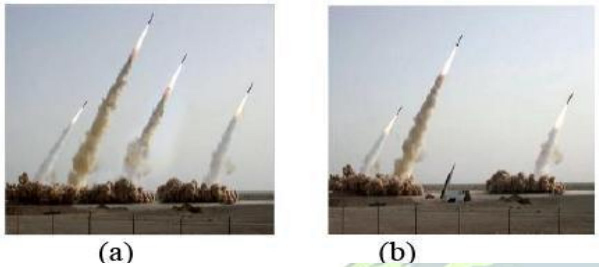


Fig. 1. Example of copy-move forgery [11] (a) the forged image with four missiles and (b) the original image with three missiles.

The existing keypoint based methods detect the forgery by spotting the high entropy areas, which are called the "keypoints". This method is less complex because it has fewer calculations and faster process. Commonly used key-point based methods are: Scale Invariant Feature Transform (SIFT) [5] and Speed up Robust Features (SURF) [7]. The existing keypoint based forgery detection method can avoid the first two problems of block-based method. The recall rate of existing keypoint based methods is very poor.

To solve above-discussed problems, the proposed method combines both block-based and keypoint based methods. It enhances the performance of copy-move image detection

II. Background

First DCT based copy move image forgery detection method (CMFD) is proposed by J. Fridrich et al. [1]. In this method, DCT applied on all small blocks of image and quantized DCT coefficient. After this Similar DCT coefficient block mark as tempered part on the image. Another DCT based Method is proposed by N. D.Wandji et al. [2]. Here Feature vector extracted from DCT coefficient of each block of image and sorted feature using lexicography. Similar pairs of blocks were marked as tempered part of the image. This method works efficiently in case of rotation, scale, blur, and noise.

Khan et al. [3] proposed a DWT based CMFD methods which methods applied DWT to compress image up to the fixed level. This fixed level depends on the size of the image. This process reduces the dimensional of the image.

Muhammad et al. [4] proposed a new method to detect the passive copy-move forgery. In their method, they used dyadic wavelet transform (DyWT) to analyze the data. The advantage of this method over the discrete wavelet transform (DWT) based transformation and there is no reduction of the wavelet coefficients within the scales. There are two main sets of information necessary to find the tempered areas in this method. The first set is to find the similarity between original and tempered areas. This information can be found using DyWT at scale one with coefficients of LL1 sub-band. The second set of information is to estimate noise of the original areas and tempered areas. It is found using DyWT at scale one by considering wavelet coefficients of HH1 sub-band.

S. Bayram et al. [5] proposed a CMFD method based on FMT (Fourier-Mellin Transform). Counting bloom filter method is used to improve detecting process of this method. This method is invariant with rotation (up to 10) and scaling (up to 10).

H. Huang et al. [6] proposed CMFD methods based on SIFT key-point descriptors. In this method, key-points divided into two sets and one set contains one element and another set contains remain of key-points. After getting two sets, there is apply BBF (Best-Bin-First) method and save matching key-points. This process is repeated for all key-points. This method is also worked well in case of rotation and scaling transform.

V. T. Manu at al. [7] proposed a CMFD method based on segmentation and SURF. In this method, simple linear iterative clustering (SLIC) method is used for image segmentation and SURF method is used for extract key-points on the image. After this, each region denoted by the label based on key-points in that region.The similar region on the image finds out by the label and matched key-points within the region.

Christlein et al. [8] carried out a comparison of block-based and key point-based techniques used in this connection they have reached the conclusion that block-based methods enhance the detection performance, while the key-point based techniques reduce the complexity of computation. However, the absence of automatic tampering detection is the main drawbacks of these tow kind of methods.

In this study, most of the papers are used either existing block-based or key point based techniques for detecting copy-move image forgery.To enhance the performance of copy-move image forgery detection, the proposed method combines both block-based and keypoint based method.

The rest of this paper is organized as follows. In section III details of the proposed method is described. Section IV gives the results of the proposed method. Finally, the conclusion is drawn in Section V.

III. Proposed Method

This section describes the proposed copy move image forgery detection scheme. Fig. 2 show the flowchart of the proposed copy-move image forgery detection scheme and it does in four phases.

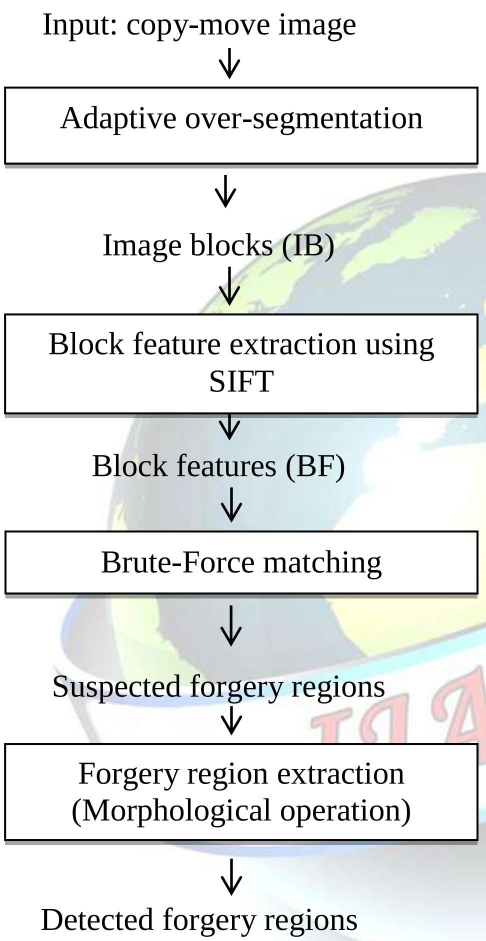

Input: copy-move image
Adaptive over-segmentation
Image blocks (IB)
Block feature extraction using SIFT
Block features (BF)
Brute-Force matching
Suspected forgery regions
Forgery region extraction (Morphological operation)
Detected forgery regions

Fig 2: flowchart of the proposed copy-move image forgery detection scheme.

A. *Phase 1: Adaptive over-segmentation*

The first phase of the copy-move image forgery detection scheme is the adaptive over-segmentation method. This method segment the input copy-move image into non-overlapping and irregular blocks adaptively is called image blocks. The simple linear iterative clustering (SLIC) algorithm is used to segment the input copy-move images into non-overlapping and irregular superpixels.The initial size of the superpixels is essential to get an accurate forgery region. With help of DWT (discrete wavelet transform) technique, obtain the initial size of the superpixels.The DWT techniques analyse the frequency distribution of the input image.

Generally, DWT decomposes the original image into low pass (approximation) and a high pass (detail) component. In the proposed method, 4 levels DWT using Haar wavelet is used. The detailed component contains three coefficient namely vertical coefficient (CV), the horizontal coefficient (CH) and diagonal coefficient (CD). To do this method following steps are needed:

STEP 1: Apply DWT to the input copy-move image to obtain the coefficients of the low-frequency and high-frequency sub-bands using the following equations [10].

$$E_{LF} = |\sum CA_4| \qquad (1)$$

$$E_{HF} = \sum_i (\sum|CH_i| + \sum|CV_i| + \sum|CD_i|).$$

i= 1,2,3,4 (2)

STEP 2: Calculate the percentage of the low-frequency distribution PL F [10].

$$P_{LF} = \frac{E_{LF}}{E_{LF}+E_{HF}} * 100 \qquad (3)$$

STEP 3: Determine the initial size S [10].

$$S = \begin{cases} \sqrt{0.02 * M * N}, & P_{LF} > 50\% \\ \sqrt{0.01 * M * N}, & P_{LF} \leq 50\% \end{cases} \qquad (4)$$

STEP 4: Apply SLIC segmentation algorithm together with the calculated initial size S to segment the input image to obtain the image blocks (IB).

B. *Phase 2 - Block feature extraction*

The second phase of the copy-move image forgery detection is the block feature extraction. In this phase, scale-invariant feature transform (SIFT) is applied in each block to extract the SIFT feature points. The output of this phase is blocked features (BF). SIFT is used to detect and explain the local features in images. Local features means, it describes the image patches (keypoints in the images) of an object and also it represents the texture in an images patch. SIFT technique only detecting stable feature points in an image.

In copy-move image forgery detection, keypoints orientation on original and forgery part are equal and same structure and feature value (descriptor values) of this key point are similar on both parts.The main steps of this phase are,

1. Finds the key points in the image.
2. Draws the small circles on the locations of key points.

3.Then, computes the descriptors from the key points.

C. Phase 3: Brute-force matching

Brute-force matching is one of the simplest feature matching methods in OpenCV-Python. Before applying brute-force matching, a number of segments and labeled values are obtained. After that brute-force matching is applied. This method takes the descriptor of one feature in the first segment and is matched with all other features in the second segment using some distance calculation and the closest one is returned. If any features are matched with one another, copy-move forgery takes place in the image.

In the proposed feature matching method, two thresholds are defined to match the blocks. They are feature point matching threshold (TR_P) and block matching threshold(TR_B).Considering, the match is a good match if the distance from point 'm'(feature point in the first block) is less than the 75% of the distance on point 'n'(feature point in the second block) and appending that point to good. After getting good feature point matching, next step is to obtain the matched blocks by setting block matching threshold. Then labeling the matched feature points in the matched blocks. From this step, got suspected forgery regions.

D. Phase 4: Forgery region extraction (Morphological operation)

In forgery region extraction method, the morphological close operation is used to detect more accurate forgery regions. Morphological operations are based on the image shape. It needs two input: original and structuring element or kernel. The structuring element decides the nature of the operation.The morphological close operation is dilation followed by erosion and it is useful in closing small gaps inside the foreground objects and keeps the shape of the region unchanged.

IV. RESULT AND DISCUSSION

The dataset for the copy-move forgery detection testing is taken from image communication laboratory [12]. The dataset contains 220 images of which 110 are tampered and 110 original images. In the dataset, the copied regions are of classes of living, nature, man-made.

The proposed method is implemented on Raspberry Pi3 model b using Python Language with OpenCV. Python version 2.7 and OpenCV version 3 are used. Window 7 is used as an operating system. OpenCV-Python is a library of Python bindings designed to solve computer vision problems. The libraries Numpy, Open cv2, Matplotlib, Pywt are used for the implementation purpose.

The experimental result of the proposed method is shown below. Fig.3(a) is the original image and fig.3(b) is the forged image. Here one car is copied and pasted into another location in the same image.

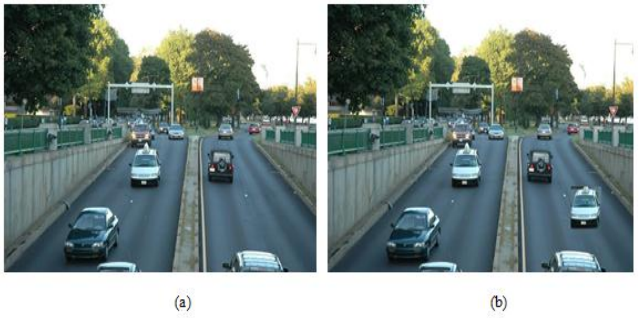
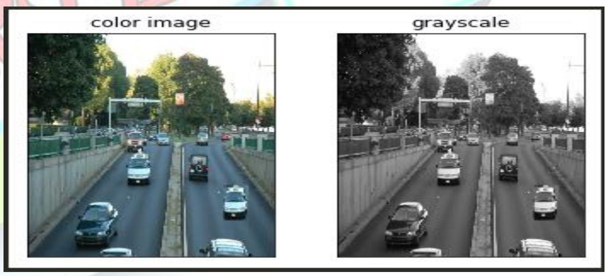


Fig.3. (a) Original image, (b) Forged image

In phase 1, the input copy-move color image is converted into gray scale image. Because DWT only working in grayscale images. It is shown in Fig. 4.



(a) (b)

Fig. 4: (a) Input image-copy-move image (color image), (b) copy-move image (gray scale image)

Fig. 5 shows the DWT result of the test image. The result contained four images. They are labeled as LL (approximation image), LH (horizontal image),HL (vertical image) and HH (diagonal image). From this step, got the initial size of the superpixels S= 56

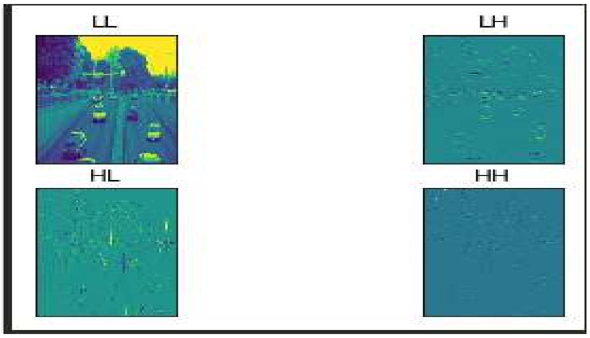


Fig. 5: DWT result of the test image.

After getting the DWT result, applied the SLIC segmentation algorithm with a calculated initial size *S*. The image was segmented and obtained image blocks. The result is shown in Fig. 6.

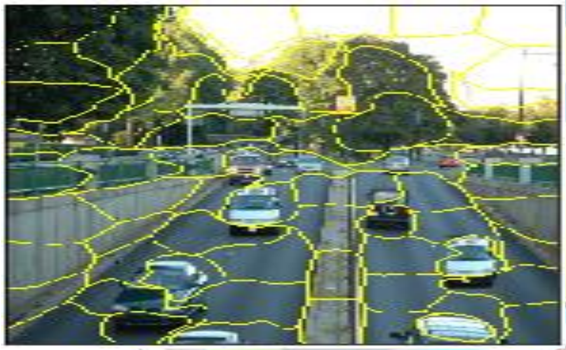


Fig. 6: The result of phase 1(Image blocks).

The Fig.7. shows the output of block feature extraction using SIFT.

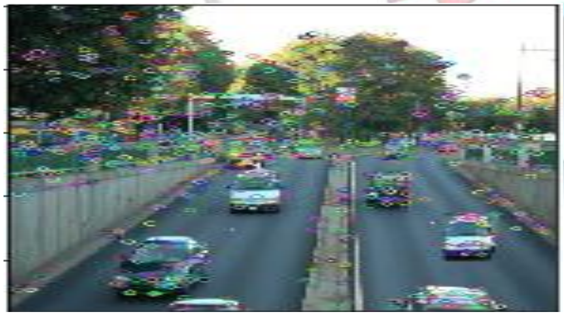


Fig. 7: The result of phase 2(Block features).

Fig.8 (a) is the output of brute-force matching, i.e. suspected forgery regions and Fig.8 (b) is the output of the morphological operation. From this step got the accurate forgery regions.

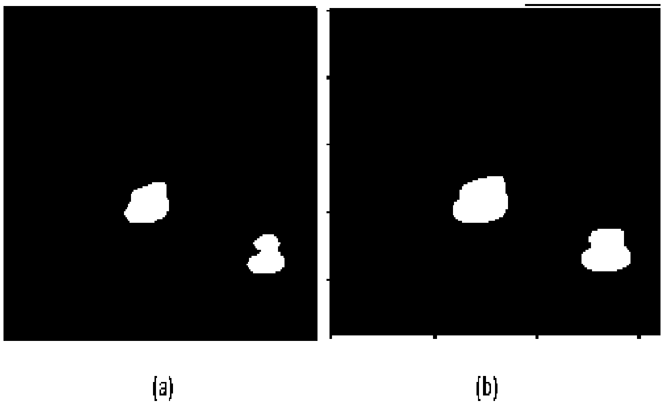


Fig.8: (a) Result of phase 3(suspected forgery regions), (b) Result of phase 4 (detected forgery regions)

To get an accurate result, the input image was resized. So the size of the input image is 480*320 and number of keypoints present in the image are 1048. The block matching and feature point matching threshold is 8 and 0.75 respectively.

VI. Conclusion

The copy-move forgery detection is a big challenge to detect. Copy-move image detection based on adaptive over-segmentation and brute-force matching method is proposed in this paper. The main advantage of this method is that it combines block-based and keypoint based methods. So it enhances the performance of the copy -move image forgery detection and overcomes the limitations of existing block-based methods. Experimental result shows that proposed method is effectively detected the copy-move foregry with minimum false match. As a future study, this proposed method can be applied to other types of forgery such as image splicing, image enhancement and also it is applied in forged videos and audios.

Acknowledgment

I wish to record my indebtedness and thankfulness to all those who helped me to prepare this paper titled Copy-move image forgery detection using adaptive over-segmentation and brute-force matching and present it in a satisfactory way. First I thank God Almighty for her providence and for being the guiding light throughout the project.

I want to start expressing my thanks to my guide Assistant Professor Ms. Binet Rose Devassy, Dept. of Electronics and Communication Engineering for her valuable advice and guidance towards this work. I received motivation, encouragement and hold up from her during the course of work.

REFERENCES

[1]. J. Fridrich, D. Soukal, and J. Lukáš, “Detection of copy-move forgery in digital images,” in Proc. Digit. Forensic Res. Workshop, Cleveland, Aug. 2003.

[2]. N. D. Wandji et, “detection of copy-move forgery in digital images based on DCT”, *The Scientific world Journal, Volume* 2014.

[3]. Khan, S., kulkarni, A, “Detection of copy-move forgery using multi resolution characteristic of discrete wavelet transform”, *International conference on workshop on emerging treads in technology*. ICWET11, New York, NY, USA, 2011, pp. 127-131.

[4]. G .Muhammad, M. Hussain, and G. Bebis” Passive copy move image forgery detection using undecimated dyadic wavelet transform”, *Digital Investigation*, vol. 9, pp. 49-57. 2012.

[5]. S. Bayram, H. T. Sencar, and N. Memon, “An efficient and robust method for detecting copy-move forgery”, in Acoustics, Speech and Signal Processing,, ICASSP ,*IEEE International Conference* on, 2009, pp. 1053-1056.

[6]. H. Huang,W. Guo and Y. Zhang, “Detection of copy-move forgery in digital images using SIFT algorithm”, *in Pacific-Asia Workshop on Computational intelligence and industrial application*, IEEE, 2008, 2, pp. 272-276.

[7]. VT Manu, BM Mehtre “Detection of Copy-Move Forgery in Images Using Segmentation and SURF”, *Advances in Signal Processing and Intelligent Recognition Systems*, 2016, Springer.

[8]. V. Christlein, C. Riess, J. Jordan, C. Riess, and E. Angelopoulou,“An evaluation of popular copy-move forgery detection approaches,”*IEEE Trans. Inf. Forensics Security*, vol. 7, no. 6, pp. 1841–1854, Dec.2012.

[9]. X. Bo, W. Junwen, L. Guangjie, and D. Yuewei, “Image copy-move forgery detection based on SURF,” in *Proc. Int. Conf. Multimedia Inf. Netw. Secur. (MINES)*, Nov. 2010, pp. 889–892.

[10]. Pun, Chi-Man, Xiao-Chen Yuan, and Xiu-Li Bi. "Image forgery detection using adaptive over segmentation and feature point matching." *IEEE Transactions on Information Forensics and Security 10.8 (2015): 1705-1716*.

[11]. Shivakumar, B. L., and Lt Dr S. Santhosh Baboo. "Detecting copy-move forgery in digital images: a survey and analysis of current methods." *Global Journal of Computer Science and Technology* (2010).

[12]. Dataset, MICC-F220 [accessed 2018 May 15]. http://lci.micc.unifi.it/labd/cmfd/MICC-F220.zip

BIOGRAPHY

First Author

4th Semester, M. Tech, Embedded Systems, Department of Electronics and Communication Engineering, Sahrdaya College of Engineering and Technology, Kodakara, Thrissur, India

Second Author

Assistant Professor , Project guide, Department of Electronics and Communication Engineering, Sahrdaya College of Engineering and Technology, Kodakara, Thrissur, Completed M.Tech in Applied Electronics.12 years of teaching experience.