A Novel Detection Algorithm for Image Copy Move Forgery

Jen-Chun Lee
Department of Electrical Engineering,
Chinese Naval Academyine
Kaohsiung, Taiwan
i923002@gmail.com

Chien-Ping Chang
Department of Computer Science and Information Engineering, Chien Hsin University of Science and Technology, Jhongli, Taiwan
chang.chienping@gmail.com

***Abstract*—With the increasing popularity of digital media and the ubiquitous availability of media editing software, innocuous multimedia are easily tampered for malicious purposes. Therefore, it is necessary to have reliable and efficient methods to detect copy-move forgery for applications in law enforcement, forensics, etc. In this paper, based on Histogram of Orientated Gradients, we propose a blind forensics approach for the detection of copy move forgery. Experimental results and analysis show that our proposed method can effectively detect multiple copy-move forgery and precisely locate the duplicated regions, even when an image was distorted by translation, rotation, blurring, brightness change, and color reduction operations.**

Keywords—copy-move forgery; digital image forensics; histogram of orientated gradients; duplicated region detection.

I. INTRODUCTION

In today's digital age, sometimes seeing is no longer believing, since our modern life is full of digital images and (maliciously) tampering these digital images is easy and simple by using digital image processing tools which are widely available (e.g. Photoshop). Since digital images play a crucial role and have an important impact, the authenticity of images is significant in our social and daily life. How much we can believe in seeing is becoming an intractable problem [1]. In general, existing image forgery detection techniques are described as active [2-4] and passive (blind) [5-6] methods. Active methods are usually related to digital signature and watermarking, which have been used in the past to detect image manipulations and forgeries. But the significant drawback in digital signature or watermarking technology is that the data must be preprocessed, such as embedding watermark in the images.In contrast to active methods, passive methods are usually based on supervised learning by extracting certain features to distinguish the original images from tampered ones. The practicality and wider applicability of passive methods make them a hot research topic.

Copy-move is the most common operation for generating a digital image forgery, defined as a part of the image itself is copied and pasted into another part of the same image to conceal an important object or sometimes to show more than one object. Nowadays, the vide availability of image processing software makes the creation of a tampered image using copy-move operation particularly easy. The artificial region introduced by copy-move forgery results in almost imperceptible by human eyes. Therefore, the detection of copy-move forgery is a preliminary but desirable study for image forensics. In this paper, we focus on this topic. We present an effective and robust image copy-move forgery detection algorithm based on Histogram of Orientated Gradients (HOG) [7]. We conducted rigorous experiments using images modified using highly convincing techniques to demonstrate the robustness of the proposed method in dealing with multiple copy-move forgeries. Compared with other methods, the main advantages of our method can be summarized as:

- The proposed technique is able to precisely locate duplicated regions without being affected by common post-processing attacks, such as image translation, rotation, blurring, brightness change, and color reduction operations.
- The dimension of the feature vector is lower that can be used to reduce the computation complexity.

The remainder of the paper is organized as follows. Section 2 introduces the Histogram of Orientated Gradients, while Section 3 presents the proposed method for detecting copy-move forgery. In Section 4, we present the results of experiments designed to evaluate the performance of the proposed method in detection accuracy and computational complexity. Conclusions are presented in Section 5.

II. HISTOGRAM OF ORIENTATED GRADIENTS

The HOG descriptor [7] has gained traction in the vision community, and particularly in object recognition, for several reasons. First, it is a vector-space model, where perceptual similarity is approximated by euclidan (or cosine) distance between two HOG vectors. This means that many off-the-shelf learning and database algorithms can work directly on HOG representations. Second, it appears to be a reasonably good model of perceptual similarity: it uses intensity gradients rather than intensity directly, which means that the responses of edges are localized; it is sensitive to local but not global contrast due to its normalization scheme; it can handle minor misalignment due to the bilinear interpolation between HOG cells; and many other reasons also apply. Third, it is very fast to compute: computing a HOG pyramid for a 500-by-500 image can take less than 2 seconds on a single core, and firing a sliding-window template at all positions and scales can happen equally fast via fast fourier-transform convolution.

For copy-move forgery detection, we can only rely on the shape and texture of the tampered images, so HOG feature is more appropriate. The HOG feature is closely related to the scale-invariant feature transform (SIFT) [8-9] feature descriptor, but while SIFT is intended to be run at a sparse set of interest points, HOG is intended to be run over a dense grid. We implemented the HOG feature as it was described in [7], where it was used in the context of pedestrian detection. First, the 2D gradient of the image is computed using a vertical and horizontal [-1; 0; 1] filter. Then, the image is divided into *M* cells of *N*N* pixels. A histogram with *H* bins is computed and normalized given the weighted gradient at each pixel, for each of the cells. The concatenation of the histograms from each cell yields a *H*M* length feature vector for the image.

III. Proposed scheme

The most important function of an algorithm for the detection of copy-move image forgery is determining whether a given image contains duplicated regions. Since the different post-processing operations, including rotation, blur degradation and contrast changes, etc., of copied regions are unknown, if we compare every possible pairs pixel by pixel, the computational complexity will be very higher, none can endure that. Obviously, it is more practical to divide the suspicious image into blocks for detecting the duplicated regions.

In order to take an efficient detection, some appropriate and robust features must be extracted from the blocks. Therefore, good features are able to represent the entire block, provide robustness against common post-processing operations, and reduce the computational complexity of the detection algorithm.

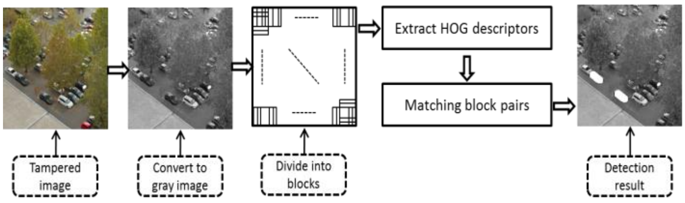

Fig. 1. Diagram of detection algorithm

The diagram of the proposed scheme is shown in Fig.1. The copy-move image forgery detection algorithm includes several steps, the details of which are explained separately in the following.

A. Forgery image pre-processing

At the beginning of the method, the RGB image *C* is transferred into a grayscale image *I*, by the following formula,

$$I = 0.299R + 0.587G + 0.114B \quad (1)$$

where R, G, B are red, green, and blue channels of the color image *C*, *I* is its l*uminance component.*

B. Tampered Image is Divided into Fixed-Size Overlapping Blocks

In order to find out the forged regions, the image is usually divided into overlapping sub-blocks. Therefore, square blocks are used in the proposed method. We first divide the forgery grayscale image *I* of *M*N* into overlapped sub-blocks of *L*L* to calculate HOG descriptors. Consequently, the image is divided into *(M-L+1)*(M-L+1)* overlap blocks in all.

C. Each Block used the HOG to Obtain HOG Descriptors with the Same Size

HOG is applied to each block. Here, we consider 4 bins for the local histogram. The histogram channels are evenly spread over 0 to 180 degrees, so each histogram bin corresponds to a 45 degree orientation interval. The obtained cell histograms are then combined into a descriptor vector of each block. Therefore, we can obtain four features to represent each block. For an forgery image of size of *M*N*, matrix *A* would have *(M-L+1)*(M-L+1)* rows and 4 columns, where 4 is the number of features.

D. Match these HOG Features each other

In order to reduce the time of matching, the similar feature vectors will be stored into the neighbor rows by lexicographical sorting. Thus the detection can be done by lexicographically sorting the rows of *A* matrix, so that the features of the duplicated block pairs will come successively. Block matching is to find out the corresponding blocks, and to detect the forged regions correctly. In the proposed scheme, we search for the corresponding blocks by estimating the Euclidean distances of the feature vectors.

E. Post-processing of the detection result

The forged regions can be determined, which is achieved by marking the copied region and the tampered region and remove the isolated blocks. In general, all the detected blocks including the original blocks and forgery blocks are marked to generate the final detection result. Fig. 2(c) shows an example of the proposed method of marking.

Normally, there are some falsely detected blocks marked on the initial detection map, and these false blocks should be removed. To this end, we design a detector to remove them. The proposed detector operates as follows. Suppose that the marked image is divided into *n* non-overlap blocks with the size of 16*16. If the number of “white” pixels is less than 64 in the block, all pixels of the block are regarded as original image. Otherwise, keep the number of the white pixels and do nothing. After detecting, some small isolated false matches can be removed. Fig. 2(d) shows the detection result after the proposed detector operation.

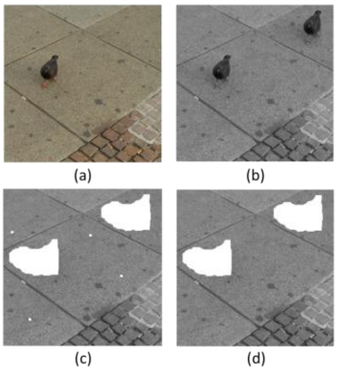

Fig. 2. Post-processing of detection results. (a)Original image, (b) tampered image, (c) initial detection result, and (d) final detection map.

IV. EXPERIMENT RESULTS AND DISCUSSION

This section describes the results obtained from experiments performed using the proposed algorithm. In our experiments, the proposed method is evaluated in two publicly available databases that are designed for image forgery detection. The first one was obtained from the CoMoFoD database [10]. All images are recorded by a Canon EOS 7D camera and stored in CR2 (Canon RAW version 2) format as minimally processed data. These forgery images consist of 200 png images with a resolution of 512*512 in small image category. Acquisition was performed under various conditions outside, such as a natural setting, among buildings, and overlooking the city. Besides, the second dataset are several color PNG images released by the Image Manipulation Dataset [11]. They all have high resolution images (about 800*500 to 3200*2400 pixels) included 48 base images, separate snippets from these images, and a software framework for creating ground truth data. These images had been manipulated using copy-move forgery with other processes, such as translation, rotation, blurring, and color reduction. Figure 3 presents the forged images used in the experiments. All experiments were performed on a personal computer with 2.1GHz CPU, 4GB memory, running Matlab R2010b. The experimental results are detailed in the following sections, according to the various processes used to manipulate the forged regions.

A. Performance evaluation

To illustrate the performance of the proposed algorithm, we referenced two evaluation criteria, the correct detection ratio (CDR) and the false detection ratio (FDR), defined as follows:

$$\mathrm{CDR} = (|\mathrm{C} + \tilde{\mathrm{C}}| + |\mathrm{F} + \tilde{\mathrm{F}}|)/(|\mathrm{C}| + |\mathrm{F}|) \qquad (2)$$

$$\mathrm{FDR} =(|\tilde{C} - C|+|\tilde{F} - F|)/(|\tilde{\mathrm{C}}|+|\tilde{F}|) \qquad (3)$$

where C is the copy region, F is the tampered region, while $\tilde{C}$ and $\tilde{F}$ are the tampered copy region and the detected tampered region, respectively. | | refers to the area of the region, ∩ refers to the intersection of two regions, and – refers to the difference between two regions. CDR indicates the performance of the algorithm in correctly locating the pixels of copy-move regions in the tampered image, while FDR reflects the percentage of pixels that are not contained in the duplicated region but are nevertheless included by the implemented method. The closer CDR is to 1 and FDR is to 0, the more precise the method.

B. Effectiveness and accuracy test

In the following experiment, we select some color images with the size of 512*512 pixels from the first dataset to test the effectiveness of our algorithm. All the doctored images in this experiment are without any post-processing operation and the corresponding detection results are illustrated in Figs. 3. The top row shows the tampered images, and the bottom gives the detection results. Owing to space constrains, just a part of the experimental results are given here.

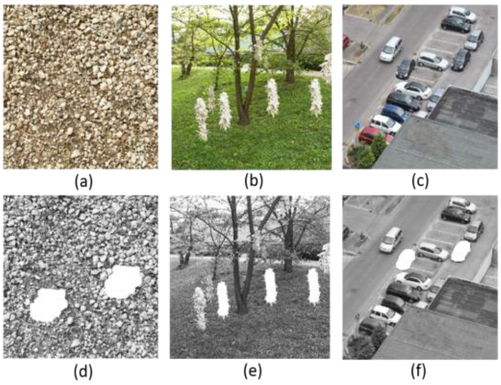

Fig.3. An example to detect multiple copy-move forgery image. (a)-(c) The tampered images, and (d)-(f) the detection results of tampered images.

Fig. 3 shows that the accuracy rate CDR is generally greater than 0.95 and the false positive rate FDR equals to 0, that is, our algorithm can locate the tampered regions quite precisely. In addition, Fig. 3 also indicates that our algorithm can find the duplicated regions precisely when all the duplicated regions are non-regular and meaning, even though there are extremely similar scene or flat regions in the image, such as large areas of sand or leaf.

C. Analysis of robustness against post-processing attacks

The ability to resist post-processing attacks is fundamental to copy-move detection methods. There are many different types of post-processing attacks that can be applied to forged images with the aim of hiding tampering traces. Most common post-processing attacks are image rotation, blurring, adjustment of brightness, and color reduction. For each color channel in the forged image, the number of intensity levels was reduced from 256 to 32, 64, or 128. Images obtained by reducing the number of intensity levels have nearly imperceptible degradations compared to the original image with 256 intensity levels per channel. For brightness change, changing the brightness of the image was obtained by mapping the intensity values of the original image that were between lower and upper bound to interval [0, 1].

The experiments are also conducted on the first dataset to test the robustness of our algorithm. In implementation, the detection of duplications with block sizes of 16*16 is employed. The CDR and the FDR are listed in Table 1.

TABLE 1 CORRECT DETECTION RATIO AND FALSE DETECTION RATIO ON COMOFOD DATABASES.

Attacks		CDR	FDR
Image rotation		0.814	0.232
Images blurred (filter size)	3*3	0.994	0.003
	5*5	0.976	0.012
	7*7	0.946	0.092
color reduction (levels)	32	0.981	0.041
	64	0.986	0.029
	128	0.992	0.014
adjustment of brightness (ranges)	[0.01, 0.95]	0.995	0.006
	[0.01, 0.9]	0.992	0.011
	[0.01, 0.8]	0.983	0.025

It is known from the Table 1 that the correct detection ratios are very high on blurring, color reduction and adjustment of brightness. Detection results using tampered images that were distorted by color reduction are presented in Table 1. These results show that the proposed method works better when dealing with colors of a higher bit depth. In addition, the proposed method clearly provides high detection performance when the images are distorted using 3*3 and 5*5 averaging filters, but not as well when a 7*7 averaging filter was employed. According to the various brightness of image, the CDR/FDR is also presented in Table 2. As the detection results show, even in the range of [0.01, 0.8], the detection performance of the proposed method is still reliable. It also demonstrates that the proposed algorithm is highly robust against changes in image brightness.

However, the proposed scheme can obtain the higher false detection ratio on rotation. The main reason is that the HOG descriptors differ between the original regions and the rotated region, which can reduce the effectiveness of the algorithm. Nonetheless, the proposed method still provides good detection performance for small rotations.

V. Conclusions

Copy-move is a common method to create forgery images. It works without any digital watermarks or signatures information. This paper proposes an effective method for detecting duplicated regions based on the HOG. Compared with previous works, our approach used less features to represent each block. Experiment results demonstrate that the proposed algorithm could not only endure the multiple copy-move forgery, but also robust against actions aimed at concealing forgery, including image slight rotation, color reduction, blurring, adjustment of brightness, and with low computational complexity. This study therefore makes a valuable contribution to the field of multimedia forensics.

References

[1] T. Gloe, M. Kirchner, A. Winkler, R. Behme, "Can we trust digital image forensics?" In: Proceedings of the 15th international conference on Multimedia. 2007, pp. 78-86.

[2] C. Rey, J. L. Dugelay, "A survey of watermarking algorithms for image authentication", EURASIP J. Appl. Signal Process. Vol. 1, 2002, pp. 613-621.

[3] N. M. Yeung, "Digital watermarking introduction", CACM. Vol. 41, 1998, pp. 31-33.

[4] J. Fridrich, "Methods for tamper detection in digital images", In: Proceedings of the ACM Workshop on Multimedia and Security. 1999, pp. 19-23.

[5] J. Fridrich, D. Soukal, and J. Lukas, "Detection of copy–move forgery in digital images", In Proceedings of Digital Forensic Research Workshop. 2003, pp. 19-23.

[6] W. Luo, Z. Qu, F. Pan, J. Huang, "A survey of passive technology for digital image forensics", In: Front. Comput. Sciences of China, vol. 1, 2009, pp. 308-322.

[7] N. Dalal, B. Triggs, "Histograms of oriented gradients for human detection", Computer Vision and Pattern Recognition, 2005, pp. 20–25.

[8] X. Pan, S. Lyu, "Region duplication detection using image feature matching", IEEE Trans. Inf. Forensics Secur, vol. 4, 2010, pp. 857–867.

[9] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra, "A SIFT-based forensic method for copy-move attack detection and transformation recovery", IEEE Trans. Inf. Forensics Secur, vol. 6, 2011, pp. 1099–1110.

[10] CoMoFoD database, available at: http://www.vcl.fer.hr/comofod.

[11] Image Manipulation Dataset, available at: http://www5.cs.fau.de/research/data/image-manipulation/