2012 International Conference on Image, Vision and Computing (ICIVC 2012)
IPCSIT vol. 50 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V50.2

Detection of Copy-Move Forgery by Clustering Technique

Nattapol Chaitawittanun [+]

Faculty of Agriculture Technology, Phetchabun Rajabhat University, Thailand

Abstract. Due to rapid advancement of powerful image processing software, digital images are easy to manipulate and modify by ordinary people. Lots of digital image are edited for a specific purpose and more difficult to distinguish form their originality. We propose a clustering method to detect a copy-move image forgery of JPEG, BMP and TIFF. The process starts with reducing the color of the photos. Then we use the clustering technique to divide information of measuring data by Hausdorff Distance. The result shows that the purposed methods is capable of inspecting the image file and correctly identify the forgery.

Keywords: image forgery, copy-move, digital image.

1. Introduction

Photographing is popular and interesting activities which can be done everywhere. The major equipment of taking a photo is a digital camera which is convenient, inexpensive and easy to use. In addition, it can save the images and instantly display them [1]. That is the reason why a photo from digital cameras is popularly used in many medias, for examples, newspapers, magazines, or social network and including a crime scene evidence [2]. These photos may contain important events and be used as evidence. Nowadays there is a doubt that the pictures have been changed or not [3]. Retouching photos is now harmfully cultural competence spreading all over the internet. Celebrities, actors, politician, or even civilians can be a victim of retouching as well [4]. Tampering images might lead harmfully to misunderstanding or misleading the truth which the suspect reputation of people in the photos.

2. Related Work

There are 2 types of digital image forgery; Copy-move and Image Slicing. Copy-move takes some parts of the same picture and paste onto another part as shown in Figure 1.

(a) (b)

Fig. 1: Copy-move (a) original (b) fake picture – mouse pad was covered.

[+] Corresponding author. Tel.: + 6656717100; fax: +6656717151.
E-mail address: nattapol_ctwtn@hotmail.com.

Image Splicing takes some parts from other picture and paste on the original picture to create a new photo and change the look of the original picture [7] as shown in Figure 2.

Fig. 2: Image Splicing

They are two types to examine faked pictures: active and passive [5]. Active process uses digital watermark to examine the fake pictures as shown in Figure 3. Hiding information into the picture before using can be used to examine the history of that picture [6]. Nevertheless, this technique also has limitation such as the user has to know how to embed the secret information onto the picture. This technique is inappropriate and difficult to inspect the picture.

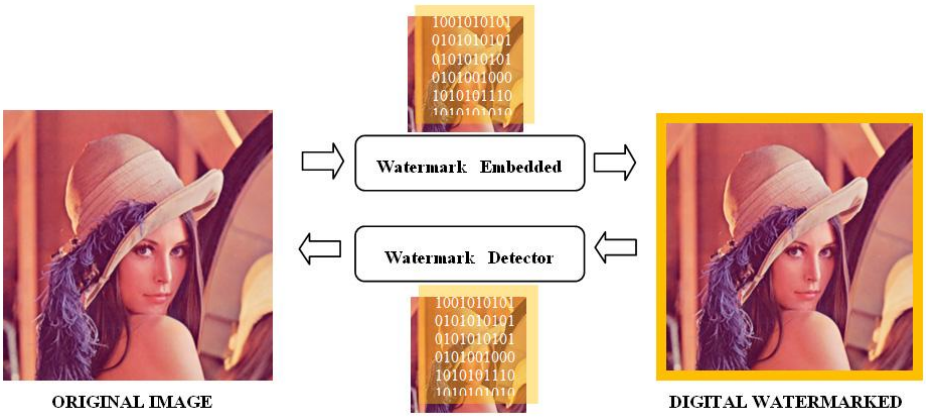

Fig. 3: Digital Watermark Process

In contrast, the passive technique does not embed information into a picture. This technique is appropriate and easier. Many researchers have focused on passive image forgery detection. Fridrich [9] has developed techniques of overlapping block and DCT which extract feature of the images, then compare the similarity of block. Popsecu and Farid [10] use PCA to reduce the dimension of the block. Farid and Bravo [8] suggest the idea of using vision of human being to examine shadow of objects, reflection of objects and distortion of objects. The image forgery detection which has developed by most researchers are feature extraction by using various techniques such as DCT and PCA.

3. Proposed Method

Copy-move tampering is done by copying a region of the image and pasting it on another place in the same image. When a region is copied and pasted to another place, it will keep some of its underling features that can be used to identify tampering. The feature used here is the color pattern.

Specifically, we study the color present in an image where one of its regions is replicated, which has almost the same color pattern for both the copied and pasted parts. The general framework of our process is as shown in Figure 4:

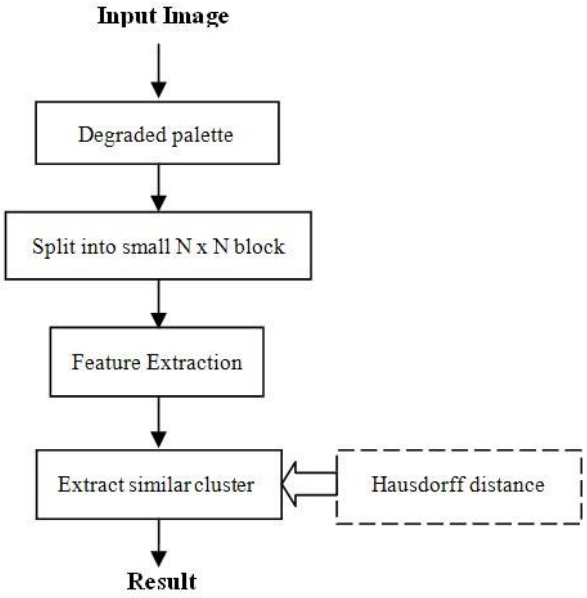

Fig. 4: The process of copy-move detection

Step 1: Decreasing image details

We first blur the image *f* for eliminate noise and detail, and then degrade the color of image.

Step 2: Splitting image into blocks NxN

Split the image *f*, of size m_f x n_f, which is tiled as blocks of pixels selected by sliding, pixel by pixel, from the top-left corner to the bottom-right corner.

Step 3: Extract colors of splitting blocks and cluster data

We extract characteristic color with every block and categorize data of the image.

Step 4: Clustering the similarity of colors by Hausdorff distance

Finding the similarity data is the process to identify a duplicate position by measuring distance of information group by Hausdorff distance. Given two finite point sets $A=\{a_1,\ldots,a_m\}$ and $B=\{b_1,\ldots,b_n\}$, the Hausdorff distance is defined as

$$H(A,B) = \max(h(A,B),h(B,A)) \quad (1)$$

When

$$h(A,B) = \max_{a\in A} \min_{b\in B} \|a-b\| \quad (2)$$

and || || is some underlying norm on the points of *A* and *B*. The function *h(A,B)* is called the directed Hausdorff distance from *A* to *B*. It identifies the point a ∈*A* that is farthest from any point of *B* and measures the distance from a to its nearest neighbor in *B*. The function *h(A,B)* in effect ranks each point of A based on its distance to the nearest point of *B* and then uses the largest ranked such point as the distance.

4. Experimental Result

We tested the performance of our proposed method on JPEG, TIFF and BMP which have each of photo files are 100 images. All images are of 512x384 pixels. The photo was edited by copy-move technique as shown in Figure 5.

(a) (b) (c)

(d) (e) (f)

Fig. 5: (a - c) original image (d - f) tampered image by copy-move technique

Figs. 5(d)-5(f) show an example of a copy-move forgery. Fig 5(d) shows the modification of image is copied and pasted balloon in the image. Fig 5(e) shows weed picture is copied and pasted flower in the image. Fig 5(f) shows turtle picture is copied the upper turtle and pasted in the lower part.

The results can be visually inspected in Figs. 6(a)-6(c). The red areas depict the duplicated regions that were successfully detected. The measure of accuracy is summarized in Table 1.

(a) (b) (c)

Fig. 6: Test images (a), (b), (c) was the result of the detection

The result of the detection shows the accuracy of Copy-move technique of JPEG file which can be identified the duplicate position correctly at 64.36%. TIFF and BMP files show the accuracy at 62.54% and 60.98 %. Average detection time of BMP file spent 120 seconds on a machine having Intel Core2 Duo 2.1 GHz CPU and 4 GB RAM. In addition, JPEG and TIFF spent 150 and 180 seconds.

Table. 1: Results obtained from the example forgeries.

Image Type	**Accuracy Rate (%)**
JPEG	64.36
TIFF	62.54
BMP	60.98

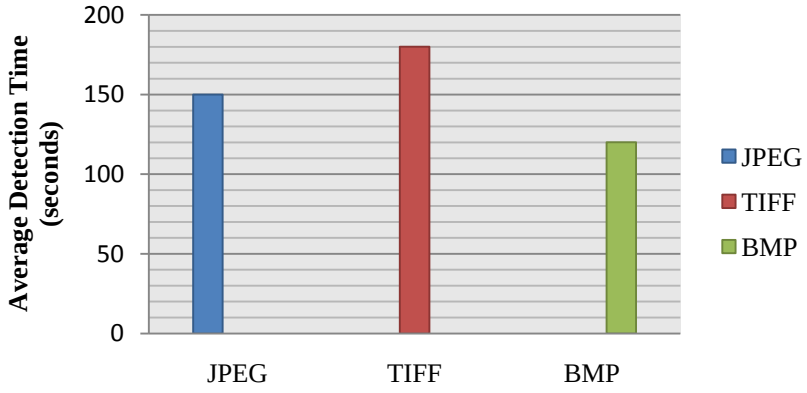

Fig. 7: Average detection time of each file format

5. Conclusion

Digital image forgery detection is an interesting research topic in forensics science. An effective detection of specific copy-paste type of image tampering has been proposed in this paper. In this paper, we show that our process is useful to identify the copy-paste region. The proposed method can detect duplicated region from all sample images. In the future, we would like to detect other types of image files and enhance performance of the proposed detection.

6. References

[1] L. Weiqi, Q. Zhenhua, P. Feng, H. Jiwu. A survey of passive technology for digital image forensics. Springer Science. Frontiers of computer science in China.2007, vol. 1, no. 2, pp. 166-179.

[2] M.K. Johnsos. Light and optical tools for image forensics. Ph.D. Thesis, Dartmouth College, Computer Science Deptl., Germany. 2007.

[3] D.A. Brugioni. Photo fakery: the history and techniques of photographic deception and manipulation. Virginia :Brassey's publishers, 1999.

[4] Z. Lint, R. Wang, X. Tang, H.Y. Shum. Detecting Doctored images using camera response normality and consistency. in Proc. Computer Vision and Pattern Recognition.2005, vol. 1, no. 43-48.

[5] B. Mahdian and S. Saic. A bibliography on blind methods for identifying image forgery. ELSEVIER. Signal Processing: Image Communication.2010, vol. 25, Issue 6, pp. 389-399.

[6] I. Cox, M. Miller, J. Bloom. Digital Watermarking : Principles & Practice. Morgan Kaufmann, 2001.

[7] Y.F. Hsu and S.F. Chang. Detecting Image Splicing using Geometry Invariants and Camera Characteristics Consistency. IEEE International Conference. Multimedia and Expo. 2006, pp. 549-552, July 9-12.

[8] H. Farid and M. Bravo. Image forensic analyses that elude the human visual system. SPIE Symposium on Electronic Imaging, San Jose, 2010.

[9] J. Fridrich, D. Soukal, J. Lukas. Detection of Copy-Move Forgery in Digital Images. in Proc. Digital Forensic Research Workshop, Cleveland, OH, Aug, 2003.

[10] A. Popescu and H. Farid. Exposing digital forgeries in color filter array interpolated images. IEEE Trans. Signal Processing.2005, vol. 53, no.10, pp. 3948–3959.