DETECTING COPY-PASTE FORGERY OF JPEG IMAGE VIA BLOCK ARTIFACT GRID EXTRACTION

Weihai Li [1], *Yuan Yuan* [2], *and Nenghai Yu* [1]

[1] MOE-Microsoft Key Laboratory of Multimedia Computing and Communication,
University of Science and Technology of China, Hefei 230027, China
{whli, yhn}@ustc.edu.cn

[2] School of Engineering and Applied Science, Aston University,
Birmingham B4 7ET, United Kingdom
yuany1@aston.ac.uk

ABSTRACT

JPEG is probably the most widely used image compression standard in taking digital pictures, e.g., in most digital cameras. As a result, synthetic images by the trick operation of *copy-paste* are usually from and to JPEG images. Realizing that it might be impossible to find a method that is universal for all kinds of forgeries, we proposed a novel blind approach to detect *copy-paste* trail in doctored JPEG images and meanwhile locate the doctored area. The approach works well even when a JPEG image is truncated or multi-compressed, by extract the DCT block artifact grid and detect mismatch of the grid. Experiments well demonstrate the effectiveness of the proposed approach.

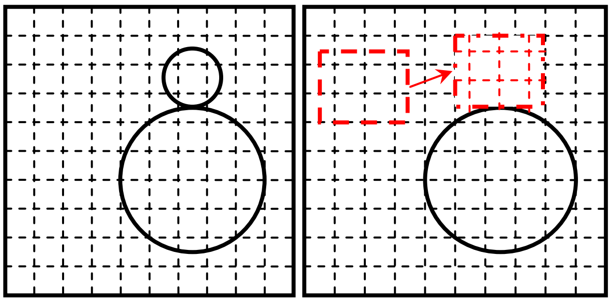
1. INTRODUCTION

Today, powerful image processing softwares, such as the Photoshop, allow people to modify photos conveniently and unperceivedly. It is now a big challenge to authenticate images.

There are two kinds of techniques for image forensics: one is active protection, and the other is passive detection. Digital watermarking [1] and signature are two main active protection techniques, in which something are embedded into images when they are obtained.

If special information cannot be extracted from image, then we know the image was tampered. Unfortunately, most present imaging devices do not contain any watermarking or signature module, and that astricts the application of active protection. The passive detection is to check the integrity of a single image, including techniques of nature image statistics analysis [2], modification trails detection [2,3], and consistency verification between image and imaging device [4].

However, most authentication algorithms require pending image to be uncompressed and high quality. As for the widely used JPEG format, only two kinds of algorithms were proposed. One is used to detect double JPEG compression. It is already noticed [2] that periodic property caused by double quantization appears in the histogram of DCT coefficient. An algorithm [5] was proposed to detect doctored JPEG images and further locate the doctored parts by examine the double quantization effect hidden among the DCT coefficients. A serious matter is that the detection will fail if the image is thrice compressed.



(a) Original image (b) Doctored image

Figure 1. Example of copy-paste forgery

The other algorithm [6] is to verify the uniformity of block artifact (BA), which is defined as DCT quantification errors. However, the evaluation of BA is not so accurate, and BA itself waves within an image. This algorithm may fail if the levels of BA between doctored parts and undoctored parts can not be distinguished.

In this paper, a new JPEG image forensics approach is proposed to detect copy-paste forgery based on the check of block artifact grid mismatch. A DCT grid is the horizontal lines and the vertical lines that partition an image into blocks. And a block artifact grid (BAG) is the grid embedded in an image where block artifact appears. The DCT grid and BAG match together in undoctored images. When an image slice is moved, the BAG within it also moves.

To make image visual unperceived after copy-paste forgery, the BAG usually can not be cared since the slice must be placed in a certain place. Figure 1 shows a simple example of copy-paste forgery. As shown in this example, the forgery is to copy a blank area and paste it to cover the small circle. When this operation is done, the BAG in the bland area is copied and pasted together. It can be noticed that the gird in the pasted area is mismatch to neighbor grid.

Thus, our forensics approach is to locate the BAG firstly, and then check whether the BAG mismatches or not. Once a BAG mismatch is affirmed, then the image can be authenticated as doctored.

In our approach, the accurate level of blocking artifacts is not important as discussed in [7,8]. What we care is where the block artifact locates. Following these principles, a simple algorithm is designed to mark the BAG in section 2. In section 3, the BAG marking algorithm is applied to authenticate images. Experiment results demonstrate that this approach can identify copy-paste forgery efficiently.

From the above analysis, it should be mentioned that our approach works even if the copied area came from another image, if only the image is also JPEG compressed. This condition is often true since most images are stored in JPEG format. Resistibility to image truncation is another virtue of our algorithm, while other algorithms will fail.

2. BAG EXTRACTION

As we all know that high frequency AC coefficients of a DCT block are usually zero after quantification when compressing. If a complete DCT block is located, high frequency AC coefficients of the block are usually zeros. Otherwise some values can be found since BAG exists, which can be treated as an additive defective step signal. Even when the texture is complex and the high frequency AC coefficients are not zero, the right block location will bring smaller high frequency AC coefficients, because there is no BAG impact.

Then, the valley of high frequency AC coefficients values corresponds to the BAG location.

As a simplification, let's discuss a 1-D signal sequence firstly.

To locate the BAG, a measure, called as local effect (LE), is defined with the absolute ratio of the eighth DCT coefficient to the first DCT coefficient within a window of 8 signals, as shown in formula (1)

$$LE_i = \left|\frac{S_7}{S_0}\right| \qquad (1)$$

Here, LE_i is the local effect of window from the ith signal to the (i+7)th signal, S_j (j=0 or 7) is the (j+1)th DCT coefficient of signal $s_i\ s_{i+1}, \ldots, s_{i+7}$. S_0 is used to normalize the illuminant.

$$S_j = \sqrt{\frac{\alpha_j}{8}}\sum_{n=0}^{7} s_{i+n}\cos\frac{j(2n+1)\pi}{16} = 0 \ \ (j = 0,1,\cdots 7) \qquad (2)$$

where

$$\alpha_j = \begin{cases} 2 & j = 0 \\ 1 & j \neq 0 \end{cases} \qquad (3)$$

Slide the window along the signal sequence, a local effect sequence can be calculated. A sample signal sequence and its local effect are shown in figure 2, where the signals are originally blocked by 8. It is clear that minimum LE values appear at the block edge. It can also be noticed that the peaks of LE correspond strongly to the strength of block artifacts, but weakly to the strength of signals.

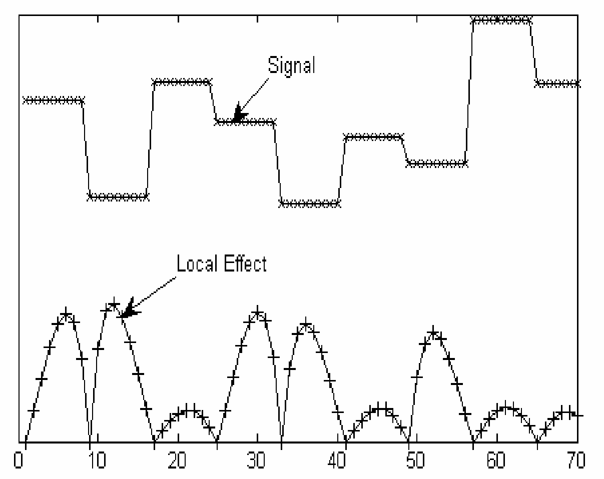
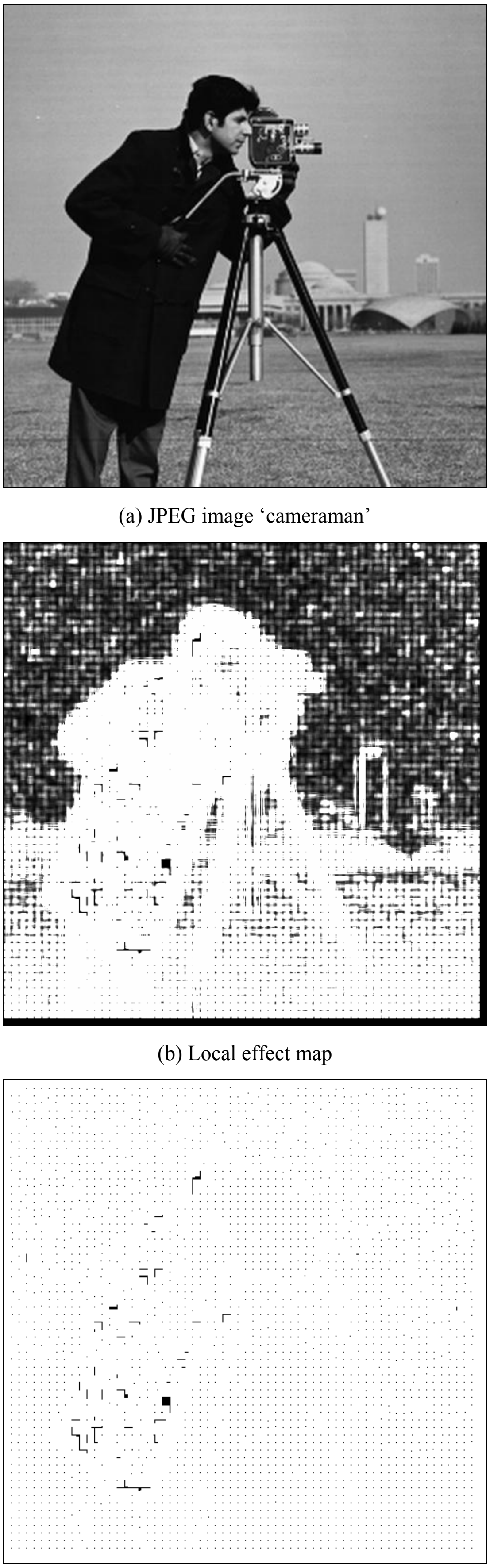


Figure 2. Example of 1-D BAG extraction

For 2-D image, the block is assumed to be 8*8, as it is used in most applied JPEG standard.

Suppose the luminance of pixels in a 8*8 window is $[s_{ij}]$ $(0 \le i,j \le 7)$, and $[S_{uv}]$ $(0 \le u,v \le 7)$ is the corresponding DCT coefficients, shown as formula (4), in which the definitions of α_u and α_v are the same with α_j in formula (3).



(a) JPEG image ‘cameraman’

(b) Local effect map

(c) BAG extraction

Figure 3. BAG extraction of JPEG image ‘cameraman’

$$S_{uv} = \frac{\sqrt{\alpha_u \alpha_v}}{8} \sum_{i=0}^{7} \sum_{j=0}^{7} s_{ij} \cos\frac{u(2i+1)\pi}{16} \cos\frac{v(2j+1)\pi}{16} \quad (4)$$

Then the local effect is defined with the right column and bottom raw AC coefficients, (5).

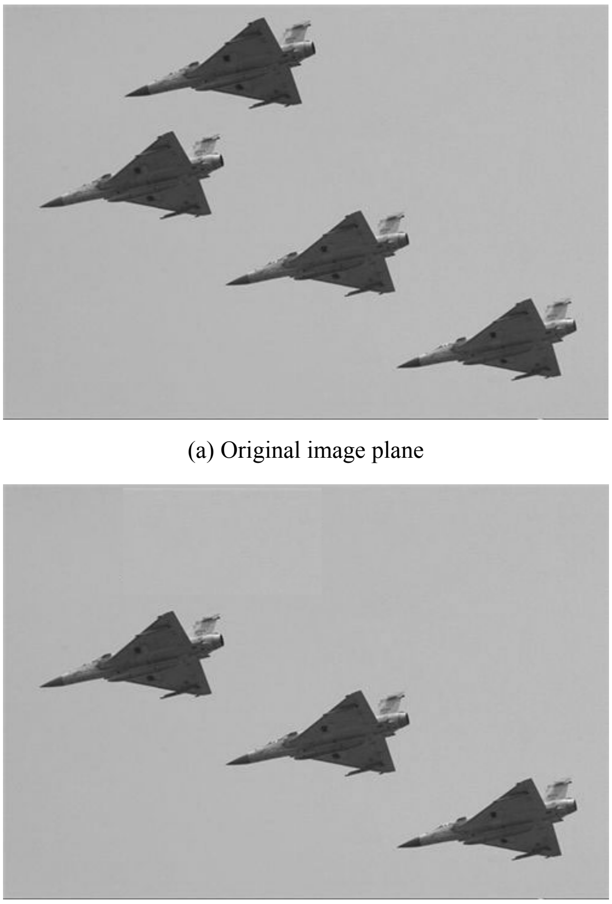
$$LE = \sqrt{\frac{\sum\limits_{i=7\,\text{and/or}\,j=7} S_{ij}^{2}}{S_{00}^{2}}} \quad (5)$$

Slide the window in the whole image, and a local effect map of LE can be obtained. Figure 3 shows an example of the local effect map of image cameraman.

In figure 3(b), the dark pixels mean small LE, and bright pixels correspond to large LE. It can be seen that pixels on the block edges have mostly smaller E than their neighbors, and they form the BAG. This grid locates the block edges, and exists in all lossy JPEG image.

To extract the BAG more clearly, we can mark the local minimal value points and obtain the cross-points of BAG, shown in figure 3(c).

3. IMAGE FORENSICS VIA BAG EXTRACTION



(a) Original image plane

(b) Doctored image plane(BMP)

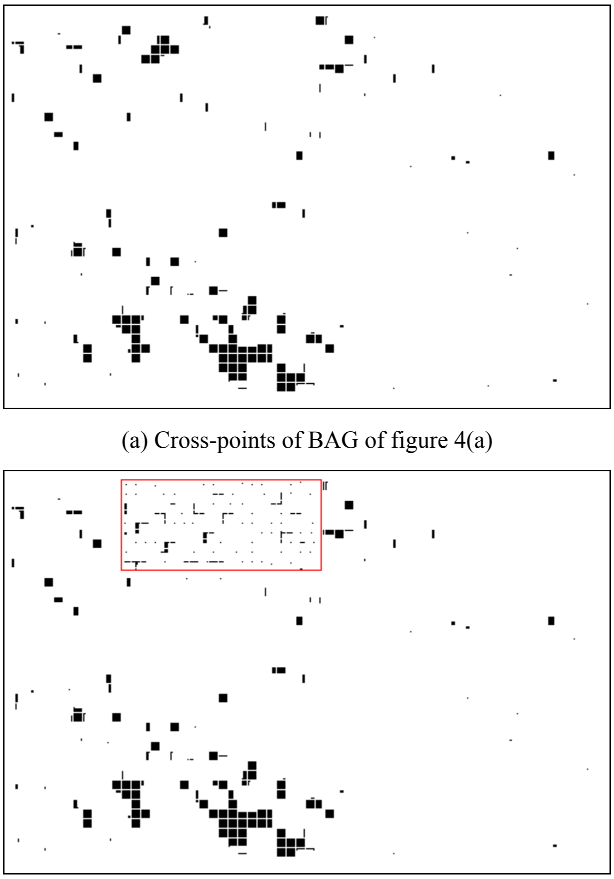
Figure 4. Example of copy-paste to hide object

A common goal of image juggle is to add or hide some special objects. To achieve this goal, the copy-paste operation is the most frequent applied process. Image inpainting is a useful technique to cover objects. But it is not a mature technique, especially for large recover area. Because of that, we just focused on the copy-paste forgery in this paper.

If the copied area comes from the same image, one or more duplicate area will exist in the image. Then the techniques based on the duplicated area detection may expose this forgery. On the other hand, if the copied area comes from other image, they can cheat these techniques.

In this paper, we are trying to authenticate the copy-paste operations if the copied image is JPEG compressed.

To make a spurious image, the copied area has to be placed in some fixed position to cheat human eyes, as we have discussed in section 1. However the BAG contained in the copied area usually can not snap to the BAG of the target image at the same time. Thus a trail is hidden in the image. If the trail is detected by the BAG marking algorithm, the image is authenticated as doctored.


(a) Cross-points of BAG of figure 4(a)

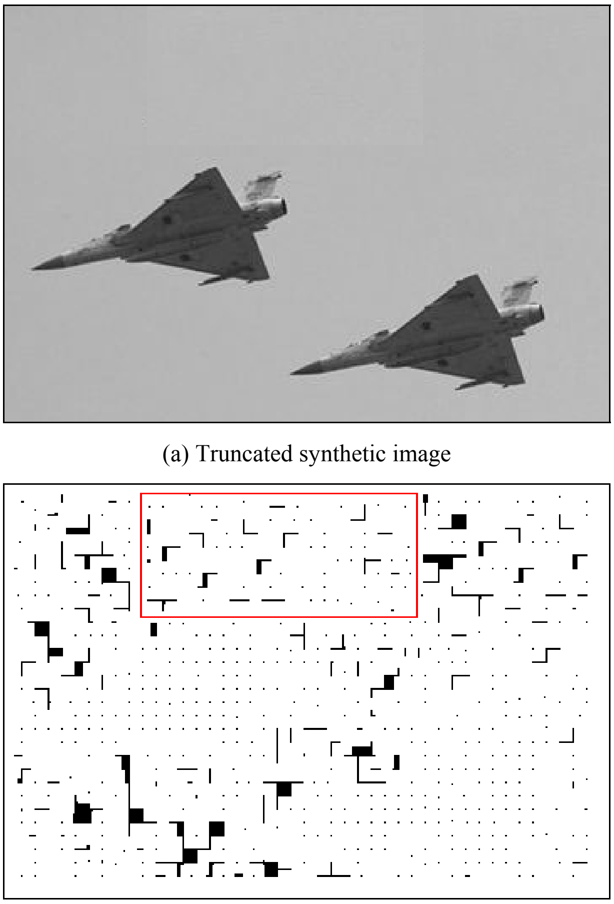
(b) Cross-points of BAG of figure 4(b)

Figure 5. BAG extraction of images in figure 4

Figure 4 gives an example of copy-pasted forgery to hide object. Image (a) is an original JPEG image from NASA website, and (b) is a doctored image (saved in BMP format) with one plane concealed by copying a neighbor sky and pasting to the position of the plane. The sizes of images are 500*334.

When the BAG extraction algorithm is applied to the figure 4, the BAG can be marked as shown in figure 5. In figure 5, the cross-points in normal positions are omitted to make a clearer view. From figure 5(b) it is clear that the doctored area is located. We can see that the doctored area is located clearly.

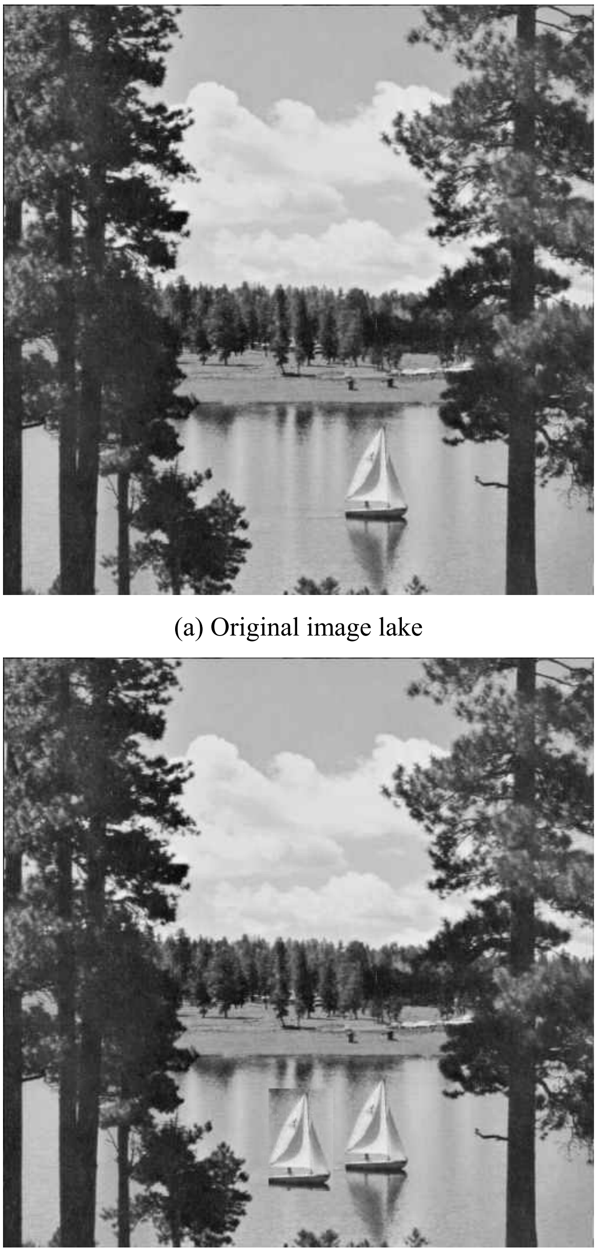
Truncation is a simple but efficient method to avoid detections based on double JPEG qualification [5] or based on block artifacts [6]. However, our algorithm still works. If the doctored image 4(b) is truncated, the detected cross-points of BAG grid is shown in figure 6. Since the normal BAG grid is shifted with image truncation, they remained in the detection image. We can see that the doctored area can be located since the cross-points are mismatch.


(a) Truncated synthetic image

(b) Cross-points of extracted BAG

Figure 6. Example of truncated synthetic image

Figure 7 gives another example of copy-pasted forgery of adding object. Image 7(a) is original JPEG image, and (b) is doctored image with one more boat duplicated. The image sizes are 512*512. This time, the doctored image is JPEG compressed with quality factor 95.



(a) Original image lake

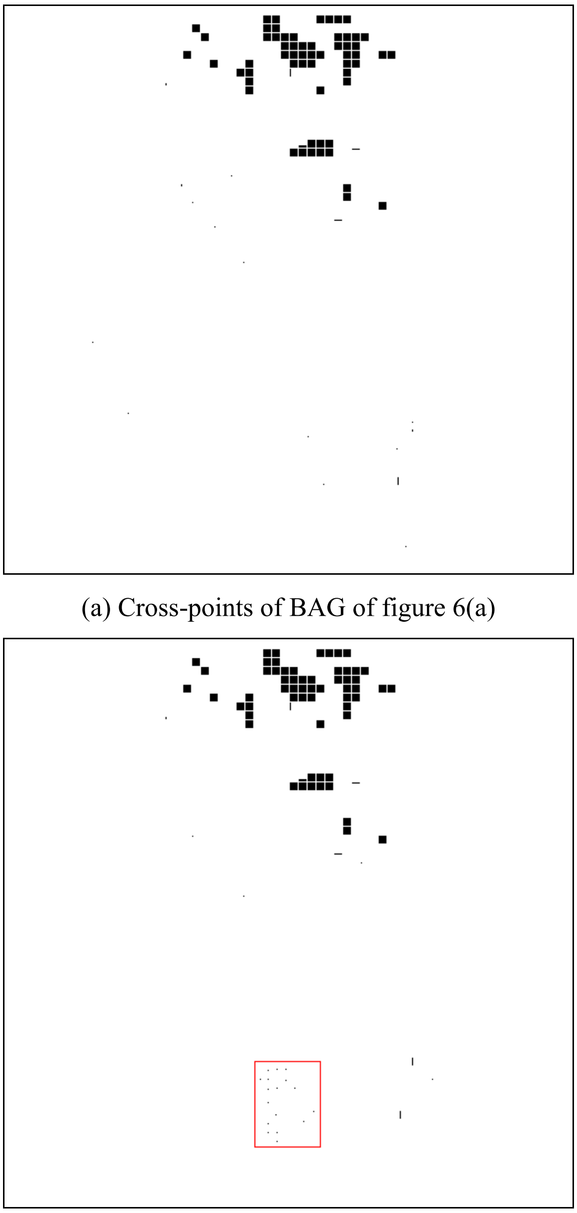
(b) Doctored image lake (JPEG)

Figure 7. Example of copy-paste to add object

Appling the BAG extraction algorithm to figure 7, the BAG can be generated as shown in figure 8. Again the cross-points in normal positions are omitted.

It should be mentioned that the JPEG compression, which is applied when saving the doctored image, has two influences. Firstly, the compression brings a new BAG into the doctored area, which is aligned to the BAG of undoctored area since they are all from the standard DCT blocking operation. Secondly, the compression blurs the BAG which was copy-pasted with the doctored area. That results in a phenomenon that the marked BAG in the copy-pasted area in figure 8 is much weaker than that in figure 5. However, the extracted BAG can still be used to authenticate images.

These experiment results demonstrate that our approach can detect copy-paste forgery effectively whether the copied area came from the same image or not, if only the copied image is JPEG compressed.



(a) Cross-points of BAG of figure 6(a)

(b) Cross-points of BAG of figure 6(b)

Figure 8. BAG extraction of images in figure 6

4. CONCLUSION AND FUTURE WORK

Passive image forensics is a great challenge in image processing techniques. There is not a method that can treat all cases, but many methods each can detect a special forgery. In this paper, a JPEG image forensics approach is proposed to detect copy-paste forgery based on the check of block artifact grid mismatch. This approach is available whether the copied area came from the same image or not, if only source image is JPEG compressed. This algorithm also works when the doctored image is truncated, however other existing algorithms will fail in this case. Experiment results demonstrate that this method works efficiently for copy-paste forgery.

This achievement is a preliminary study on this method. Our future work may focus on the following: Improving the BAG marking algorithm to achieve clearer grid map and reduce computation load; design a machine judging algorithm to check the alignment of BAG, and then test this approach on more copy-pasted images.

5. ACKNOWLEDGEMENTS

This paper is supported by the Science Research Fund of MOE-Microsoft Key Laboratory of Multimedia Computing and Communication (Grant No.06120808).

6. REFERENCES

[1] W.N. Lie, G.S. Lin, and S.L. Cheng, “Dual Protection of JPEG Images Based on Informed Embedding and Two-Stage Watermark Extraction Techniques”, *IEEE Trans. Information Forensics and Security*, vol. 1, no. 3, pp. 330-341, Sep. 2006.

[2] A.C. Popescu, and H. Farid, “Statistical Tools for Digital Forensics”, in *Proc. the 6th International Workshop on Information Hiding*, Toronto, Canada, 2004.

[3] W.H. Li, and B. Wang, “A Statistical Analysis on Differential Signals for Noise Level Estimation”, in *Proc. the 6th International Conference on Machine Learning and Cybernetics*, Hong Kong, China, Aug. 2007, pp. 2150-2153.

[4] J. Lukas, J. Fridrich, and M. Goljan, “Digital camera identification from sensor pattern noise”, *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205-214, June 2006.

[5] J.F. He, Z.C. Lin, L.F. Wang, and X.O. Tang, “Detecting doctored JPEG images via DCT coefficient analysis”, *Lecture Notes in Computer Science*, Springer Berlin, vol. 3953, pp.423-435, 2006.

[6] S.M. Ye, Q.B. Sun, and E.C. Chang, “Detecting digital image forgeries by measuring inconsistencies of blocking artifact”, in *Proc. IEEE International Conference on Multimedia and Expo 2007*, Beijing, China, July 2007, pp.12-15.

[7] A.C. Bovik, and S. Liu, “DCT-domain Blind Measurement of Blocking Artifacts in DCT-coded Images”, in *Proc. IEEE International Conference on Acoustics, Speech and Signal Processing*, Salt Lake City, UT. USA, pp. 1725-1728, 2001.

[8] F. Pan, X. Lin, S. Rahardja, and etc., “A Locally Adaptive Algorithm for Measuring Blocking Artifacts in Images and Videos”, in *Proc. the 2004 International Symposium on Circuits and Systems*, Singapore, May 2004, pp. 23-26.