Signal Processing 89 (2009) 1821–1829

Contents lists available at ScienceDirect

Signal Processing

journal homepage: www.elsevier.com/locate/sigpro

Passive detection of doctored JPEG image via block artifact grid extraction

Weihai Li [a,*], Yuan Yuan [b], Nenghai Yu [a]

[a] MOE-Microsoft Key Laboratory of Multimedia Computing and Communication, University of Science and Technology of China, Hefei, Anhui 230027, China
[b] School of Engineering and Applied Science, Aston University, Birmingham B4 7ET, UK

ARTICLE INFO

Article history:
Received 14 November 2008
Received in revised form
21 March 2009
Accepted 23 March 2009
Available online 1 April 2009

Keywords:
Doctored image forensic
JPEG compression
Block artifact grid
Grid mismatch

ABSTRACT

It has been noticed that the block artifact grids (BAG), caused by the blocking processing during JPEG compression, are usually mismatched when interpolating or concealing objects by copy–paste operations. In this paper, the BAGs are extracted blindly with a new extraction algorithm, and then abnormal BAGs can be detected with a marking procedure. Then the phenomenon of grid mismatch or grid blank can be taken as a trail of such forensics. Experimental results show that our method can mark these trails efficiently.

1. Introduction

It has been noticed that digital synthesized pictures are flooding everywhere with aids of modern image processing softwares, e.g. Adobe Photoshop. There are some fascinating applications the convenient image-synthesis technique can afford: one can pretend that he had been to somewhere by inserting his own image to a scene; some miracles can be made by combining some unrelated images together, etc. However, this technique also brings some legal crisis, since it is hard to discriminate picture evidences real or fake. To vindicate people's confidence on pictures, more and more experts put their eyes on the techniques of image forensics.

There are two kinds of techniques for image forensics: active and passive. Active protection techniques, such as proposed in [1], are to embed some watermarks or signatures into original pictures when they are achieved. If pictures are tampered, the embedded information will be demolished. Unfortunately, most present imaging devices do not contain such modules. Thus active protection techniques cannot work on most existent doctored images. Many passive detection techniques have been proposed from different aspects. High order statistical analysis is to test whether an image has same statistical characteristics as nature picture [2,3]. Trails detection and location is to detect whether an image contains certain doctored trail and located it if possible [4]. Consistency verification is to check whether an image contains special marks which come from claimed device [5–7]. Rationality judgment is to verify whether an image is reasonable to nature phenomena [8]. However, tampering an image is usually easier than detecting a tampered image. It may be easy for a faker to evade a detection algorithm, but it will be very hard to evade all detection algorithms. Thus we need more detection methods.

Till now, most of these techniques require the doubtful images to be uncompressed and high quality. As for the widely used JPEG image format, there are mainly three kinds of methods based on JPEG characteristics. Double JPEG quantization detection is to detect whether an image was JPEG compressed twice [9–11], and He et al. [12] had improved it to detect partial doctored JPEG image and even to locate tampered areas. Ye et al. [13] proposed

* Corresponding author.
E-mail address: whli@ustc.edu.cn (W. Li).

0165-1684/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.sigpro.2009.03.025

another method to detect doctored JPEG image by checking the uniformity of quantization remainders. However, these two methods may fail under the following conditions:

- The JPEG image may be truncated. Then a new 8∗8 block may contain two or four original DCT blocks, so that the image will be judged as uncompressed by both methods.
- The original images or doctored images may be compressed more than twice. Then the periodic property caused by double quantization will disappear.

Fan and de Queiroz [14] proposed a lightweight method to check whether an image is JPEG compressed and further

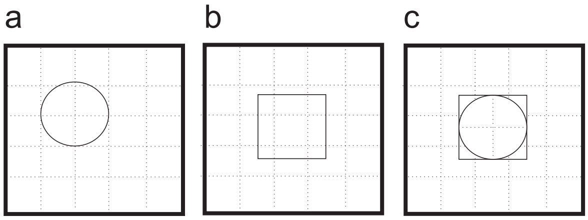

Fig. 1. Demonstration of BAGs mismatch: (a) original image A, (b) original image B and (c) synthetic image C.

locate the whole position of block artifacts. However, since Fan and de Queiroz's method is a statistical method throughout the whole image, it can give only a whole result without details, and detection result is easy to be interfered by mismatched block artifacts when JPEG image is copy–pasted.

Some purposes of image counterfeiting is to interpolate special objects into original images by copy–paste processing, or conceal special objects from original image by copy–paste processing or by inpainting processing [12,15]. Here the inpainting processing can also be treated as a copy–paste processing, which copied from an uncompressed computer graphics.

It is well known that during lossy JPEG compressing, blocking process will introduce some horizontal or vertical breaks into image. These breaks form an 8∗8 grid, called block artifact grid (BAG). It has been noticed [12,13,16] that when copy–paste processing is done, the copied slice must be pasted in proper place to illude human eyes, thus the BAG in copy–pasted slice and the BAG in target image are usually mismatched, see Fig. 1.

In Fig. 1(a) and (b) are two original JPEG images and (c) is a synthesized image, in which a inscribed disc was interpolated from (a) into (b). The dot lines are BAGs. It is clear in (c) that the BAG in the pasted slice mismatches to the BAG in surrounding parts.

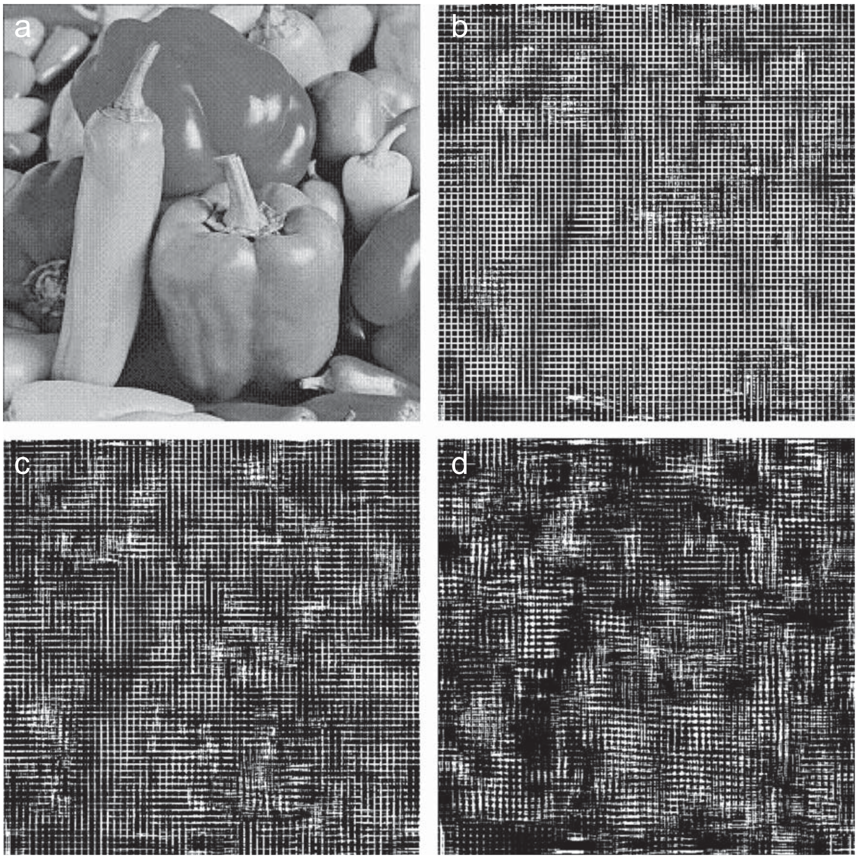

Fig. 2. Comparison of extracted BAG images for different JPEG compression QF: (a) original image capsicum, (b) extracted BAG image (QF = 50), (c) extracted BAG image (QF = 75) and (d) extracted BAG image (QF = 85).

In this paper, a new algorithm is proposed to blindly extract the BAGs first, and then this algorithm is applied to JPEG image forensics. The areas where BAGs mismatch to others or the areas where BAGs are missing are likely to be doctored areas.

The rest of this paper will be formed like the following. In Section 2, the BAGs extraction algorithm is given. Unlike other block artifact estimation algorithms [17,18], what we care here is not the absolute level of block artifact but the locations of BAGs. Then the algorithm is applied to image forensics in Section 3, including the cases of copy–paste from a JPEG image, copy–paste from an uncompress image, and crop of images. A comparison with Ye et al.'s method is also given in Section 3. Finally, a short conclusion is made in Section 4.

2. BAG extraction algorithm

For widely used JPEG compression standard, the blocking processing introduces horizontal and vertical breaks into images, which is known as block artifacts. This phenomenon is usually treated as flaw of JPEG, and many efforts have been done to estimate it or to weaken it. However, the block artifact is utilized in this paper to detect whether an image is tampered or not. To do this, the block artifact grid should be extracted firstly as clearly as possible.

The noises in a JPEG image can be divided into two kinds. One kind is nature noises, which come from light scatter, lens faulty, electronic noise, and so on. These noise levels are very low for modern digital cameras. The other kind is the BAG noise, which corresponds to JPEG compression factor. The BAG has the following characteristics: the grid is formed by horizontal lines and vertical break lines, which have a periodicity of 8 at both directions. Thus, we can extract weak horizontal and vertical edges with periodicity of 8 separately, and then combine them as the BAGs. For simplicity, we just focus on gray-scale images only in this paper. For color image, we only deal with the luminance component since which component is $8*8$ blocked in JPEG standard.

A general procedure to extract horizontal BAG lines contains two parts. For an image S, the weak horizontal edges are firstly extracted as image E_h. Then lines with periodicity 8 in E_h are strengthened and we got image G_h.

2.1. Extract weak horizontal edges from image S

Since horizontal BAG lines are regarded as weak horizontal edges, an absolute second-order difference is

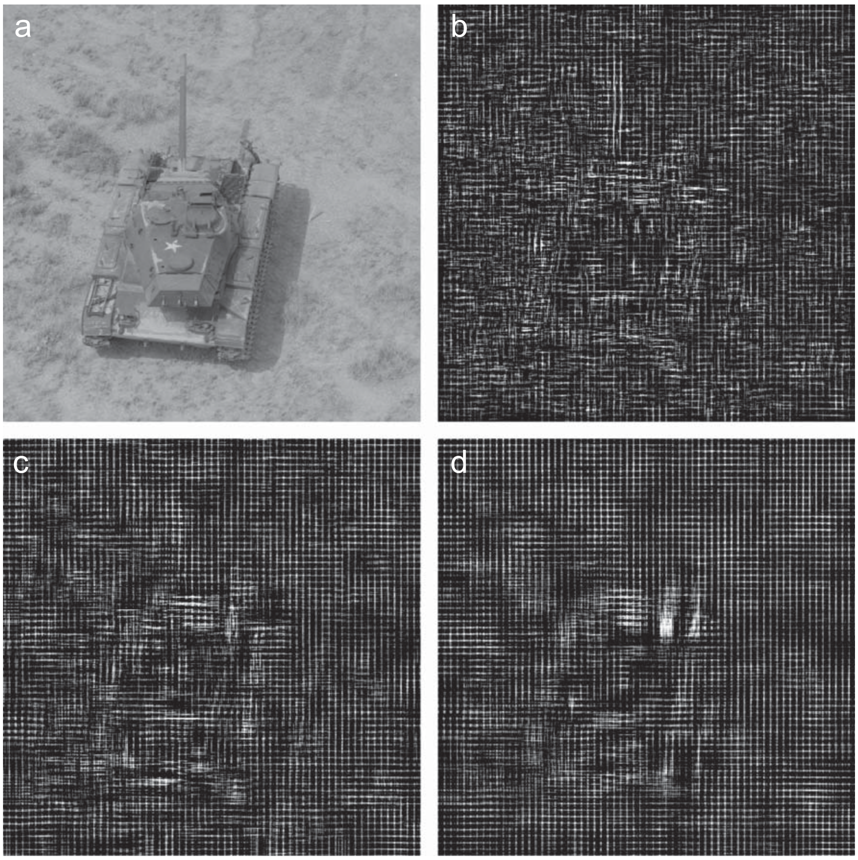

Fig. 3. Comparison of extracted BAG images with different AC: (a) original image tank ($QF = 75$), (b) extracted BAG image ($AC = 17$), (c) extracted BAG image ($AC = 33$) and (d) extracted BAG image ($AC = 49$).

calculated firstly to extract weak horizontal edges from an image. Suppose $s(y, x)$ are pixels in doubtful image S and $d(y, x)$ are elements in absolute second-order difference D, which can be calculated with the formula

$$d(y,x) = |2s(y,x) - s(y-1,x) - s(y+1,x)| \tag{1}$$

In subsequence steps, a median filter is applied to efficiently remove the interference coming from strong image edges. But, in order to further weaken edge influence and to avoid false alarm caused by periodic line edges, we ignore all differentials larger than 50 (this is not a rigorous value). Generally, block artifacts are much smaller than 50, so there is no danger to miss block artifacts.

Then, every 33 columns (two blocks on each side) are accumulated horizontally to enlarge weak horizontal lines in D, see formula (2). We note $AC = 33$. In order to equalize amplitudes throughout result image, a local median is reduced from each elements as shown in formula (3) in which the function $Mid[A\{\}]$ returns the median of set $A\{\}$. Thus $e(y, x)$ are elements in image E_h.

$$e_s(y,x) = \sum_{i=x-16}^{16} d(y,i) \tag{2}$$

$$e(y,x) = e_s(y,x) - Mid[\{e_s(i,x)|y-16 \leqslant i \leqslant y+16\}] \tag{3}$$

The number of columns to accumulate and the number of rows to equalize are selected equal to form a macro-block. If AC is too large, small doctored area may be missed. Thus AC should be as small as possible. But if the AC is too small, the weak BAG lines may not be strengthened adequately and image edge influence is still noticeable. Fig. 3 gives a comparison of extracted BAG image with different AC. It can be seen that image edge influence is visible when $AC = 17$ and almost invisible when $AC = 49$. In this paper, we choose $AC = 33$ as a likely value that balance the two aspects.

2.2. Extract lines with periodicity 8 from image E_h

BAGs are periodic signals which appear only on boundaries of $8*8$ blocks, so the extracted BAG image should also has period of 8. Another noticeable feature is that BAGs are local phenomenon, or we can say that block artifact only related with an $8*8$ block and its four neighbor blocks. For a given compression quality factor, the level of BAGs correlates to image content, and BAGs even does not appear on some boundaries. What is more, remained image edges may also influence the result and cause few random strong lines. To enhance BAGs from noise, the weak horizontal edge image E_h is further periodical median filtered with the formula

$$g_h(y,x) = Mid[\{e(i,x)|i = y-16, y-8, y, y+8, y+16\}] \tag{4}$$

Here $g_h(y, x)$ are the elements in the extracted horizontal BAG line image G_h. In formula (4), five elements with spacing 8 are used in the median filter. Thus strong BAGs and weak BAGs can be smoothed, and strong burst lines without period 8 can be removed. The more elements used in the median filter, the better the extracted BAGs

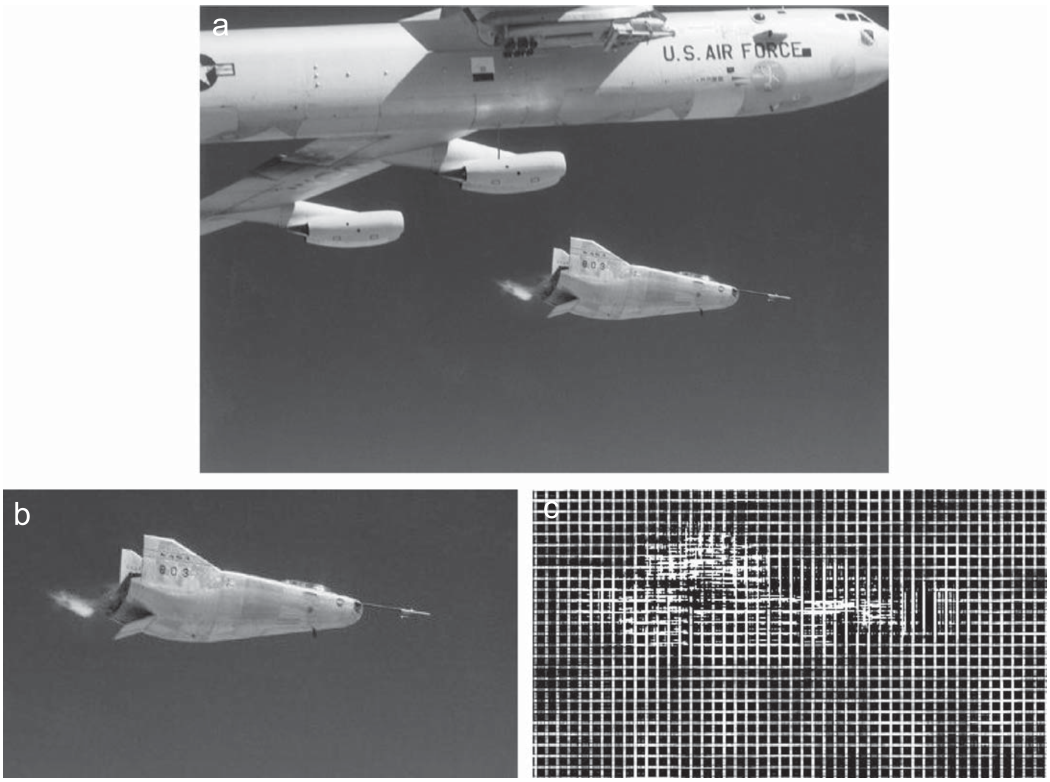

Fig. 4. Detection of cropped image: (a) original image, (b) cropped image and (c) extracted BAG image.

will be, however, the more possible the doctored area may be missed.

Similarly, the vertical BAG line image G_v can be extracted. Add G_h and G_v together, and the final BAG image is obtained.

$$g(y,x) = g_h(y,x) + g_v(y,x) \tag{5}$$

In formula (5), $g_v(y, x)$ are elements in the extracted vertical BAG line image G_v, and $g(y, x)$ are elements in the extracted final BAG image G. Fig. 2 shows an example of BAG extraction. Fig. 2(a) is an original image capsicum. Fig. 2(b), (c) and (d), are extracted BAG images from compressed Fig. 2(a) with quality factor (QF) 50, 75 and 85, respectively (see also Fig. 3). Obviously, our method works better for low QF. Anyway it is still efficient for high QF after being further processed, shown in Fig. 6(a).

3. Image forensic via BAG extraction

In this paper, we will discuss the following kinds of image tampering: image cropping, object concealing by inpainting technique or by copy–paste processing from a non-JPEG format image, object interpolation or concealment by copy–paste processing from a JPEG format image.

3.1. Detection of image cropping

Image cropping is a simple method to conceal some object. People may crop images and only store what they want. However, few people care whether they crop along block boundaries. Thus the BAGs in cropped image are often shifted from original positions, and it can be found in extracted BAG image.

Fig. 4 shows a simple example of image cropping. Fig. 4(a) is the original image downloaded from the NASA

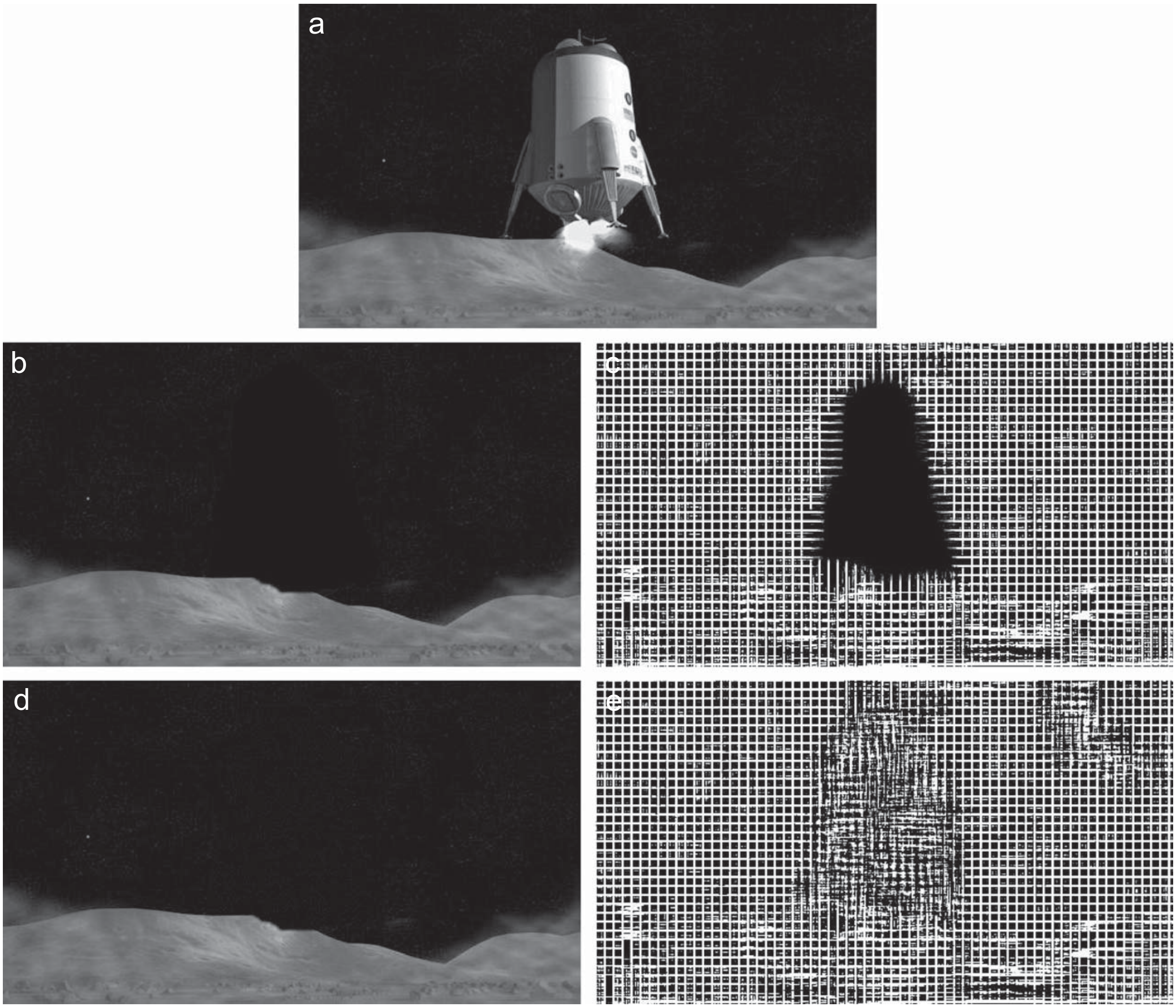

Fig. 5. Detection of painted image: (a) orginal image, (b) doctored image by filling pour black, (c) extracted BAG image from (b), (d) doctored image by filling random dark color and (e) extracted BAG image from (d).

website and compressed with mspaint.exe. Fig. 4(b) is a cropped part form Fig. 4(a), and (c) is the extracted BAG image from Fig. 4(b). From Fig. 4(c), it is very clear that the BAGs located at wrong position. Thus we can conclude that Fig. 4(b) is not an original image, but a cropped image.

3.2. Detection of painted image

Another method to conceal object is image painting, including image inpainting, computer graphics, and so on. Theoretically, these can be treated as a special case of copy–paste processing which is copying from an uncompressed image. Since the copied slice is uncompressed, no BAG will be extracted from the pasted area. However, nature images always contain small noises, and BAGs exist after JPEG compressed, even for a dark background. So if there are large blank in the extracted BAG image, then we can conclude that these area is doctored.

To simplify the analysis in this paper, we just detect the tampering of copy–paste processing, given in Fig. 5. Fig. 5(a) is an original image downloaded from the NASA website and compressed with mspaint.exe. Fig. 5(b) and (d) are doctored images from Fig. 5(a) with the spacecraft concealed by filling the area with pour black color or with random dark color, respectively. Fig. 5(c) and (e) are BAG images extracted from Fig. 5(b) and (d), respectively.

It is clear in Fig. 5(c) that the area corresponding to the spacecraft is totally blank. That is because pixels in this area are all black (gray value 0) and no edge exists. In Fig. 5(e), there are mussy "BAGs" extracted in the area corresponding to the spacecraft. These "BAGs" are caused by some tiny influence from noise, and their values are much smaller than real BAGs.

Taking one with another, if large dark area or faint area is detected, we should doubt that this area is painted by inpainting, or by computer graphics, or by copy–paste processing from an uncompressed image, or other similar methods.

3.3. Detecting of copy–pasted image which copied from a JPEG image

Copy–paste processing is a frequently used method to tamper an image. Since JPEG format is the mostly employed image format, more likely the copied slice came from JPEG images. As we have discussed above, the copied slices must be placed on certain positions to delude human eyes, and the matching of BAGs are hardly considered. So if a BAG mismatching phenomena is detected, it can be treated as possible clue of tampering.

However, the check of BAG mismatching in an extracted BAG image is quite boring and subjective. In the following, a marking procedure is introduced to mark BAG mismatching areas routinely.

Take a view on an $8*8$ block $A = [a]_{8*8}$ of BAG image, which located at a normal position. If the BAGs locate at abnormal positions in this block, there will be BAG lines in the $6*6$ center-matrix. Thus we can denote BAG locations with b, the maximum summation along the 6 rows and 6 columns minus the minimum summation at block border,

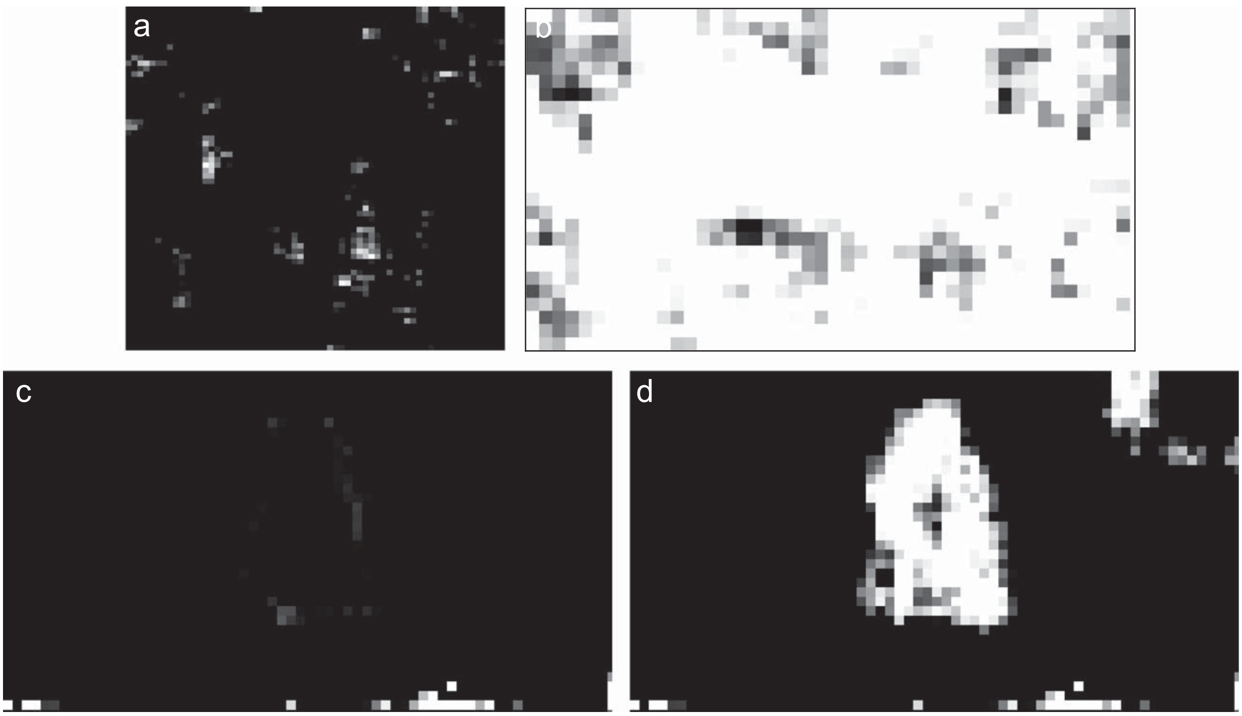

Fig. 6. Examples of marked BAG images: (a) marked image of Fig. 2(d), (b) marked image of Fig. 4(c), (c) marked image of Fig. 5(c) and (d) marked image of Fig. 5(e).

as given in the formula

$$b = \mathrm{Max}\left\{ \sum_{i=2}^{7} a(i,x) \middle| 2 \leqslant x \leqslant 7 \right\} - \mathrm{Min}\left\{ \sum_{i=2}^{7} a(i,x) \middle| x = 1,8 \right\} + \mathrm{Max}\left\{ \sum_{i=2}^{7} a(y,i) \middle| 2 \leqslant y \leqslant 7 \right\} - \mathrm{Min}\left\{ \sum_{i=2}^{7} a(y,i) \middle| y = 1,8 \right\} \quad (6)$$

In formula (6), the function Max[$A\{\}$] and Min[$A\{\}$] returns the maximum or minimum value of set $A\{\ \}$, respectively. Then the block A is filled with value b, and final marked image is obtained.

As an example, the extracted BAG images Fig. 2(d), Fig. 4(c), Fig. 5(c) and (e) are marked and given in Fig. 6. In Fig. 6(a) and (c), the marked area are quite few and dispersed, so we know BAGs in these two images locate at normal positions if there are BAGs (there is no BAGs in some area of Fig. 5(b)). In Fig. 6(b), there are quite many marked blocks, so we know the BAGs locate at abnormal positions. The non-uniform of marked values in Fig. 6(b) is

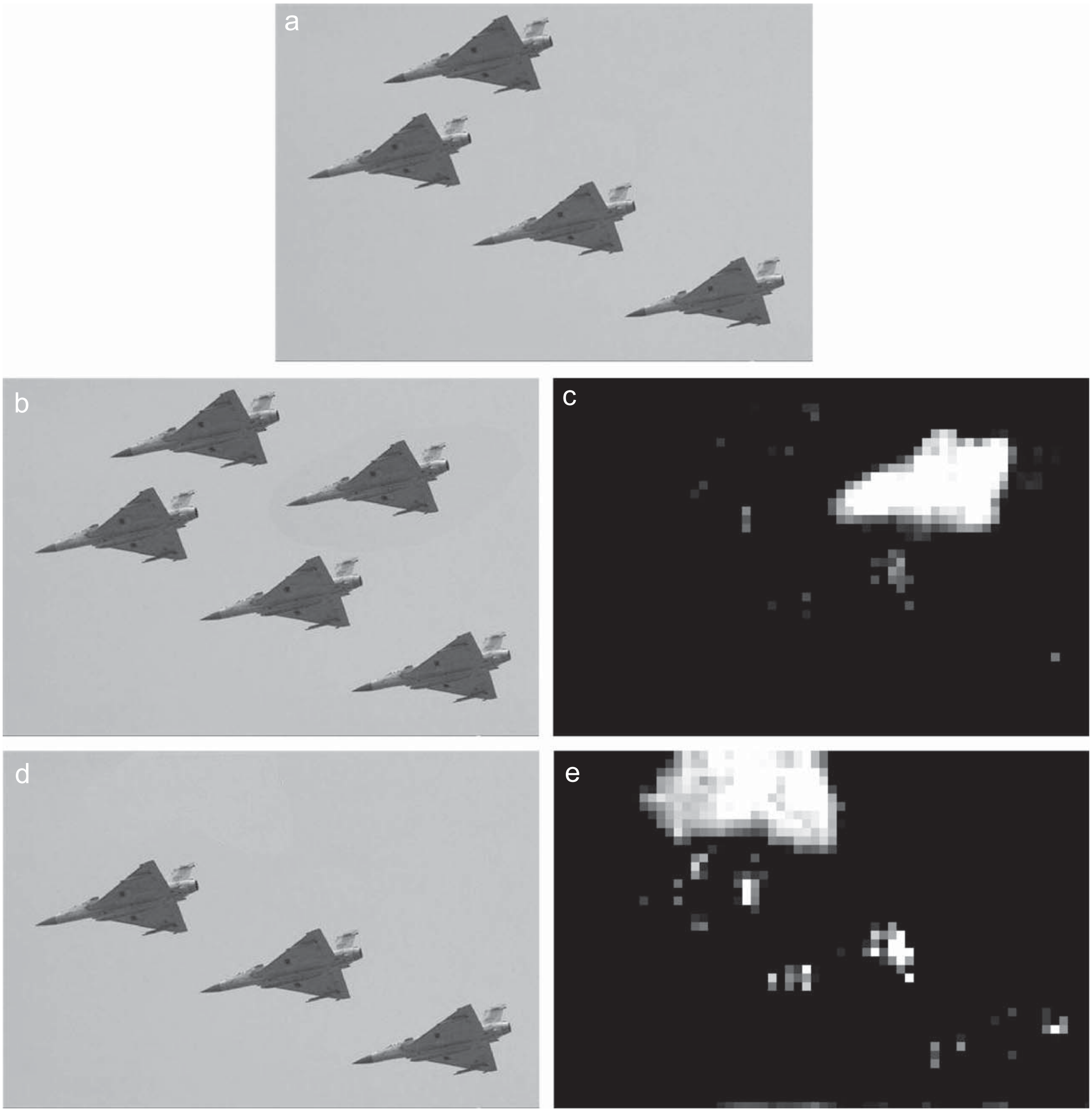

Fig. 7. Detection of copy–pasted image: (a) original image, (b) doctored image with one airplane interpolated, (c) marked BAG image of (b), (d) doctored image with one airplane concealed and (e) marked BAG image of (d).

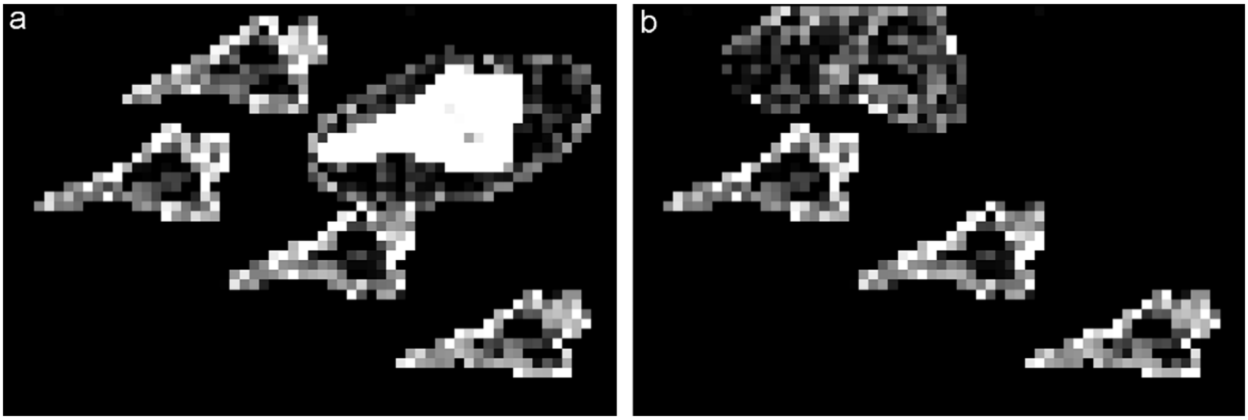

Fig. 8. Detection of copy–pasted image by Ye et al.'s method: (a) detection of Fig. 7(b) and (b) detection of Fig. 7(d).

caused by the non-uniform of block artifacts. In Fig. 6(d), mussy "BAGs" are marked, and the doctored area is thus located.

In the following of this paper, the marking procedure will be used to detect copy–paste tampering when copied slices came from JPEG images.

Fig. 7 is detection examples of object interpolation and object concealing by copy–paste processing. Fig. 7(a) is downloaded from the NASA website and compressed with mspaint.exe. Fig. 7(b) is a doctored image with one more airplane interpolated which copied the original top-second one, and Fig. 7(d) is a doctored image with the original top-first airplane concealed by copying a nearby sky and paste on it. Fig. 7(c) and (e) are marked BAG images corresponding to Fig. 7(b) and (d), respectively, in which the doctored areas are marked correctly.

Ye et al. also proposed a method to detect copy–paste forgery by measuring inconsistencies of blocking artifacts [13], where block artifact at block corners are estimated via a 2×2 pattern comparing between block center and corners. Fig. 8 gives detection experiments by Ye et al.'s method. The results show that Ye et al.'s method can also mark forgery areas correctly. However, the block artifact $B(i)$ defined in Ye et al.'s method is not consistent throughout an image, which are bigger in texture areas than in plain areas. From Fig. 8(b) it can be seen that the block artifacts caused by plane edges are even stronger than by copy–paste forgery. Compared with Fig. 7, we may conclude that our method restrains image edges better.

From the above three subsections we can conclude that our method is efficient to detect most doctored JPEG images, unless the BAGs match each other hit-and-miss sporadically. To detect JPEG images routinely, the BAG image should be extracted and checked firstly to judge whether the image is cropped (if BAGs are not in correct positions) or pasted with a non-JPEG compressed slice (if there is a blank area in BAGs), then image is cropped to ensure that BAGs are located at correct positions, and mark the BAG image to judge whether the image is pasted with a JPEG compressed slice.

For a 256×256 image, our BAG image extraction program costs 24 s with MATLAB 7.0 environment on a IBM T43 notebook PC (1.73 GHz CPU, 512 MB memory). The cost seems too big, but it should be mentioned that 99.6% time of our program is spent on median filters, formulas (3) and (4), which are done by bubble sorting data and pick the median one. If the median filters are optimized, the computation cost will be cut down significantly.

4. Conclusion

Passive image forensics is a great challenge in image processing techniques. This paper focuses on the passive detection of doctored JPEG image via the check of abnormal block artifact grid. A new algorithm is proposed to blindly extract BAGs from JPEG images and check abnormal BAGs routinely. The efficiency of this algorithm is validated by experiment results. Then the algorithm is applied to passive JPEG image forensics. Some demonstrations show our method can detect JPEG images tampering efficiently, such as cropping processing, inpainting processing, and copy–paste processing, which copied from either JPEG source images or from uncompressed source images. Our future works include improvement on the BAG extraction algorithm to achieve clearer BAG images, development of the marking procedure to check the alignment of BAGs more intelligently.

Acknowledgments

This paper is supported by the Science Research Fund of MOE-Microsoft Key Laboratory of Multimedia Computing and Communication (no. 06120808) and Open Research Project of Image Processing and Image Communication Laboratory of Jiangsu Province of China (no. ZK207007).

References

[1] W.N. Lie, G.S. Lin, S.L. Cheng, Dual protection of JPEG images based on informed embedding and two-stage watermark extraction techniques, IEEE Transactions on Information Forensics and Security 1 (3) (September 2006) 330–341.

[2] T.T. Ng, S.F. Chang, Q. Sun, Blind detection of photomontage using higher order statistics, in: IEEE International Symposium on Circuits and Systems, Vancouver, Canada, 2004, pp. 688–691.
[3] W.H. Li, B. Wang, A statistical analysis on differential signals for noise level estimation, in: Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, China, 2007, pp. 2150–2153.
[4] A.C. Popescu, H. Farid, Statistical tools for digital forensics, in: The 6th International Workshop on Information Hiding, Toronto, Canada, 2004, pp. 128–147.
[5] A.C. Popescu, H. Farid, Exposing digital forgeries in color filter array interpolated image, IEEE Transactions on Signal Processing 53 (10) (October 2005) 3948–3959.
[6] J. Lukas, J. Fridrich, M. Goljan, Digital camera identification from sensor pattern noise, IEEE Transactions on Information Forensics and Security 1 (2) (June 2006) 205–214.
[7] Z. Lin, R. Wang, X. Tang, et al., Detecting doctored images using camera response normality and consistency 2005, in: IEEE Conference on Computer Vision and Pattern Recognition, San Diego, USA, 2005, pp. 1087–1092.
[8] M.K. Johnson, H. Farid, Exposing digital forgeries by detecting inconsistencies in lighting, in: ACM Multimedia and Security Workshop, New York, USA, 2005, pp. 1–10.
[9] D. Fu, Y.Q. Shi, Q. Su, A generalized Benford's law for JPEG coefficients and its applications in image forensics, in: Proceedings on SPIE Electronic Imaging, Security and Watermarking of Multimedia Contents IX, vol. 6505, 2007, pp. 1L1–1L11.
[10] J. Lukas, J. Fridrich, Estimation of primary quantization matrix in double compressed JPEG images, in: Proceedings on Digital Forensic Research Workshop, Cleveland, USA 〈http://www.ws.binghamton.edu/fridrich/Research/paper_3_color.pdf〉, 2003.
[11] T. Pevny, J. Fridrich, Detection of double-compression in JPEG images for applications in steganography, IEEE Transactions on Information Forensics and Security 3 (2) (February 2008) 247–258.
[12] J.F. He, Z.C. Lin, L.F. Wang, X.O. Tang, Detecting doctored JPEG images via DCT coefficient analysis, in: Lecture Notes in Computer Science, vol. 3953, Springer, Berlin, pp. 423–435.
[13] S.M. Ye, Q.B. Sun, E.C. Chang, Detecting digital image forgeries by measuring inconsistencies of blocking artifact, in: IEEE International Conference on Multimedia and Expo, Beijing, China, 2007, pp. 12–15.
[14] Z.G. Fan, R.L. de Queiroz, Identification of bitmap compression history: JPEG detection and quantizer estimation, IEEE Transactions on Image Processing 12 (2) (February 2003) 230–235.
[15] J. Sun, L. Yuan, J. Jia, et al., Image completion with structure propagation, ACM SIGGRAPH 24 (3) (July 2005) 861–868.
[16] W.H. Li, N.H. Yu, Y. Yuan, Doctored JPEG image detection, in: Proceedings of International Conference on Multimedia and Expo 2008, Hannover, Germany, ICME Proceedings, 2008, pp. 253–256.
[17] A.C. Bovik, S. Liu, DCT-domain blind measurement of blocking artifacts in DCT-coded images, in: IEEE International Conference on Acoustics, Speech and Signal Processing, Salt Lake City, USA, 2001, pp. 1725–1728.
[18] F. Pan, X. Lin, S. Rahardja, et al., A locally adaptive algorithm for measuring blocking artifacts in images and videos, in: Proceedings of the 2004 International Symposium on Circuits and Systems, ISCAS'04, Singapore, pp. 23–26.