

DETECTING DIGITAL IMAGE FORGERIES BY MEASURING INCONSISTENCIES OF BLOCKING ARTIFACT

Shuiming Ye^{1,2}, Qibin Sun¹, and Ee-Chien Chang²

¹ Institute for Infocomm Research, Singapore 119613

² School of Computing, National University of Singapore, Singapore 117543

Email: shuiming@i2r.a-star.edu.sg, qibin@i2r.a-star.edu.sg, changec@comp.nus.edu.sg

ABSTRACT

Digital images can be forged easily with today's widely available image processing software. In this paper, we describe a passive approach to detect digital forgeries by checking inconsistencies of blocking artifact. Given a digital image, we find that the blocking artifacts introduced during JPEG compression could be used as a "natural authentication code". A blocking artifact measure is then proposed based on the estimated quantization table using the power spectrum of the DCT coefficient histogram. Experimental results also demonstrate the validity of the proposed approach.

1. INTRODUCTION

Digital watermarking and signature are two main techniques of image authentication. However, most images captured today actually do not contain any digital watermark or signature. Therefore, it is required to passively check the integrity of digital image. The first attempt is to detect the traces of specific manipulation during forgery creation, such as resampling [1], copy-paste [2, 3], and color filter array interpolation [4]. The second attempt is based on the statistics of natural image [5], inconsistencies based on scene lighting direction [6], or camera response normality [7]. All these approaches are effective in some aspects, but new approaches are still desirable for practical applications.

JPEG image format is popularly used in most digital cameras and image processing software. Usually JPEG compression introduces blocking artifacts. Manufacturers of digital cameras and image processing software typically use different JPEG quantization table to balance compression ratio and image quality. Such differences will also cause different blocking artifacts in the images acquired. When creating a digital forgery, the resulted tampered image may inherit different kind of compression artifacts from different sources. These inconsistencies, if detected, could be used to check image integrity. Besides, forgeries creation process would also change the blocking artifacts, because the blocking artifacts of the affected blocks will change a lot by tampering operations such as image splicing, resampling, and local object operation such as skin optimization. Therefore, the blocking artifact inconsistencies found in a given image may tell the history that the image has been undergone.

In this paper, we propose a passive way to detect digital image forgery by measuring its quality inconsistency based on JPEG blocking artifacts. A new quantization table estimation based on power spectrum of the histogram of the DCT coefficients is firstly introduced, and blocking artifact measure is calculated based on the estimated table. The inconsistencies of the JPEG blocking artifacts are then checked as a trace of image forgery. Our proposed approach is able to detect spliced image forgeries using different quantization table, or forgeries which would result in the blocking artifact inconsistencies in the whole images, such as block mismatching and object retouching. In addition, our proposed quantization table estimation algorithm is much faster than maximum likelihood based methods [8, 9].

The paper is organized as follows. In Section 2, we present our proposed method with details of blocking artifact measure, quantization table estimation, and forensic analysis based on blocking artifact measure. The experimental results and conclusions are then given in Section 3 and 4, respectively.

2. PASSIVE IMAGE FORENSIC BASED ON BLOCKING ARTIFACT MEASURE

2.1. Blocking Artifact Measure

Blocking artifact measure plays an important role in areas of image and video processing such as optimal bit allocation and post-processing. Here we explore it to detect image forgeries.

Blocking artifact for each block is estimated via:

$$B(i) = \sum_{k=1}^{64} |D(k) - Q(k) \text{round}(\frac{D(k)}{Q(k)})| \quad (1)$$

where $B(i)$ is the estimated blocking artifact for the testing block i , and $D(k)$ is the DCT coefficient at position k . $Q(1:64)$ is the estimated DCT quantization table. The blocking artifact measure (BAM) for the whole image is then calculated based on the blocking artifacts of all blocks:

$$BAM = \frac{1}{N} \sum_i B(i) \quad (2)$$

where N is the total number of image blocks.

To estimate the JPEG quantization table, a method called maximum likelihood estimation (MLE) is proposed

in [8, 9] based on the total estimated blocking artifact at DCT frequency i given an estimated step $Q(i)$. In [10], a statistical model based on Benford's law for the probability distribution of the first digits of the JPEG coefficients is used to estimate the JPEG quantization factor. For a given candidate $Q(i)$, a complicated maximum likelihood estimation based on quantization artifacts of the whole coefficients must be computed. Therefore, these methods are very time consuming since they are all based on exhaustive searching for estimation. In next sub-section, we present a faster quantization table estimation algorithm based on histogram power spectrum of DCT coefficients.

2.2. Quantization Table Estimation

It is observed that if the histogram of DCT coefficients contain periodic patterns, then the coefficients are very likely to have been quantized with a step of this periodic [8]. These periodic artifacts are particularly visible in the Fourier domain as strong peaks in the mid and high frequencies. Therefore, the derivatives of the histogram power spectrum of DCT coefficients could be used to estimate the quantization table.

Fig. 1 shows the DCT coefficient histograms for a JPEG compressed image and the original uncompressed image. The histogram was calculated for the coefficients at DCT frequency $Q(6)$ (the fifth AC component). We can see that these two histograms are very similar, except that for JPEG compressed image (Fig. 1(a)) there are some peaks at the positions of multiple of q (here $q=4$). Note also that this type of period is not present in the uncompressed image (Fig. 1(b)).

The periodic peaks in the histogram are particularly visible in its power spectrum as strong peaks (Fig. 2). In Fig. 2, we show the power spectrum of the histograms of an uncompressed image and the JPEG compressed image. The histogram (H) of the DCT coefficients at position i is firstly calculated, and then the histogram power spectrum (P) is achieved using the Fast Fourier Transform.

The estimated power spectra of the two images are shown in Fig. 2(a) and Fig. 2(b), respectively. A combined view of those peaks provides us with a signature of the quantization step used. The second order derivative (S) of P is then low-pass filtered, and the positive values are eliminated. The reason is that if there is a local maximum $f(x)$ at x , then the derivatives $f'(x)=0$, $f''(x)<0$, and $f'''(x)$ is a local minimum. The number of negative local minimum of S is found to be equal to $(Q(i)-1)$. The second differentiable S and its filtered version are shown in Fig. 2(c) and Fig. 2(d), respectively.

We use the whole image to estimate quantization table. The procedure of the quantization table estimation is: (1) Calculating DCT coefficients of each 8×8 image block; (2) Calculating the power spectrum (P) of the histogram of DCT coefficients for each of the 64 frequencies; (3) Calculating the second derivative of P , and then low-pass filtering it; (4) Calculating the local minimum number (Num) of the filtered second derivative of P ; (4) the estimated quantization step of the DCT frequency is

estimated as $Num+1$.

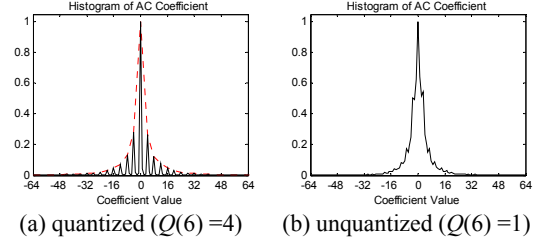


Fig. 1: Histogram of DCT coefficients

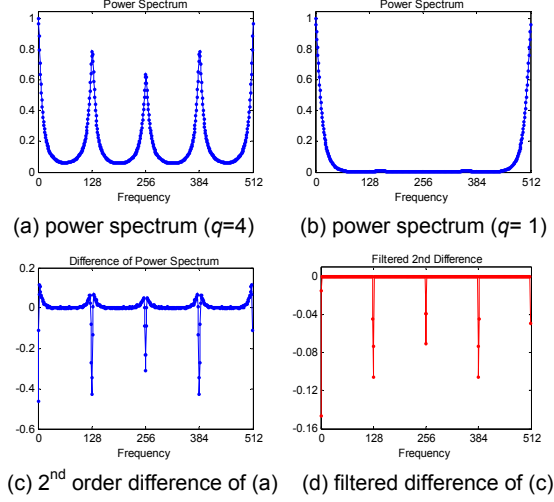


Fig. 2: Power spectrum of DCT coefficient histogram

Table 1 lists the correctly estimated table of the default finest quality setting of two digital cameras, where there are many different quantization steps.

Table 1: Quantization table of different cameras
(a) Nikon Coolpix5400 (b) Sony P10

1	1	1	1	1	2	2	2
1	1	1	1	1	2	2	2
1	1	1	1	2	2	3	2
1	1	1	1	2	3	3	2
1	1	1	2	3	4	4	3
1	1	2	3	3	4	5	4
2	3	3	3	4	5	5	4
3	4	4	4	4	4	4	4

1	1	1	1	1	2	3	3
1	1	1	1	1	3	3	3
1	1	1	1	2	3	3	3
1	1	1	1	3	4	4	3
1	1	2	3	3	5	5	4
1	2	3	3	4	5	6	5
2	3	4	4	5	6	6	5
4	5	5	5	6	5	5	5

Our proposed quantization table estimation algorithm is much faster than that of [8, 9, and 10]. Table 2 shows the results of quantization table estimation of our proposed method, compared with the optimization based method used in [8, 9]. The testing image is *Lena* with dimension 512×512 , quantized with JPEG factor from 100 to 50. These results were generated with program compiled by Visual C++ 6.0 on Dell Dimension 8250 PC (3060 MHz CPU, 512MB memory, and Windows XP operation system). From the results we can see that our method is much faster. The reason would be that for each given DCT coefficient, the algorithms in [8, 9] need to calculate blocking artifact for every possible $Q(i)$ based on the DCT coefficients of the whole image. On the contrary, our

algorithm only computes once. Furthermore, our algorithm can estimate arbitrary quantization table which is often adopted in different brand of digital cameras, whereas the algorithm proposed in [10] can only detect a standard compression factor, since it re-compress the image by a sequence of preset Q-factors. This step also makes the algorithm in [10] slower than our proposed one. On the other hand, the estimation errors of 64 quantization steps grow when quantization factor decreases. The reason would be that high frequency DCT coefficients would be all zero when quantized by large step. Therefore, we only use the first 32 DCT frequencies in blocking artifact estimation.

Table 2: Quantization table estimation time (ms)

Quality factor	100	90	80	70	60	50
MLE based method	15091	14957	14893	14950	14828	14737
Proposed method	241	227	228	225	222	228

2.3. Image Forensic Analysis based on Blocking Artifact Measure

Given a digital image, the blocking artifacts introduced during image compression could be used as a “natural authentication code” to check its integrity. We observed that when people forge image, they usually make use of JPEG images from different sources such as different digital cameras or by different manipulations. Such forgery usually makes the blocking artifact measurements inconsistent. Therefore, image forgeries could be done by finding the inconsistencies of blocking artifacts.

To check the integrity of an image, we first segment it into areas and then check the blocking artifact consistency of these segments. Suspicious area is selected for evaluation, the other areas are used to estimate the quantization table, and the *BAM* of the image is calculated based on the estimated table. If blocking artifact inconsistencies are detected, the image is deemed as suspicious. By detecting the inconsistency of the segments, we could possibly tell whether or not the image is from one simple shot of one camera.

3. EXPERIMENTAL RESULTS

Our testing images include two part: photos taken by several digital cameras (including Nikon Coolpix5400, Canon Ixus500, Sony P10, and Canon A85), and images from JPEG2000 testing set. The results shown in Fig. 3 validate our proposed algorithm in detecting digital forgeries. We created 500 forgeries randomly spliced from 500 untouched photos. The total image inconsistency measures of the original images and composed forgeries are show in Fig. 3. These results demonstrate that the propose measure can successfully distinguish digital forgeries from original images.

The blocking artifacts of every block would be useful to tell where the tampered areas are. In Fig. 4(a), a portrait patch taken from JPEG2000 testing image *Woman* (uncompressed) is extracted using Adobe PhotoShop and spliced into a landscape taken by Canon Ixus500. The blocking artifact measure of Fig. 4(a) is 2136.5, which is

much larger than the maximum of the untouched images shown in Fig. 3. The detected blocking artifacts (Fig. 4b) show two different values denoting the tampering areas.

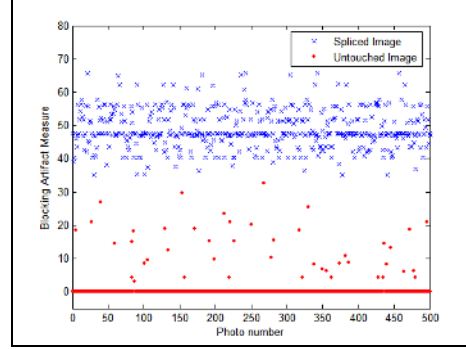


Fig. 3: Measures for tampered or authentic images



(a) tampered image



(b) blocking artifact detected ($BAM = 2136.5$)



(c) blocking artifact detected after JPEG recompression ($BAM = 97.1$)

Fig. 4: Blocking artifact inconsistencies detection

If the tampered image is further JPEG compressed, the primary quantization table could be estimated using method proposed in [11], and then it is used to measure the blocking artifact. The blocking artifact measure of the JPEG compressed version (using quantization factor 75) of Fig. 4(a) is 97.1. Fig. 4(c) is the result of artifact detected of the JPEG compressed version of Fig. 4(a).

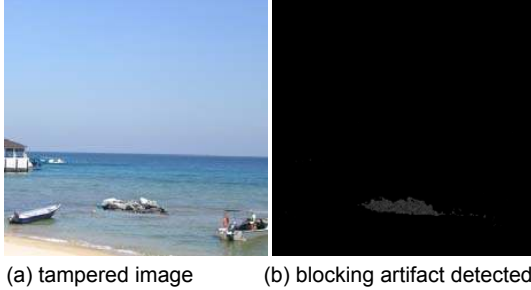


Fig. 5: Forgery image spliced from two images by the same camera (Nikon Coolpix5400) (BAM =45.4)

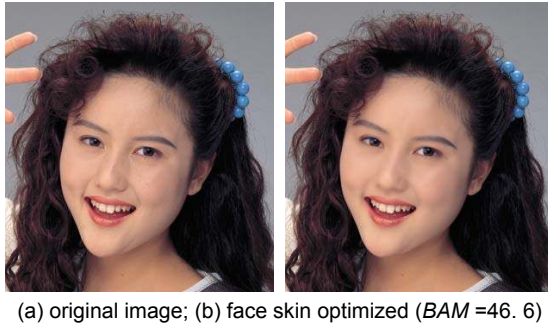


Fig. 6: Forgery of face skin optimization detection

The blocking artifact inconsistencies not only come from different quantization table, but also can be caused by block mismatching, resampling (Fig. 5), or local filtering (Fig. 6). Fig. 5 shows a forgery photo which was composed from two photos taken by the same cameras under same environment. A pile of stones was extracted from one photo and then spliced into another photo. Due to the resampling and block mismatching, the spliced area can be detected according to the different blocking artifacts. On the other hand, Fig. 6 shows a typical face skin optimization operation widely used by photographer. The face in Fig. 6(a) was polished using PhotoShop blur tool. The forgery shown in Fig. 6(b) can be detected by blocking artifact inconsistencies, which are shown in Fig.

6(c). The blocking artifact measure of Fig. 6(b) is 46.6, whereas that of Fig. 6(a) is only 5.9.

4. CONCLUSIONS AND FUTURE WORK

Detection of digital forgery without assistance of signature or watermarking is an emerging research topic. In this paper we propose a passive approach to detect digital forgeries by checking image quality inconsistencies based on blocking artifacts caused by JPEG compression. Experimental results validate the proposed approaches. Further work could be done on discovery of other image quality inconsistency measure.

REFERENCES

- [1] A. C. Popescu and H. Farid, "Exposing Digital Forgeries by Detecting Traces of Re-sampling", *IEEE Transactions on Signal Processing*, vol. 53, no. 2, pp.758-767, 2005.
- [2] F. Fridrich, D. Soukal, and J. Lukas, "Detection of Copy-Move Forgery in Digital Images", *Digital Forensic Research Workshop*, Cleveland, USA, Aug. 2003.
- [3] T. Ng, S.F. Chang, and Q. Sun, "Blind Detection of Photomontage using Higher Order Statistics", *IEEE International Symposium on Circuits and Systems*, Canada, May 2004.
- [4] A.C. Popescu and H. Farid, "Exposing Digital Forgeries in Color Filter Array Interpolated Images", *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3948-3959, 2005.
- [5] S. Lyu and H. Farid, "How Realistic is Photorealistic?", *IEEE Transaction on Signal Processing*, vol. 53, no. 2, pp.845-850, Feb. 2005.
- [6] M.K. Johnson and H. Farid, "Exposing Digital Forgeries by Detecting Inconsistencies in Lighting", *ACM Multimedia and Security Workshop*, New York, NY, 2005.
- [7] Z. Lin, R. Wang, X. Tang, and H.-Y. Shum, "Detecting Doctored Images Using Camera Response Normality and Consistency", *IEEE Conference on Computer Vision and Pattern Recognition*, pp.1087-1092, 2005.
- [8] J. Fridrich, M. Goljan, and R. Du, "Steganalysis based on JPEG Compatibility", *SPIE Multimedia Systems and Applications*, vol. 4518, Denver, CO, pp. 275-280, Aug. 2001.
- [9] Z. Fan and R. de Queiroz, "Identification of Bitmap Compression History: JPEG Detection and Quantizer Estimation", *IEEE Transaction of Image Processing*, vol. 12, pp. 230-235, Feb. 2003.
- [10] D. Fu, Y.Q. Shi, and W. Su, "A Generalized Benford's Law for JPEG Coefficients and Its Applications in Image Forensics", to appear in *SPIE* 2007.
- [11] J. Lukas and J. Fridrich, "Estimation of Primary Quantization Matrix in Double Compressed JPEG Images", *Digital Forensic Research Workshop*, Cleveland, Ohio, Aug. 2003.