JPEG Copy Paste Forgery Detection Using BAG Optimized for Complex Images

Dessalegn Atnafu AYALNEH*, Hyoung Joong KIM*, Yong Soo CHOI**

*CIST (Center for Information Security Technologies), Korea University

**Division of Liberal Arts & Teaching, SungKyul University

Dessalegn_atne@korea.ac.kr, khj-@korea.ac.kr, ciechoi72@gmail.com

***Abstract*— Image forgery detection is one of important activities of digital forensics. Forging an image has become very easy and visually confusing with the real one. Different features of an image can be used in passive forgery detection. Most of lossy compression methods demonstrate some distinct characteristics. JPEG images have a traceable zero valued DCT coefficients in the high frequency regions due to quantization. This appears as a square grid all over the image, known as Block Artifact Grid (BAG). In this paper the BAG based copy-paste forgery detection method is improved by changing the input DCT coefficients for Local Effect computation. The proposed method has shown a better performance especially for complex images.**

***Keywords*— Copy-paste forgery, JPEG, Block Artifact Grid, Local Effect**

I. Introduction

The development of computer technology has enabled digital image forgery extremely easy and leaves no visual clue of being tampered. This fact is deteriorating the historical trust of image evidences. In digital investigation, there are active and passive ways to authenticate integrity of digital images. Active techniques involve embedding of data during the time of recording or sending. Digital watermarks and digital signatures are widely used active image authentication techniques. However, it is not always feasible to embed a watermark or signature to an image. This limits the use of active techniques.

Passive authentication techniques are based on the analysis of different image attributes to detect inconsistencies that might be caused by forgery. Different features of image can be used for forgery detection [1], pixel statistics of natural image, lossy compression artifacts, the nature of image capturing devices, and the characteristics of interaction between physical object, light and camera and so on. This paper focuses on the lossy compression artifact based passive authentication technique for JPEG images.

II. JPEG Compression

JPEG is widely used lossy image compression technique which exploits the fact that human eye is less sensitive to changes of high frequency components. JPEG transformation functions operate block wise, i.e. after breaking the whole image into 8x8 pixel blocks.

JPEG encoder first transforms the pixel values into frequency domain using discrete cosine transformation (DCT). It transforms spatial domain to frequency domain as shown in eq(1). In a DCT matrix the high frequency components are located in the lower right side of the block. The next transformation is quantization, which is the only lossy part of JPEG compression. It is designed in such a way that it suppresses most of high frequency components. Quantization table decides which frequency components to suppress. The final step in JPEG is entropy coding, which is Huffman or arithmetic coding that follows the zigzag scanning and run-length encoding, which are reversible processes.

$$F(u,v) = \frac{1}{4} C(u)C(v) \sum_{x=1}^{8} \sum_{y=1}^{8} \{ f(x,y) \cos\frac{\pi(2x+1)u}{16} \cos\frac{\pi(2y+1)V}{16} \} \quad ..eq(1)$$

$$For\ u\ and\ v\ \in \{1,2,\ldots,8\}$$

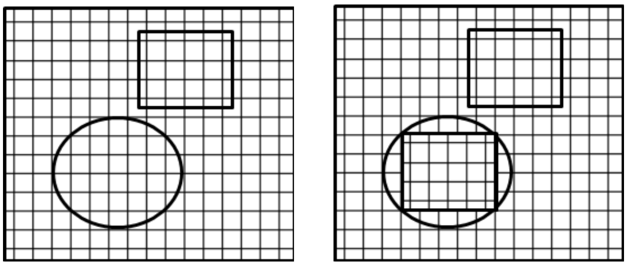
$$where$$

$$C(k) = \begin{cases} \frac{1}{\sqrt{2}}, for\ k = 0 \\ 1, otherwise \end{cases}$$

JPEG decoder does the inverse of the encoder transformations in a reverse order, entropy decoding, run-length decoding, reverse zigzag scan, inverse quantization and inverse DCT transform. Finally it puts the decompressed blocks in a right order to get the image.

III. Block Artifact Grid (BAG)

After JPEG compression, the image has zero DCT coefficients in the high frequency regions. In frequency domain each blocks appear to have zero high frequency components that are located near the right bottom of the DCT matrix. This leaves a noticeable trace of zero DCT coefficients that makes square grid of zero's all over JPEG compressed image. The square grid created due to information loss by JPEG compression is called Block Artifact Grid (BAG) [2]. This artifact is exploited to authenticate originality of JPEG images. For instance in intact JPEG compressed image all the BAG appear to be matched all over the image. The schematic diagram in fig 1.a. shows a matched BAG appears all over the image. Whereas, if portion of the image is copied and pasted else were, there is a 63/64 = 98.44% probability that the BAG in the duplicated area will not match with the rest of the image as shown in fig 1.b.

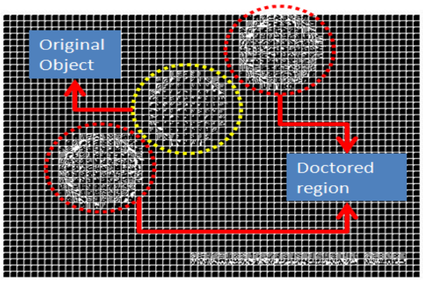


a. Original b. tampered

Figure 1. Fig 1. BAG before and after copy-paste forgery

In a copy-paste forged image blocks of the doctored region has higher entropy than the normal region of the image. It is caused due to the mismatched BAG. Fig 2.a. shows a sample image of three moons on a dark sky, but only the middle is real. Fig 2.b. shows plot of DCT coefficients of the forged image. The white square grid is inserted in order to visualise distribution of DCT coefficients. As we can see AC coefficients of the duplicated object has higher entropy than the original object. In other words, even if the duplicated object looks exactly like the original for human eyes, there is a noticeable change in magnitude of higher frequency DCT coefficients. This feature is exploited to detect forgery.

a) Doctored image



b) DCT coefficient plot

Figure 2. Copy-paste forged image DCT coefficient plot

IV. BAG DETECTION

Fig 2.b demonstrates how copy-paste forgery affects the pattern of DCT values. We need detection algorithm that can amplify the existing grid effect caused by the copy paste forgery. Li et al [2] proposed using Local Effect, the sum of square of the DCT coefficients at the bottom row and the right end side column and normalized by the square of DC coefficient. Eq (2) shows the definition of Local Effect (LE).

$$LE = \sqrt{\frac{\sum_{i=8||j=8} F^2(i,j)}{F^2(1,1)}} \dots\dots\dots eq(2)$$

$$where, F(i,j)\ is\ a\ DCT\ transform\ based\ on\ eq(1)$$

The LE computation above helps to detect the BAG location in JPEG image. For JPEG image the LE value gets minimizes when the BAG fits. If there is a forgery there will be a non-zero DCT coefficients on the bottom row and/or left end column. As a result LE value gets high and it implies which there is a BAG mismatch. LE value is computed by moving the 8x8 window all over the image and the BAG can be plotted. The area where we have mismatching grid is possibly tampered region. Dijana et al [3] extended the application of BAG mismatch detection in different types of forgery. They used it to detect spliced images, and when edges of the forged region smoothen by averaging values of neighbouring pixels. The proposed detection approach is demonstrated on forged image shown above in fig2.a. For convenience the matching grid is replaced by a single dot on the upper left corner, and only the mismatched BAG represented by grid as shown in fig 3.

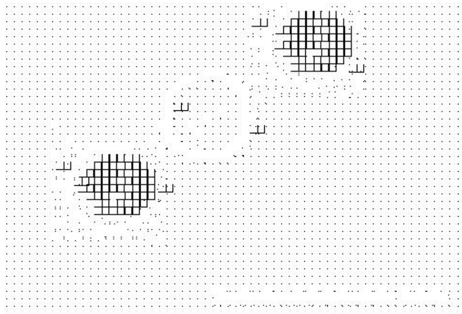
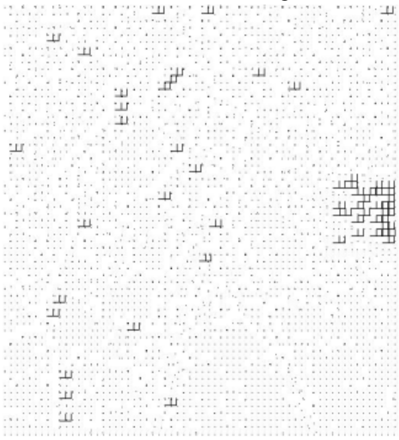


Figure 3. The BAG plot for a doctored image in fig 2.a.

This approach detects forgery very well on images with smooth background. In case of complex images, it is possible to have larger magnitude of high frequency DCT components located on the right bottom region of DCT coefficients. As result LE computation indicates a BAG mismatch detected even though there is no forgery. The camera man image in fig 4.a. is copy-paste forged to duplicate the tower on the right side. As we can see on Fig 4.b. even if the algorithm has detected the forged area, it also has shown some false positive on the intact regions.

a. Doctored image

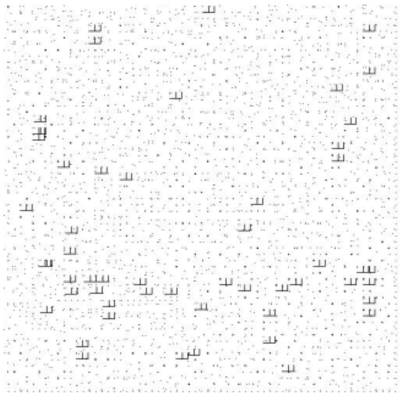


b. BAG plot

Figure 4. Forgery detection of cameraman image

This approach totally fails to detect forgery in very complex images. Fig 5.a. shows a forged image of tank in a desert, i.e. in the picture the lower tank is forged. The output of the detection algorithm on fig 5.b. shows that there are BAG mismatch all over the image. In this particular example the algorithm has failed to detect the forgery.

a. Doctored image



b. BAG plot

Figure 5. Forgery detection of Tank image

V. OUR PROPOSED METHOD

In the previous method the authors considered a window with all zeroes except last column and last row, as shown on fig 6.1. As a result, the algorithm output has false positive on complex images. It even fails to detect forgery in some cases. One of reasons can be the way the LE is computed. In JPEG compressed image the DCT coefficients in the lower anti triangular matrix usually have high probability of being zero. This is related to the JPEG quantization table design where the quantization values in the lower anti-triangular matrix are higher to suppress those frequency components. In this paper a window shown in fig 6.b is proposed for LE computation to improve the BAG mismatch detection algorithm.

1	0	0	0	0	0	0	1
0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	1
0	0	0	0	0	0	0	1
1	1	1	1	1	1	1	1

a. Old Window (W1)

1	0	0	0	0	0	0	1
0	0	0	0	0	0	1	1
0	0	0	0	0	1	1	1
0	0	0	0	1	1	1	1
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1

b. New Window (W2)

Figure 6. Windows used to consider portion of 8x8 DCT coefficients

Therefore in the proposed approach all DCT coefficients in the lower anti-triangular matrix are considered in LE computation. Eq (3) shows the LE computation using the window W2 in fig 6.b.

$$LE = \sqrt{\frac{\sum_{i=1}^{8}\sum_{j=1}^{8}(F(i,j)W_{ij})^2}{F(1,1)^2}} \ldots\ldots\ldots eq(3)$$

$$where, F(i,j)\ is\ a\ DCT\ transform\ based\ on\ eq(1),$$
$$and\ W_2\ is\ matrix\ shown\ in\ fig\ 6.b.$$

VI. RESULT ANALYSIS

The proposed approach is tested with images of different complexity in order to compare the performance with the previous method. Fig 7, 8 and 9 shows the experimental result of the proposed technique applied to tampered moon, cameraman and tank images respectively. Both methods perform very well on smooth image as shown in fig 3 and fig 7. As the complexity of the image increases the previous method detects the forgery with some false positive result around edges as shown in fig 4. However, the proposed technique shows much better result as shown in fig 8. In very complex images like Tank the previous method has failed to detect the forged area with a high false positive rate all over the image as shown in fig 5. However, the proposed technique is able to detect the forged region with some false positive rate (fig 9). As we can see from the experimental results image complexity results false positive due to the possibility of non-zero DCT coefficients on the bottom row and left end column of the block. Considering the DCT values on the lower anti-triangular matrix area in LE computation gives a better estimate of BAG mismatch.

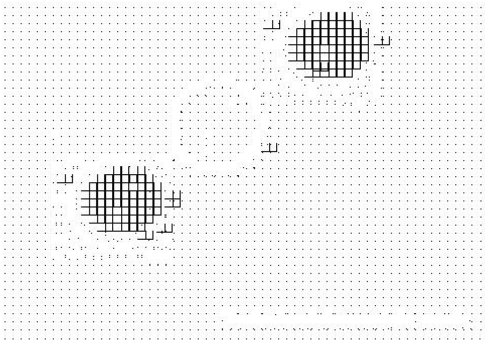


Figure 7. BAG mismatch detection of moon in figure 2.a using proposed method

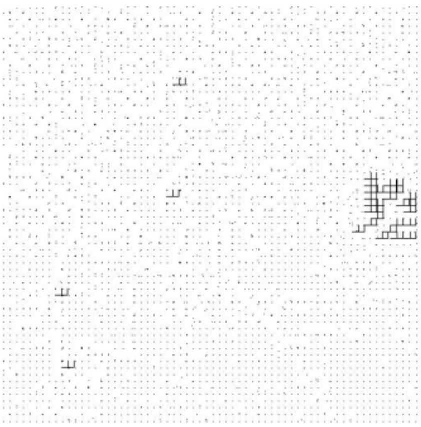


Figure 8. BAG mismatch detection of cameraman in figure 4.a using proposed method

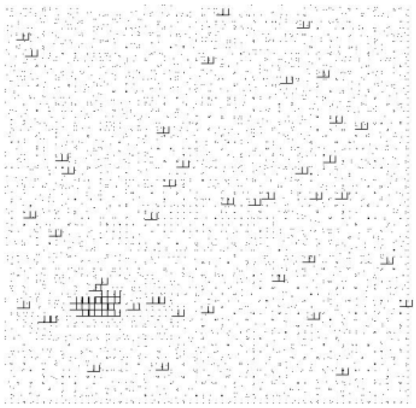


Figure 9. BAG mismatch detection of moon in figure 5.a using proposed method

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (No. 2012015587) and, Ministry of Culture, Sports and Tourism(MCST) and Korea Creative Content Agency(KOCCA) in the Culture Technology(CT) Research & Development Program.(No. R2012050022).

REFERENCE

[1] H. Farid, "A Survey of Image Forgery Detection", *IEEE signal processing magazine,* 2009.

[2] W. Li, Y. Yuan, N. Yu, "Detecting copy-paste forgery of JPEG via block atrifact grid extraction", *MOE-Microsoft Key Laboratory of Multimedia Computing and Communication,* 2007

[3] D. Tralic, J. Petrovic, S. Grgic, "JPEG Image Tampering Detection Using Blocking Artifacts", *19th International Conference on Systems, Signals and Image Processing (IWSSIP)*, p. 5-8

[4] W. Li, Y. Yuan, N. Yu, "Passive detection of doctored JPEG image via block artifact grid extraction", *journal of signal processing*, 2009, Pages 1821-1829

Bibliography

Ayalneh Dessalegn Atnafu received the B.S. degree in Electrical Engineering from Defence University College, Debre Zeit, Ethiopia, in 2003 and the MS degree in Electrical and Computer Engineering from Addis Ababa University, Addis Ababa, Ethiopia in 2008. Currently, he is working toward the Ph.D. degree in Multimedia Security Laboratory, Graduate School of Information Security, Korea University, Seoul, Republic of Korea, since 2012. His research interest includes multimedia forensics, data hiding, image processing, and security management.

Hyoung Joong Kim received the B.S., M.S., and Ph.D. degrees from Seoul National University, Seoul, in 1978, 1986, and 1989, respectively. He joined the faculty of the Department of Control and Instrumentation Engineering, Kangwon National University, Korea, in 1989. Since 2006, he has been a Professor at the Center of Information Security and Technology, Graduate School of Information and Security, Korea University, Seoul. His research interests include parallel and distributed computing, multimedia computing, and multimedia security. He has contributed to MPEG standardization for digital item adaptation, file format, symbolic music

representation, and multimedia application format, with more than ten contributions and the same number of patents. In addition, he has filed many patents and published more than 30 reviewed papers in international journals including IEEE and ACM, and two peer reviewed book chapters. He was the prime investigator of the national projects during 1997–2005 developing interactive and personalized digital television. He has served as Guest Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY and EURASIP JOURNAL OF ADVANCES IN SIGNAL PROCESSING, and has been Technical Program Chair of many international conferences including International Workshop on Digital Watermarking. He is a Vice Editor-in-Chief of the LNCS TRANSACTIONS ON DATA HIDING AND MULTIMEDIA SECURITY, Associate Editor of well-known international journals, and Editor of many Lecture Notes in Computer Science series Prof. Kim is a member of ACM and several Korean academic societies.

YongSoo Choi received the B.S., M.S. and Ph.D. degrees in the Department of Instrumentation and Control Engineering from the Kangwon National University, Korea, in 1998, 2000 and 2006, respectively. From 2006 to 2007, he was a research professor with the Center for Technology Fusion in Construction, YonSei University, Korea. From 2007 to 2013, he was a research professor with the Brain Korea 21 of Ubiquitous Information Security, Korea University, Korea. He is currently a assistant professor with the Sungkyul Universtity, Korea. From 2013 to now, he was a Delegate of Korea for ISO/IEC JTC1/SC29. His research interests include multimedia signal processing, digital watermarking, steganography and multimedia hashing. Dr. Choi is a member of the IEEK Computer Society. He is currently an Editor in Chief of Journal of the Institute of Electronics Engineers of Korea, the Section of Computer and Information.