 ISBN 978-3-200-02328-4

# JPEG IMAGE TAMPERING DETECTION USING BLOCKING ARTIFACTS

*Dijana Tralic, Juraj Petrovic, Sonja Grgic*

University of Zagreb, Faculty of Electrical Engineering and Computing
Unska 3, HR-10000 Zagreb, Croatia
E-mail: *dijana.tralic@fer.hr*

**ABSTRACT**

Image forgery is nowadays widely used as digital images are easy to manipulate due to high availability of powerful image processing tools. It is possible to add or remove objects from an image without leaving any visible traces of tampering. This paper describes a method for detection of copy-paste manipulation on JPEG digital images. It is a type of image forgery in which a part of the image is copied to another location in the image with the intent to cover or add an important image object. The detection method was implemented through extracting and analyzing blocking artifact grids (BAGs), introduced by block processing during JPEG compression. Analysis was based on fact that BAGs usually mismatch after performing copy-paste operations. Proposed method was demonstrated on two doctored images.

***Index Terms***— doctored images, image tampering, JPEG images, copy-paste forgery, blocking artifacts

## 1. INTRODUCTION

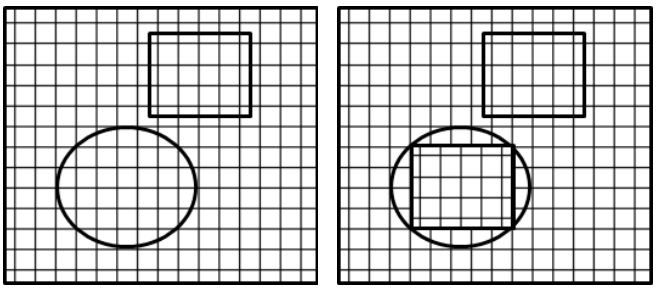
Modern image processing tools have made manipulation of digital images easier to carry out and harder to uncover. Many doctored images are used in everyday life, but development of new techniques enabled introduction of more sophisticated methods for their detection.

Image authentication methods can generally be classified as active or passive. Active methods involve embedding of some information into an image when it is archived, and include digital watermarks [1,2] and signatures. Image tampering usually destroys or modifies this embedded information, so it can be easily detected. Main issue with this approach is its application in modern devices which usually do not contain any module for digital watermarking or signatures. Passive methods on the other hand involve checking the integrity of an image, and include analysis of image statistics [3], trails detection [4], consistency verification [5] and rationally judgment [6]. Every detection technique is effective for some kind of tampering attempts, but tampering an image is still easier to perform than detecting a tampered image.

JPEG standard is a widely used image format which utilizes a lossy type of compression. There are many different techniques for detection of JPEG image tampering, such as double quantization effect hidden among the DCT coefficients [7] or checking the uniformity of quantization remainders [8].

One of properties of JPEG standard is that it divides an image into 8 by 8 pixel blocks to calculate DCT coefficients and perform quantization. This process of breaking an image into blocks introduces horizontal and vertical breaks into image, which are called blocking artifact grid (BAG). In copy-paste tampering, copied image parts are placed at proper place to hide or add an object, so the BAG in the original image and the BAG in the target image are usually mismatched.

Figure 1 shows an example of detecting a copy-paste forgery by analyzing the blocking artifacts. It is possible to see that the original image has properly aligned BAG. After copying a rectangle and pasting it inside of the oval, BAG mismatch is visible if the copied area is compared to the neighbored area.



(a) Original image (b) Doctored image

**Fig. 1.** Example of BAG mismatch after copy-paste forgery

This paper is organized as follows. In Section 2 the blocking artifacts effect in JPEG standard is described, and a method for extraction of blocking artifact grid is proposed. Section 3 draws some experimental results of copy-paste forgery detection. Conclusion and future work are highlighted in Section 4.

## 2. BLOCKING ARTIFACTS

The block based transform coding, as used in JPEG standard, causes accuracy of blocking artifacts along block boundaries [9]. They are a result of loss of transform coefficients in the process of independent quantization of each block. Those blocking artifacts can be extracted from an image to serve as a base for detection of copy-paste forgery on an image.

### 2.1. Blocking artifact grid extraction

First step in the detection of copy-paste forgery is to extract BAG of an image. In JPEG images, after quantization process, values of high frequency AC coefficients of a DCT block are usually equal to zero. If all DCT blocks are properly aligned (there was no copy-pasting forgery to cause BAG mismatching), high frequency coefficients will be equal to zero. Opposite to that, if BAG mismatches exist, the AC coefficients on higher frequencies will contain some values. Another case when high frequency AC coefficients will not be equal to zero is appearance of areas that consists of complex textures. However, in that case, AC coefficients will be much smaller than those found in case of BAG mismatching.

Location of blocking artifacts can be obtained by calculating local effect [10] of 8 by 8 pixel window

$$LE = \sqrt{\frac{\sum_{i=8 \| j=8} S_{ij}^2}{S_{11}^2}}, \quad (1)$$

where $S_{ij}$ marks AC coefficients of pixels in selected window. Local effect is defined by values of AC coefficients in right column and bottom row. AC coefficients can be obtained by 2D DCT

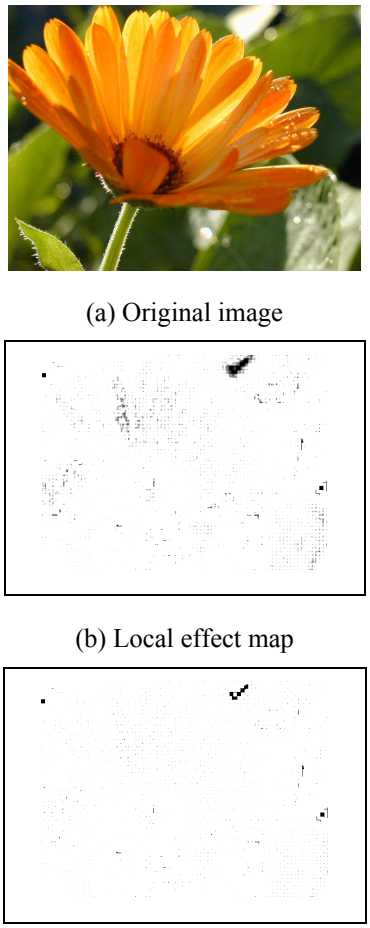
$$S_{uv} = \alpha_u \alpha_v \sum_{i=1}^{8} \sum_{j=1}^{8} s_{ij} \cos\frac{\pi(2i+1)u}{16} \cos\frac{\pi(2j+1)v}{16}, \quad (2)$$

where

$$\alpha_n = \begin{cases} \frac{1}{\sqrt{8}}, n = 1 \\ \frac{1}{2}, n \neq 1 \end{cases}, \quad (3)$$

and $s_{ij}$ marks luminance of a pixel.

BAG extraction is accomplished by sliding an 8 by 8 pixel window across the whole image, and calculating local effects for every window. Figure 2 shows an example of BAG extraction on an image. It is possible to see that local effect map, shown on figure 2(b), contains dark pixels on location with small local effect, and vice versa. Pixels on the blocks' borders have smaller value and they form BAG. After the calculation of local effect map, BAG was extracted by leaving only the local minimal value for every 8 by 8 pixel window of the image, as shown on Figure 2(c).



(a) Original image

(b) Local effect map

(c) Local minimal values map

**Fig. 2.** BAG extraction example

Similar detection method was used in paper by Li, Yuan, and Yu [10] where it effectively detected copy-paste forgery whether the copied area was taken from the same image or not. In our approach, testing was additionally performed on some images which were processed with aim to hide borders of the copied area.

### 2.2. Analysis of grid mismatches

Analysis of grid mismatches was performed with few simple searching methods, using the map of local minimal values. First step was marking all points that belong to the grid of the initial image. This processing procedure was based on the assumption that BAG of copied area must be mismatched when compared to the grid of the initial image. In most cases this assumption will be correct so it is possible to ignore all points that belong to BAG of the original image. Assumption is incorrect only in case when the copied area was placed on such location that its BAG remains aligned with BAG of the image (the probability of getting such situation is equal to 1/64).

The next step of the analysis was detecting a new, shifted grid that belongs to the copied area. The search was

performed among the remaining local minimal value points. This step also includes discarding all block areas that appear as black areas on the map of local minimal values. Those areas are the result of homogeneous surfaces in an image because in that case most of DCT coefficients have the same LE value.

Detection of shifted grid was finally performed by the following algorithm. First, the search for shifted blocks was conducted by detecting 4 local minimum points that form vertices of a square with a side length of 8 pixels. Every copied area is assumed to have at least one such segment. In other words it is assumed that the copied area is not smaller than a 16 by 16 pixel block. If any such square artifact was found, the next task was to detect all additional artifacts in that area appearing in one of two forms: "|_" if they consist of 3 points and "|" if they consist only of two points at a distance of 8 pixels. This search was repeated until no more structures were found at distance of 8 pixels in horizontal or vertical axes of any previously found artifact. Also, to increase the probability of identifying the pasted region of the image, another search was performed identifying all independent "|_" and "|" structures.

The detected blocks and structures are suspected to form a shifted grid since they indicate a significant mismatch with the initial grid.

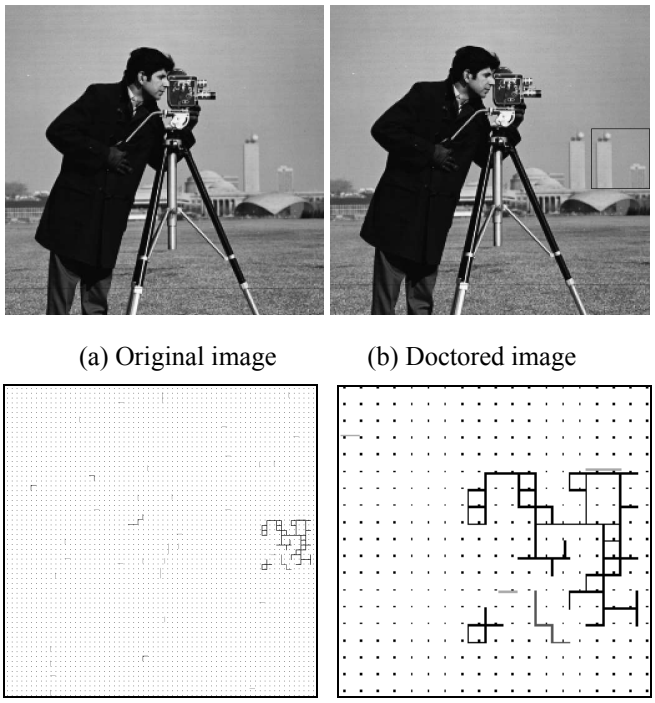
## 3. EXPERIMENTAL RESULTS

Extraction and analysis of BAG will now be presented on two examples. Figure 3(a) presents an original image of a cameraman and Figure 3(b) shows a doctored image which was created by coping and pasting the marked area. The copied area was placed in such position where it could easily cheat human eye. In this example copied area was taken from the same image, but detection would be equally effective if copied area was taken from a different JPEG image.

After the BAG extraction and analysis, copy-paste forgery was detected because of the mismatch of blocking artifacts in that area. Figure 3(c) shows detection results where it is possible to notice a significant BAG mismatch area at right side of image. Areas that do not contain at least one block can be discarded from further analysis.

Blocking artifact grid of an initial image was marked with sequence of points that are located at distance of 8 pixels (because of using 8 by 8 blocks in DCT compression). The area ofinterest is presented enlarged on Figure 3(d) in order to make better visual effect of blocking mismatch. It is visible that BAG of copied area does not match the initial grid of the image. Lines that form BAG of the copied area are not aligned with the BAG of the rest of the image.

Percentage of correct detection was used as a measure for indication of deviation of BAG on copied area and original image. In this example, 70.51% of copied area was successfully detected, and size of false positive block detection was 0.3419% of the image.



(a) Original image (b) Doctored image

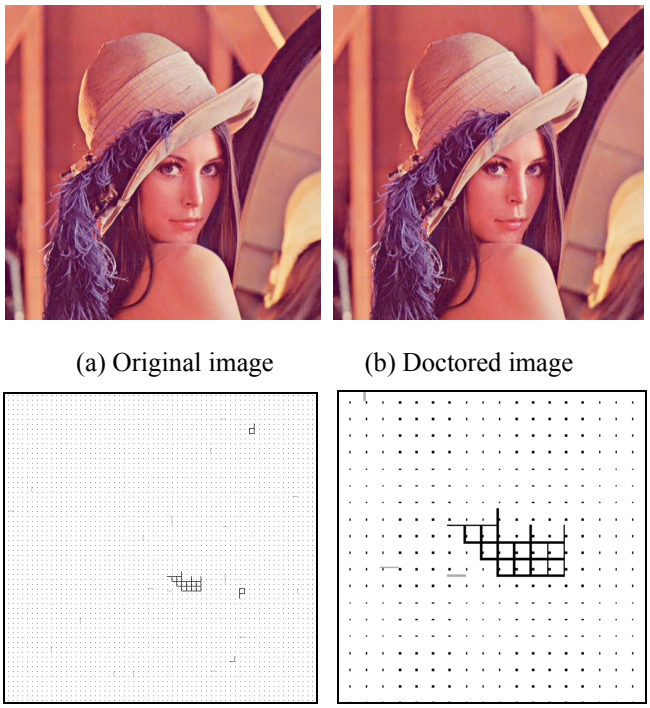
(c) Detected forgery (d) BAG mismatch

**Fig. 3.** Example of copy-paste forgery detection

Figure 4 shows another example of copy-paste forgery on an RGB image. Doctored image, visible on Figure 4(b), was created by copying a segment of Lenna's nose and pasting it slightly higher in the picture, thereby making it look smaller. This kind of image forgery is very difficult to detect by visually inspecting the doctored image, especially since borders of the copied area, after the copy-paste forgery, were processed by averaging values of neighboring pixels. That process was performed by averaging values of 2 pixels from both sides using values of their neighbors. Result of this averaging process was smoothing the borders to hide rough transitions from copied area to original area of image.

Results of the BAG extraction are shown on Figure 4(c), where it is possible to notice the mismatch of blocking artifacts exists. Although, due to the complexity of the image, other detected areas exist as well, they are all significantly smaller than the main mismatch area, even though the copy-pasted part of the image was quite small itself. Figure 4(d) presents the zoomed BAG mismatch area to allow better view. It is clearly visible that the BAG of the copied area does not align with the BAG of the initial image.

Percentage of correct detection for this example was around 74.07% of copied area, and percentage of false positive block detection was 0.293% of the image. This example demonstrates how the described approach can detect copy-paste forgery even if borders were smoothed, because processing an image to hide borders of copied area did not affect BAG of whole copied area.



(a) Original image (b) Doctored image

(c) Detected forgery (d) BAG mismatch

**Fig. 4.** Example of copy-paste forgery detection with borders smoothing

## 4. CONCLUSION

Today, detection of doctored images has important role due to many powerful image processing techniques that can be used for creation of such images. Passive image forensics presents a possible solution for detection of some types of image forgeries. Properties of JPEG images, such as the blocking artifacts introduced during compression, can be used as one of indicators of copy-paste forgery.

Extraction and analysis of the BAG mismatch can be used as an indication of image forgery whether copied area was taken from the same image or not. Also, this approach works efficiently for images where borders of copied area were smoothed by averaging values of neighboring pixels. Suggested method was successfully tested for different kind of copy-paste problems. In all tested cases, this approach allowed effective detection of copied areas on doctored images. Another advantage of this method is its independence of the size of the copied area.

Future work will include testing approach for similar problems such as hiding objects by painting some image area. Also, more sophisticate measure of deviation of BAG on copied area and original image will be developed.

## 5. ACKNOWLEDGMENT

The work described in this paper was conducted under the research projects: "Picture Quality Management in Digital Video Broadcasting" (036-0361630-1635) and "Complex System Modelling" (036-0362214-1987), supported by the Ministry of Science, Education and Sports of the Republic of Croatia.

## 6. REFERENCES

[1] M. Wu and B. Liu, *Watermarking for image authentication*, in Proc. IEEE International Conference on Image Processing, vol. 2, pp. 437–441, Chicago, Ill, USA, October 1998

[2] 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. on Information Forensics and Security, vol. 1, no. 3, pp. 330–341, September 2006

[3] W. Li and B. Wang, *A Statistical Analysis on Differential Signals for Noise Level Estimation*, Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, China, pp. 2150–2153, August 2007

[4] A. C. Popescu and H. Farid, *Statistical tools for digital forensics*, The 6th International Workshop on Information Hiding, Toronto, Canada, pp. 128–147, 2004

[5] 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

[6] M. K. Johnson and H. Farid, *Exposing digital forgeries by detecting inconsistencies in lighting*, ACM Multimedia and Security Workshop, New York, USA, pp. 1–10, 2005

[7] J. He, Z. Lin, L. Wang, and X. Tang, *Detecting Doctored JPEG Images Via DCT Coefficient Analysis*, Lecture Notes in Computer Science, vol. 3953, pp. 423–435, Berlin, Germany, 2006

[8] S. Ye, Q. Sun, and E.C. Chang, *Detecting Digital Image Forgeries by Measuring Inconsistencies of blocking artifact*, IEEE International Conference on Multimedia and Expo, Beijing, China, pp. 12–15, 2007

[9] W. Li, N. Yu, and Y. Yuan, *Doctored JPEG image detection*, 2008 IEEE International Conference on Multimedia and Expo, pp. 253–256, August 2008

[10] W. Li, Y. Yuan, and N. Yu, *Detecting Copy-Paste Forgery of JPEG Image via Block Artifact Grid Extraction*, 2008 International Workshop on Local and Non-Local Approximation in Image Processing, Lausanne, Switzerland, August, 2008