

Crop Detection Through Blocking Artefacts Analysis

Bruna A.R, Messina G, Battiato S.
{bruna, gmessina, battiato}@dmi.unict.it

Image Processing Laboratory
Department of Mathematics and Computer Science
University of Catania
Viale A. Doria 6 - 95125 Catania, Italia
<http://iplab.dmi.unict.it>

Abstract. In this paper we propose a new method to detect cropped images by analyzing the blocking artefacts produced by a previous block based compression techniques such as JPEG and MPEG family that are the most used compression standards for still images and video sequences. It is useful for image forgery detection, in particular when an image has been cropped. The proposed solution is very fast compared to the previous art and the experimental results show that it is quite reliable also when the compression ratio is low, i.e. the blocking artefact is not visible.

Keywords: crop and paste technique, DCT blocking artefacts analysis, tampered images, image forensic.

1 Introduction

In the last years, the number of forged images has drastically increased due to the spread of image capture devices, especially mobile phones, and the availability of image processing software. Copy and paste is the simplest and most used technique to counterfeit images. It can be used to obtain a completely new image by cropping the interest part or to cover unwanted details. In image forensics it is important to understand (without any doubts) if an image has been modified after the acquisition process.

There are two methodologies to detect tampered images: active protection methods and passive detection methods [1]. The active protection methods make use of a signature inserted in the image [2]. If the signature is no more detectable, the image has been tampered. These techniques are used basically to assess ownership for artworks and/or relative copyrights. Passive detection methods make use of ad-hoc image analysis procedures to detect forgeries. Usually the presence of peculiar artefacts is properly investigated and, in case of anomalies, the image is supposed to be counterfeit. Several algorithms exist in literature as reported in a recent survey [3]. Among others, a lot of methods in the field consider the possibility to exploit the statistical distribution of DCT coefficients in order to reveal the irregularities due to the presence of a superimposed signal over the original one [4, 5, 6, 7]. The usage of

Discrete Cosine Transform (DCT) artefacts analysis have a further advantage due to the fact, that is the most used compression technique; JPEG [8] for still images and MPEG compression family [9] for video sequences make use of block based DCT data compression (usually 8x8 pixel size non-overlapping windows).

While there are a lot of algorithms in literature for the estimation of the quantization (and compression) history [5, 6], there are only a few approaches for cropping detection [7]. In this paper a pipeline is suggested aiming to merge both techniques in order to obtain a more reliable system. In fact, blocking artefacts analysis works well when the image is aligned to the block boundary. But, in case the image has been cropped, this assumption is no more valid and the detection may fail. In the proposed system the quantization detection block is preceded by a cropping detection in order to align the image to the block boundary. It allows to increase the reliability of the detection and to better understand if only some parts of the image are tampered.

In Li et al. [1] the grid extraction is realized by extrapolating the Block Artefact Grid (BAG) embedded in the image where block artefact appears, i.e. the grid corresponding to the blocks boundaries. The authors introduce a measure of blockiness just considering the ratio between the sum of AC components of the first row (and column) with respect to the DC coefficient in the DCT domain. One of the main drawbacks of the method is related to the fact that it requires to compute 8x8 pixels DCT again (in a dense way) over the image under detection, just to locate properly the correct alignment. Also the detection of tampered regions corresponding to misaligned grid is demanded to a visual inspection of the resulting filtering operation without a clear and objective measure. The same authors propose in [7] an interesting approach based on spatial consideration devoted to locate the BAG just combining together a series of derivative and non-linear filters to isolate blockiness avoiding the influence of textures or strong edges present in the input image. Unfortunately, both the techniques were not properly evaluated just considering a proper dataset (high variability with respect to resolution size) and a sufficient number of misalignments cropping with respect to the 8x8 grid. Also an exhaustive comparison just considering the overall range of JPEG compression factors is lacking.

As well described in [3, 10] the new emerging fields of Digital Forensics require to provide common benchmarks and datasets that are needed for fair comparisons among the numerous proposed techniques and algorithms published in the field.

The rest of the paper is organized as follows. In Section 2 the proposed technique is described; the next Section reports a series of experiments devoted to assess the effectiveness of the method. Finally, some conclusions are given together with a few hints for the future work.

2 Proposed System

The proposed solution can be used as stand-alone algorithm to detect crop operations or it can be inserted in a typical advanced pipeline for complex tampering detection using compression artefacts analysis. The proposed solution aimed to handle images without any further compression. In this case, in fact, the further compression may

introduce blocking artefact that may deceive the algorithm. In Figure 1 an example aiming to detect the camera model from an image, after a copy/paste and re-encoding counterfeit process, is shown. In this case, the algorithms described in [5] and [6] can be used for the quantization detection, while the study proposed in [11] can be used for the signature detection block.

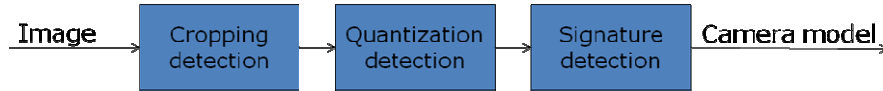


Fig.1: Block based schema of the pipeline used to retrieve the camera model from an image.

2.1 Algorithm description

The DCT codec-engines (e.g., JPEG, MPEG, etc.) typically apply a quantization step in the transform domain just considering non-overlapping blocks of the input data. Such quantization is usually achieved by a quantization table useful to differentiate the levels of quantization adapting its behavior to each DCT basis. The JPEG standard allows to use different quantization factors for each of the bi-dimensional DCT coefficients. Usually standard quantization tables are used and a single multiplicative factor is applied to modify the compression ratio [12, 13], obtaining different quality levels. As the tables are included into the image file, they are also customizable as proved by some commercial codec solutions that exploit proprietary tables. Images compressed by DCT codec-engines are affected by annoying blocking artefacts that usually appear like a regular grid superimposed to the signal. In the following, we discuss a simple example based on the Lena image. The picture has been compressed using the *cjpeg* [12] software with a properly managed compression ratio, obtained modifying the quantization tables through the variation of the quality parameter in the range {10, 90} (see Figure 2).

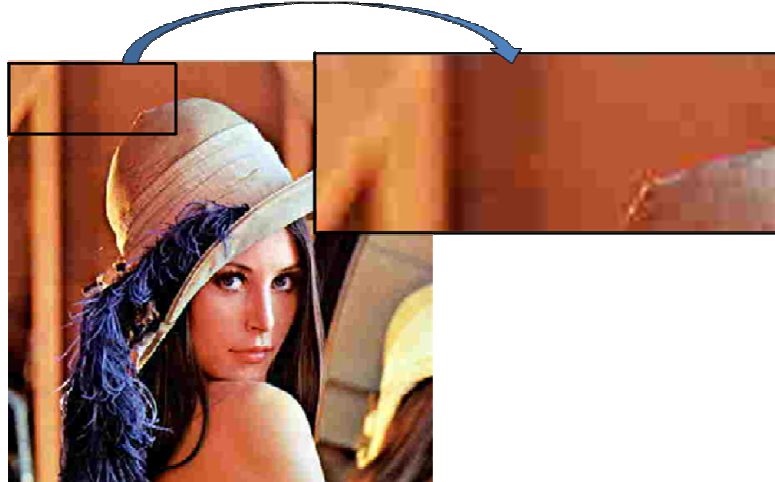


Fig.2: Blocking artefact example in a JPEG compressed image (quality factor = 40).

It is an annoying artefact visible especially in flat regions. It is also regular, since it depends on the quantization of the DCT coefficients of every 8x8 blocks. Unfortunately, this kind of artefact is not simple to be characterized (i.e., detectable) in the Fourier domain, since image content and the effect of the quantization step of the encoding pipeline mask the regular pattern, as shown in Figure 3.

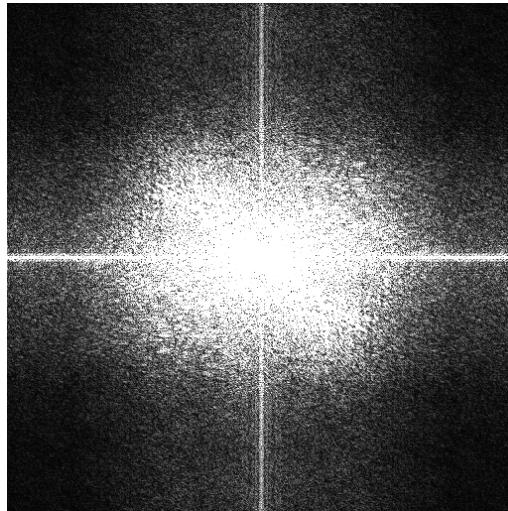


Fig.3: Results of the visualization of the Fourier spectrum applied to the compressed Lena image shown in Figure 2.

We established to work directly in the spatial domain and, in particular, in the luminance component. The blocking artefact is basically a discrepancy in all the borders between adjacent blocks. It is regularly spaced (8x8 for JPEG and MPEG) and it also affects the image in only two perpendicular directions (horizontal and vertical if the image has not been rotated).

The straightforward way to detect such artefact exploits a derivative filter along the horizontal and vertical direction. The proposed strategy could be easily generalized to consider all possible malicious rotation of the cropped image, just iterating the process at different rotation angles. In Figure 4 the overall schema of the proposed algorithm is depicted.

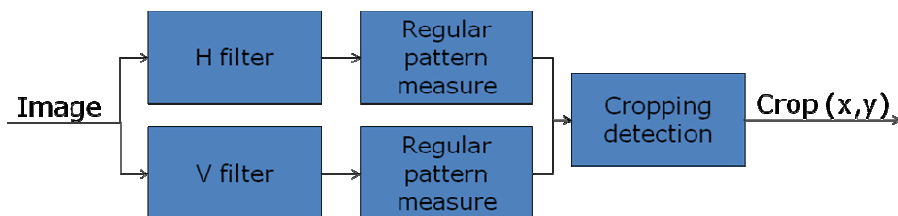


Fig.4: Block based schema of the cropping detection algorithm.

The blocks “*H filter*” and “*V filter*” are derivative filters. Basically they are High Pass Filters (HPF) usually used to isolate image contours. An example is the Sobel filter, with the following basic kernel:

$$H = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix}; \quad V = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix};$$

Fig.5: Sobel filter masks.

These filters are able to detect textures, as shown in the image below.



Fig.6: Effect of the Sobel filter (3x3 kernel size) applied to the Lena image.

It is very useful to retrieve textures of the image, but the blocking artefact effect is also masked. In order to detect only regular pattern and discard real edges, a very long taps directional filter has been used. It was obtained by properly expanding the following 3x3 filters along the horizontal or vertical direction:

$$H = \begin{bmatrix} 1 & 1 & 1 \\ -1 & -1 & -1 \\ 0 & 0 & 0 \end{bmatrix}; \quad V = \begin{bmatrix} 1 & -1 & 0 \\ 1 & -1 & 0 \\ 1 & -1 & 0 \end{bmatrix};$$

Bigger is the number of taps, better are the results, although computational time also increase. In Figure 7 is shown the result of a long directional filters with different kernel size.



Fig.7: 30 taps directional HPF applied to the Lena image. Borders are not considered (thus the vertical size in the left image and the horizontal size in the right images are less than the original size).

We define the *Regular Pattern Measure* (RPM) that computes a measure of the blockiness effect as defined in the following. Let I a $M \times N$ pixel size image and I^H, I^V the corresponding filtered images obtained by applying a directional HPF as above. For sake of simplicity let suppose to have serialized the image, by simple scan line ordering of the corresponding rows and columns just obtaining the vector $I^{H'}, I^{V'}$. The RPM values for both directions is obtained as:

$$RPM_H(i) = \sum_{j=0}^{\text{floor}(N/8)} I^{H'}(8 \cdot j + i); \quad i = 1, \dots, 7;$$

$$RPM_V(i) = \sum_{j=0}^{\text{floor}(M/8)} I^{V'}(8 \cdot j + i); \quad i = 1, \dots, 7;$$

Experiments have shown that both the RPM_H and RPM_V measures allow discriminating, in a very robust way (e.g., with respect to the main content of the image), the periodicity of the underlying cropping positions. Such values can be extracted by considering a simple order statistic criterion (e.g., the maximum). Figures 8 and 9 show the plot of the two RPM measures, in case of no cropping (e.g., blocking artefact starts with the pixel [1,1]) and in case of malicious cropping at position [6, 5].

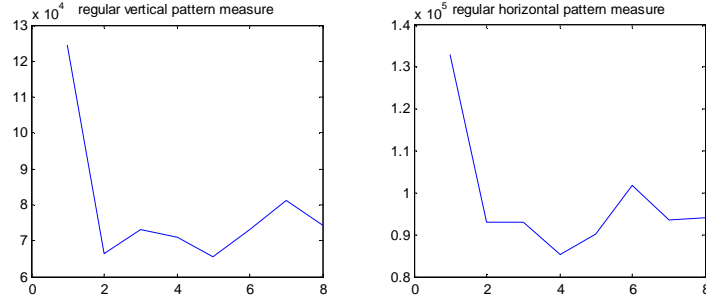


Fig.8: RPM measure without cropping. The blocking artefact starts with the pixel [1,1].

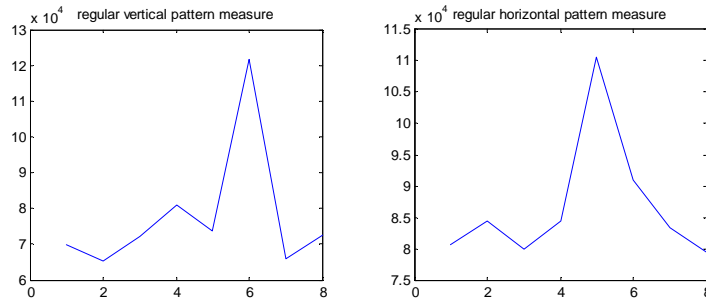


Fig.9: RPM measure with cropping. The blocking artefact starts with the pixel [6,5].

3 Experimental Results

To assess the effectiveness of any forgery detection technique, a suitable dataset of examples should be used for evaluation. According to [10] the input dataset contains a number of uncompressed images organized with respect to different resolutions, sizes and camera models. Also the standard dataset from Kodak images and from UCID v.2 have been used. The overall dataset can be downloaded from [14]. It is composed by 114 images with different resolution. Experiments were done varying in an exhaustive way the cropping position and the compression rate.

Moreover the *cjpeg* [12], (i.e., the reference code for the JPEG encoder), has been used to compress the images and the flag *-quality* was used to modify the quality from 10 (high compression ratio) to 90 (low compression ratio) with the step of 10. In particular each image has been cropped in order to test every possible cropping position in the 8x8 block, just to consider the possibility to test the method also in presence of real regular patterns in the image that could influence the results. In Table 1 are reported the overall results, described in terms of correct percentage of the cropping position detection, with respect to the involved compression ratio.

Table 1. Results of the proposed method.

| Quality factor | Accuracy (%) |
|----------------|--------------|
| 10 | 99 |
| 20 | 91 |
| 30 | 80 |
| 40 | 69 |
| 50 | 58 |
| 60 | 46 |
| 70 | 39 |
| 80 | 28 |
| 90 | 16 |

Exhaustive tests have been done for every image, every cropping position and quality factor. Thus the accuracy has been obtained considering 2891 cases.

Experimental results show that performances increase according to the compression rate. It is reasonable, since the blocking artefact increases at higher compression ratio.

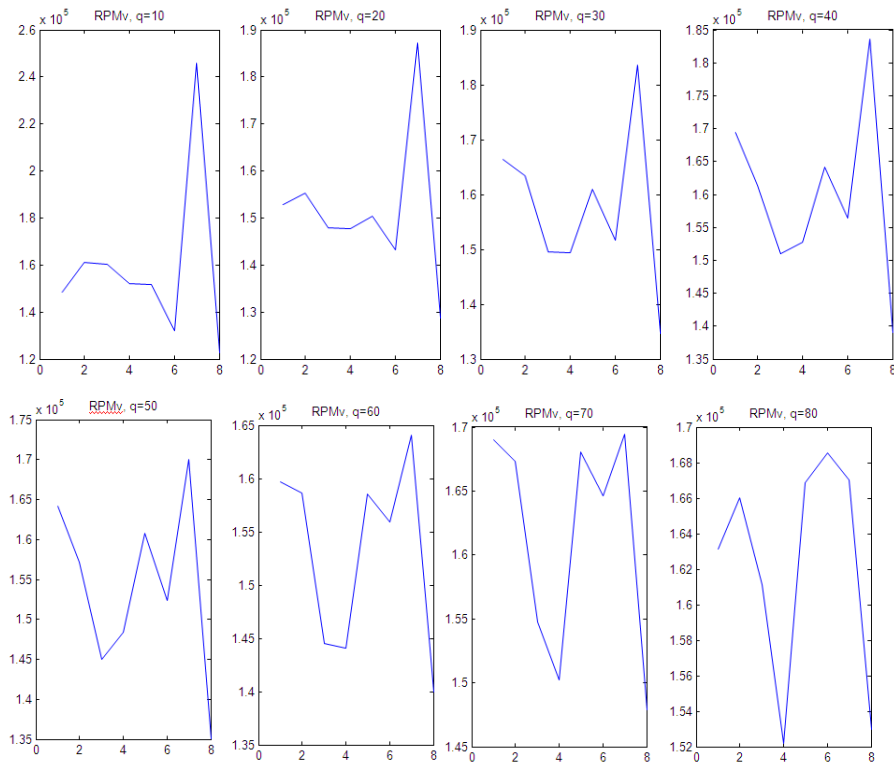


Fig.10: RPM measure obtained at varying the *quality* factor.

In Figure 10 the RPM (only vertical) measure is shown at varying the *quality* factor (real crop position = 7). Reducing the quantization (i.e., increasing the quality factor),

the peak is less evident and, in this example, with the $quality=80$ the estimation fails, since the effect of a real edge becomes predominant.

The proposed solution was compared to the method described in [1,7]. Unfortunately in these papers the cropping detection is not automatic, but it is supposed a visual inspection at the end of the process. In Figure 11 are shown the results of this method at varying the quality factor from 10 to 90 for the Lena image for a cropping position (3,5). It is evident that the cropping position is detectable up to $q=40$. Above this value it is no more visible. Similar results have been obtained for all the involved dataset.

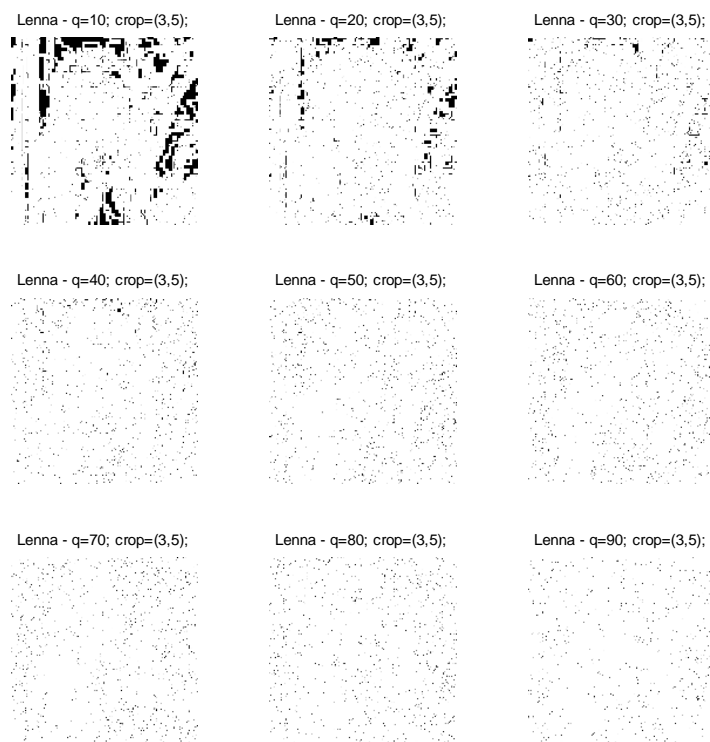


Fig.11: Li's method [1, 7] applied to Lena image at varying the $quality$ factor.

4 Conclusions

A new algorithm for cropping detection has been presented. It can be used in forensic applications to detect tampered images affected by cropping pre-compressed images. It can also be used in the pipeline with other blocks to increase the reliability of the results. The method is based on DCT artefacts analysis, in particular on the blocking

artefacts that are detected through an adaptive system working in the luminance component. Experimental results show that, according to the blocking artefact behavior, the reliability of the response increase according to the compression ratio. The main advantages of the proposed technique with respect to the state of the art are the speed (e.g. the [1] requires 50 seconds while the proposed solution requires less than 1 second for each inspection). Moreover it is a fully unsupervised (e.g., not require any visual inspection). Also its reliability is acceptable at lower compression ratio (i.e. when the blocking artefact is almost negligible). Further works will aim to increase the reliability of the system (e.g., by weighting differently the blocks contribution according to a flatness measure) and extending the methodology also to the color component, since these are heavily compressed. Moreover, further research will also devoted to exploit local information, in order to locate discrepancies inside the image (i.e., to discover copy and paste forgery).

References

1. W. Li, N.i Yu and Y. Yuan, "Doctored JPEG image detection" In Proceedings of International Conference on Multimedia and Expo, IEEE ICME (2008).
2. W.N. Lie, G.S. Lin and S.L. Cheng, "Dual protection JPEG images based on informed embedding and two-stage watermark extraction techniques" In IEEE Transactions on Information Forensics and Security 1 (2006), Pag. 330-341.
3. Judith A. Redi, Wiem Taktak and Jean-Luc Dugelay, "Digital image forensics: a booklet for beginners" In Multimedia Tools and Applications - Volume 51 Issue 1, January 2011
4. S. Battiato, M. Mancuso, A. Bosco and M. Guarnera "Psychovisual and Statistical Optimization of Quantization Tables for DCT Compression Engines" In IEEE Proceedings of International Conference on Image Analysis and Processing ICIAP 2001, Pag. 602-606 Palermo, Italy, September 2001
5. Fan, Z. and De Queiroz, R.L. "Identification of bitmap compression history: JPEG detection and quantizer estimation" IEEE Transactions on Image Processing (2003), Pag. 230-235.
6. Huang, F., Huang, J. and Shi, Y.Q. "Detecting double JPEG compression with the same quantization matrix" In IEEE Transactions on Information Forensics and Security (2010), 5 (4), art. no. 5560817, Pag. 848-856.
7. Li, W., Yuan, Y and Yu, N. "Passive detection of doctored JPEG image via block artefact grid extraction" In Signal Processing (2009), 89 (9), pp. 1821-1829.
8. <http://www.jpeg.org/jpeg/index.html>
9. <http://www.mpeg.org/MPEG/video/>
10. S. Battiato and G. Messina "Digital Forgery Estimation into DCT Domain - A Critical Analysis" In Proceedings of ACM Multimedia 2009 – Workshop Multimedia in Forensics - Beijing (China), October 2009;
11. H. Farid, "Digital Image Ballistics from JPEG Quantization", Technical Report, TR2006-583, Dartmouth College, Computer Science, 2006
12. *cjpeg* code can be found in <http://www.ijg.org/>
13. A. Bruna, M.Mancuso, A.Capra. S.Curti, "Very Fast algorithm for Jpeg Compression Factor Control" In Proceedings of SPIE Electronic Imaging 2002 - Sensors, Cameras, and Applications for Digital Photography IV - San Josè CA USA - Jan 2002
14. DBForgery 1.0: http://iplab.dmi.unict.it/index.php?option=com_content&task=view&id=41&Itemid=118