IMAGE TAMPERING DETECTION USING BAYER INTERPOLATION AND JPEG COMPRESSION

Marie-Charlotte Poilpré
I.S.B.S. Paris
(Institut Supérieur des BioSciences)
Faculté de Médecine de Créteil
9, rue du Général Sarrail
94000 Créteil
FRANCE
poilpre_mc@yahoo.fr

Patrick Perrot
I.R.C.G.N.
(Institut de Recherche Criminelle
de la Gendarmerie Nationale)
1, bd Théophile Sueur
93111 Rosny-sous-bois cedex
FRANCE
patrick.perrot@gendarmerie.defense.gouv.fr

Hugues Talbot
Université Paris-Est
A2SI-IGM CNRS UMR 8049
2 bd Blaise Pascal
93162 Noisy-le-Grand cedex
FRANCE
talboth@esiee.fr

ABSTRACT
In this paper, we describe a technique to detect image tampering using two different methods. The first is based on the Bayer interpolation process and its consequences in the Fourier domain. The second uses artifacts of the JPEG compression and more particularly in the JPEG frame observable in the Fourier domain.

Categories and Subject Descriptors
I.4.0 [**Computing methodologies**]: General – *Image processing software.*

General Terms
Algorithms, Experimentation, Security, Theory, Legal Aspects.

Keywords
Bayer interpolation, JPEG compression, probability map, Fourier transform, data forensics.

1. INTRODUCTION

Years ago, witness testimony and consent were often sufficient to convince judges and magistrates. Nowadays, 'scientific evidences' have become essential elements of forensic investigation.

Different biometric and genetic modalities can provide relevant and modern elements of evidence. To the contrary, digital media provide delinquents with various means to commit crimes and offences. Indeed, with the widespread availability of high-resolution consumer cameras and sophisticated software, people can readily insert forgeries in such media and thus fool even criminal experts. Data forensic experts are especially interested in methodologies able to detect such forgeries and be thus able to determine whether a photograph can be considered to be acceptable evidence in court proceedings.

In this paper we present such an application, named '*SAFE Images*' (for System of Authentication for Forensic Exploitation of Images), It is based on algorithms that calculates the probability map of an image and interprets the Fourier Transform of this map. Two methods are proposed to establish the authenticity of an image: a clear presence of a Bayer or other similar Colour Filter Array (CFA) interpolation scheme and the regularity of the JPEG frame.

E-FORENSICS 2008, January 21-23, Adelaide, Australia

DOI 10.4108/e-forensics.2008.2694

2. STATE OF THE ART

Analysis of image tampering is a major preoccupation in forensic sciences. Many methods have been proposed to detect manipulations. Thus, J. Fridrich in [1] and A. Popescu in [2] have developed methods to detect duplicated regions in an image. It's an efficient way to detect forgeries, but it's limited by high computation load and by the fact that it only detects one specific type of tampering.

Other methods have been proposed, such as the detection of inconsistencies in lighting, using the positioning of light sources, as presented by M. K. Johnson in [3], or the study of the sensor pattern noise, done by J. Lukás in [4]. But like the first method presented, these are only relevant to a single type of tampering.

More general techniques were studied by several research groups ([5], [6], [7] and [8]) around the idea of watermarking. The aim of these methods is to embed information in the image in order to authenticate it after some data transfer. The main limitation of this technique is that it must be assumed that the watermark cannot be easily extracted, modified and reinserted. Moreover, the watermark must be inserted at the time of the image capture, which involves cameras that must be equipped to insert such a digital signature. This method is thus not applicable to forensic sciences because of the lack of information about the images under study.

Another way to detect inconsistencies in an image is to study some image statistics [9]. This was proposed by H. Farid and A. Popescu in [10] : they observed the evolution of the Bayer interpolation pattern when a forgery is inserted in an image. This method is general and thus applicable to many tampering techniques, it is robust to compression, but the results have been obtained with images using a RAW (uncompressed) format, which is a format limited to some cameras.

In this paper, after exposing the theoretical background, we describe how Farid and Popescu's intial work was expanded to develop a more complete method, based on the Bayer interpolation and the JPEG compression. We show some of our results as well as an example of analysis.

3. THEORETICAL BACKGROUND

3.1 The Bayer interpolation

Most digital cameras are equipped with a CMOS or CCD sensors. They transform the collected light at the level of a layer of silicon, into electric signals. They thus allow manufacturers to generate a grayscale image where each pixel represents a light intensity.

In order to generate a colour image, it's necessary to code the chromatic information. The chromatic information is often represented using the RGB (Red, Green, Blue) system : these three primary colours are mixed to recreate all possible colours.

To capture the three primary colours, the sensors are coupled with a colour filter array (CFA). The most widely used CFA is the Bayer grid: it permits to capture only one of the three colours at each pixel location, according to a well defined grid, shown in fig. 1.

G	R	G	R	G
B	G	B	G	B
G	R	G	R	G
B	G	B	G	B
G	R	G	R	G

Fig. 1 : Bayer filter grid : R for red, G for green and B for blue. Note that the green cells are more numerous, ostensibly due to the higher sensitivity of the human eye for this colour.

The image obtained has to be processed in order to provide a complete RGB colour information at each pixel location. Two missing colours must therefore be interpolated at each location. Multiple algorithms exist and can be used, but they by and large all obey the same principle : missing values are computed from the value of neighboring pixels. The consequence is that each pixel is statistically correlated to its neighbors. The method developed is based on the assumption that the insertion of a forgery in an image would corrupt these correlations between pixels in an identifiable way. Tampering detection can thus be summarized as the detection of a lack of, or a modification of expected correlations in a region of the image.

3.2. The JPEG compression

An image is JPEG compressed by first colour transforming and down-sampling it. Then, the image is split into 8 by 8 pixels blocks which are then DCT transformed in order to obtain a frequency and amplitude map rather than a pixel and colour one. In this way, colour changes (value, rapidity and importance of these changes) can be better compressed. This step is very important because it permits to separate high frequencies from low. The next step is the quantization: high frequencies are reduced by dividing each DCT-transformed block by a quantization matrix Q. Very high frequencies coefficients are reduced to zero and the blocks thus obtained show a long series of null coefficients. These redundant data are then encoded with the RLE (Run-Length Encoded) algorithm, which collects together identical coefficients efficiently.
The three important steps of the JPEG compression scheme are the splitting of the image into blocks ; the quantization matrix, which defines the quality of the compression (quantity of information lost) ; and the encoding, which actually compresses the data.

4. METHODS

4.1. Probability map computation

In order to evaluate the correlation between pixels in the image, a probability map is computed, according to the method proposed by Farid in [9]. This map represents, for each pixel, its probability to be correlated to its neighborhood.
Following [9], a single probability map is computed for each channel: red, green or blue. two slightly different algorithms are used to take into account the fact that the green channel is more represented than the others (because of the high sensitivity of the human eye for that colour) in the Bayer CFA. A green pixel will interpolate its missing value from a 4-connect neighborhood (usually only in vertical or horizontal directions). On the other hand, blue and red pixels will have to interpolate their missing values vertically, horizontally and diagonally, which implies an 8-connect neighborhood. As a result, the number of coefficients applied to the neighborhood will be function of the channel chosen for the study: 4 for the green one and 8 for the others.
The probability map is computed using the Bayes probability theorem and by considering coefficients and a Gaussian noise with unknown variance to pixels and their neighbors. An optimum probability map is obtained thanks to the *Expectation Maximization* (EM) algorithm. This algorithm uses a series of convergent iterations. The first step (called E-step) estimates the probability map assuming pixels are either independent or interpolated, and the second step (M-step) calculates the new value of the parameters : in our case, the variance of the noise function and the α interpolation coefficients.
The α coefficients are computed via a linear system resolution (including either 4 or 8 equations depending on the chosen channel).
For our application, we have improved the method proposed by Farid and Popescu by eliminating the computation of the neighborhood coefficients by the EM algorithm. Indeed, we noticed that the coefficients obtained at convergence in the case of JPEG-compressed images were constant: [¼ ¼ ¼ ¼] for a 4-connect neighborhood and [-¼ -¼ -¼ -¼ ½ ½ ½ ½] for an 8-connect neighborhood (the first coefficients of the latter neighborhood are the corner ones). Therefore, we decided to keep these values constant as initial parameters of our algorithm instead of computing them. This makes the EM computation much faster since it only is necessary to estimate the noise variance.

4.2. Computation of the Fourier transform

For each channel, if pixels are considered either horizontally or vertically, it can be observed that one of every two pixels is captured (by the Bayer filter) and the other is interpolated. The probability map obtained is thus expected to show every second pixel either white (probability to be interpolated equal to 1) or black (zero probability). This remains true irrespective of the channel. This frequency of ½ is the maximal frequency that can be observed in any image: this results in the presence of one peak in each direction (vertically and horizontally). Because of the

symmetry of the Fourier transform, 4 peaks can actually be detected. In the case of the green channel, where white pixels form a quincunx lattice, these peaks are positioned at the extremities of the 2D domain, i.e. in each corner.

In addition to this basic high carrier frequency, the JPEG frames can also be detected. In the JPEG spatial domain, due to the nature of the DCT, pixels in the top and left row of each 8x8 block are more independent than those in the bottom and right rows of the same block. As a compression artifact, in effect the top and left part of each block will be visible in the probability map as high frequency areas, whereas the bottom right will be more readily uniformly white, appearing interpolated.

As a result, these 8 by 8 pixels blocks create multiple 1/8 frequency peaks in the Fourier domain, as well as their harmonics. Significant JPEG spots are positioned vertically and horizontally at 1/8, 1/16, 1/24, 1/32, … *etc ;* with decreasing intensity. The position of the spots in the Fourier domain is illustrated fig. 3.

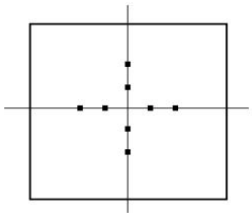

Fig. 3 : Illustration of the position of JPEG spots observed at the frequency of 1/8 and the first harmonic.

4.3. Detecting interpolation peaks

When a forgery is inserted in an image, the correlations between pixels are likely to be broken and the probability map is disturbed as a result. In the Fourier domain, the 4 interpolation peaks may disappear.
Our proposed method of tampering identification is based on the detection of the presence or absence of the Bayer interpolation peak, irrespective of the image format.
In order to facilitate the detection of these peaks, it is necessary to center them in the domain (not in the corner). To achieve this, an up sampling of the probability map, with a factor 2, is applied. This doubles the distance between adjacent pixel and therefore divides by two their frequency : the peaks are then positioned at the coordinates : (¼ ; ¼), (¼ ; ¾), (¾ ; ¼), (¾ ; ¾), as shown in fig. 2.

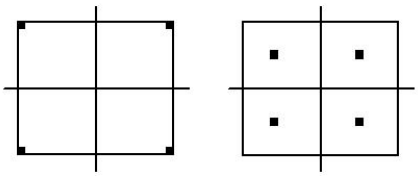

Fig. 2 : Illustration of the initial and final positions of the peaks after an up sampling of the probability map.

A post-treatment is applied to the Fourier transform as well: a threshold is chosen in order not to have too many high values. Then, a high pass filter is applied to eliminate low frequencies. After that, a normalization step is applied to force values between 0 and 1. Next, the magnitude of the Fourier transform is computed. Finally a blurring is applied.

4.4. The detection of the JPEG frame disturbance

When a copy-move forgery is committed, or when a new element is inserted in an image JPEG compressed, a new JPEG frame is created : a gap appears between the original frame and the new one. The new frame presents also a frequency of 1/8, but it is shifted with regard to the original, and thus new frequencies appear in the Fourier domain.
The images are processed in the same way as for detecting Bayer interpolation peaks : the probability map is computed and up-sampled and the Fourier transform is calculated and post-processed.
The method proposed consists of detecting a disturbed Fourier domain. Indeed, the apparition of new frequencies will be observable as a disturbance of the JPEG frame.
Shown in fig. 4 is an illustration of a Fourier transform of a manipulated image: it presents a modified JPEG frame because of the apparition of a second frame (circles in the figure) with the same frequency of 1/8 but shifted with regards to the original (squares in the figure).

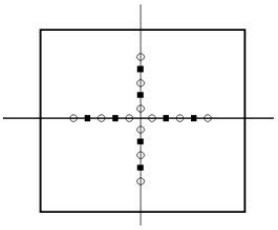

Fig. 4 : Illustration of a disturbed JPEG frame.

5. RESULTS

5.1. The detection of interpolation peaks

Images have been acquired from different image capture equipment (digital cameras, mobile phones) at various resolutions and formats (JPEG, TIF, BMP, and others).
The results obtained show that, for Bayer CFA-equipped cameras, we obtain a Fourier transforms presenting peaks of interpolation similar to those shown in fig. 5.

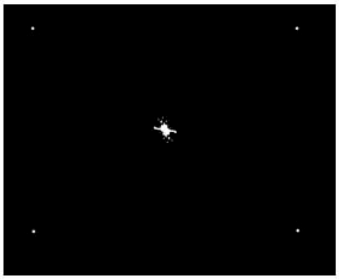

Fig. 5 : Fourier transform showing Bayer interpolation peaks.

The best channel for the detection of interpolation peaks is the green one. Indeed, green cells are most represented in the Bayer

filter and thus give more information about the chromatic interpolation process.

5.2. The detection of JPEG frame disturbance

The method has been tested by comparing original and manipulated images. The Fourier transforms obtained show that a manipulation implicates a modified JPEG frame in the Fourier domain. The fig. 6 shows JPEG frames of original and manipulated images. Note that the Fourier transform of the tampered image shows parasite frequencies (circled), which represent a shift with respect to the original.

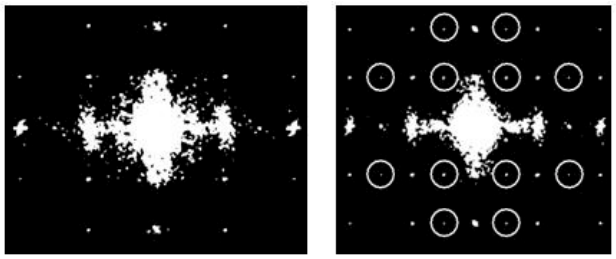

Fig. 6 : Fourier transforms of original (left) and manipulated (right) images showing a disturbance of the JPEG frame.

5.3. Proposed methodology of analysis for tampering detection

We propose the following methodology in order for experts to detect image tampering, as follows:

1- Compute the probability map of the image using the modified EM step
2- Compute the Fourier transform of the probability map obtained and express its magnitude
3- Study the expected position of the interpolation peaks and conclude on the presence or absence of these peaks (if the image is Bayer interpolated)
4- Study the JPEG frame and conclude on its aspect : intact or tampered (if the image is JPEG compressed).

Here is an example of the analysis of two images. The first is original and the second is manipulated. Shown in fig. 7 are two tested images.

fig. 7 : The two tested images :
the original on the left and the manipulated on the right.

Fig. 8 shows the two probability maps (PM) obtained. Some information can be deduced from the appearance of the PM alone Note that it can be observed that the limit between the face of the baby and the sofa (in the manipulated case) is obvious: pixels are not correlated anymore at the border of these two areas. This is due to the tampering of the yellow pillow.
Moreover, the face of the baby is more homogeneous in the tampered case; this is due to an histogram manipulation : the image is lightened. However, none of these observation are really conclusive, in particular in the absence of the reference original image.

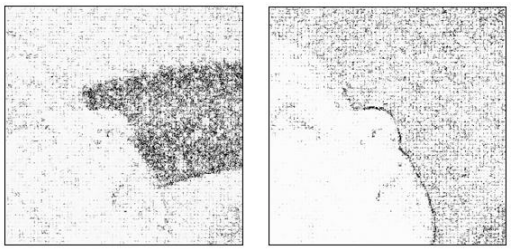

fig. 8 : The two probability maps :
of the original image on the left
and if the manipulated one on the right.

In the fig. 9 are presented the magnitude of the Fourier transforms computed from the probability maps. The first one, corresponding to the original image, shows clear interpolation peaks in the expected location. In the second, the interpolation peaks have disappeared and the JPEG is disturbed. In this case, it can also be established that the image has been re-compressed with a JPEG algorithm: the JPEG frame is more developed.

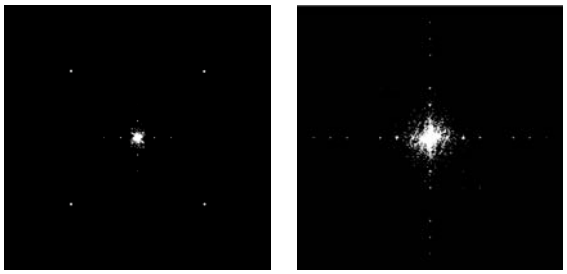

fig. 9 : The two Fourier transforms (magnitude) :
of the original image on the left
and if the manipulated one on the right.

6. DISCUSSION

The two methods presented yield encouraging results for the detection of image tampering. The Bayer CFA interpolation detection technique can readily be applied to other CFAs, and is robust with respect to various interpolating schemes, as established in [9]. The JPEG frame detection technique offers a complement of information which is also useful, and could also be used in cases where the digital image under study does not come from a device featuring a CFA (such as as scanned image for instance). Preliminary tests indicate that the JPEG technique seems robust to re-compression, although limits have not been established.

In contrast, in the case of the detection of the CFA interpolation peaks, the method only works on images captured by apparatuses equipped with CCD or CMOS captors and featuring a Bayer or equivalent CFA.

The method based on the JPEG disturbance detection is limited by the fact that all images studied by forensic experts are not necessarily JPEG-compressed. In this case, makes the proposed method will not provide any useful conclusion.

7. CONCLUSION

We have developed a method based on two principles: a detection of Bayer CFA interpolation peaks on the one hand and of peaks generated by the JPEG frame on the other. Both methods use the Fourier transform. The proposed application is only semi- automated, however is well adapted to forensic examinations. In many jurisdictions, experts cannot use purely automated methods because of the lack of nominative judgment. This application thus acts as a decision assistant tool with a view of forensic examinations.

The first results we obtained show that our two methods are complementary. Indeed, the detection of interpolation peaks is useful only if the image have been CFA-interpolated and thus is not general. On the other hand, the study of the JPEG frame is limited to the images compressed in this way. The coupling of both methods thus offers the possibility of examining a larger panel of images (with different formats, resolutions, compressions and forgeries).

Our methodology has been implemented in a software application developed in the MATLAB environment.

8. REFERENCES

[1] J. Fridrich, D. Soukal and J. Lukás, *"Detection of copy-move forgery in digital images"*, Proceedings of Digital Forensic Reserch Workshop, 2003.

[2] A. Popescu and H. Farid, *"Exposing digital forgeries by detecting duplicated image regions"*, Dartmouth College, Tech. Rep. TR2004-515, August 2004.

[3] M. K. Johnson and H. Farid. *"Exposing digital forgeries by detecting inconsistencies in lighting"*. In ACM Multimedia and Security Workshop, New York, NY, 2005.

[4] J. Lukás, J. Fridrich, and M. Goljan. *"Detecting digital image forgeries using sensor pattern noise"*. In Proceedings of the SPIE, volume 6072, 2006.

[5] C. Honsinger, P.Jones, M.Rabbani, and J. Stoffel, *"Lossless recovery of an original image containing embedded data"*, U.S. Patent Application, Docket No. 77102/E-D, 1999.

[6] J. Fridrich, M. Goljan, and M. Du, *"Invertible authentication"*, Proceedings of SPIE, Security and Watermarking of Multimedia Contents, 2001.

[7] E. Lin, C. Podilchuk ans E. Delp, *"Detection of image alterations using semi-fragile watermarks"*, Proceedings of SPIE, Security and Watermarking of Multimedia Contents, 2000.

[8] J. Fridrich and M. Goljan, *"Images with self-correcting capabilities"*, Proceedings of the IEEE International Conference on Image Processing, vol. 3, pp. 792–796, 1999.

[9] A. C. Popescu and H. Farid, *"Statistical tools for digital forensics*", Proceedings of the 6th Information Hiding Workshop, 2004.

[10] A. C. Popescu and H. Farid, *"Exposing digital forgeries in color filter array interpolated images"*, IEEE Transactions on Signal Processing, 53(10):3948–3959, 2005.