NARCAP Investigator Support Paper 01
NARCAP IS – 01, 2009

# Image Doctoring: JPEG Encoding and Analysis

Richard Tortorella
Research Associate

March 2009


## Abstract

This paper provides a brief overview of the various mathematical tools and concepts that can be utilized to investigate the potential doctoring of a JPEG encoded image file. The basic encoding of a JPEG image will be discussed along with the techniques of Block Artifact Grid (BAG) detection. EXIF header data as well as JPEG ghost detection will be discussed.

## Introduction

In the early days of photography, the 35mm negatives used by a camera were an investigator's primary key witness to forgery detection. Any modifications to a print could be quite easily detected in a manipulated negative. However, with the advent of digital cameras, the ability to investigate a potential fraudulent photograph has taken a digital perspective.

Most cameras today will store the images electronically on some type of memory medium. This is usually done in what is commonly known as a JPEG image format. This format involves applying algorithms to the raw camera data for compression and storage. The problem arises when a JPEG's validity is put into question. As there is no negative to investigate, one must turn to the JPEG themselves.

There are numerous programs that are capable of manipulating JPEG files, and if done properly, even a keen eye would have difficulty in detecting any changes.

However, not all is lost. There are several tools available to check the validity of the JPEG. These include EXIF validation and algorithm integrity. Although they do not provide the user with a one hundred percent JPEG tamper protection, they certainly do add a more quantitative solution that just a visual hunch.

.

## JPEGs and How They Work

The term "JPEG" is an acronym for Joint Photographic Experts Group – it was the name of the committee that created the standard. The standard was first issues in 1992 and formally accepted as ISO 10918-1 is late 1995. The standard itself defines the codec for the method that the image is compressed and decompressed and the way the file format itself is contained. This is vitally important for the study of image analysis, as the adherence to this format is key in detecting variations from an original source: a fake/hoax/forgery.[1]

The JPEG format utilizes a lossy type of compression. This means that information is removed from the original data set (the image) to allow for compression. This is fully acceptable in terms of daily usage, but for obvious reasons not so in astronomical, medical on any type of scientific imaging where every pixel contains potentially important information.

## JPEG Internal Structure

The JPEG encryption utilizes a sequence of markers[2]

| SHORT | BYTES | PAYLOAD | NAME | COMMENTS |
|---|---|---|---|---|
| **SOI** | 0xFFD8 | *none* | Start Of Image | |
| **SOF0** | 0xFFC0 | *variable size* | Start Of Frame (Baseline DCT) | Indicates that this is a baseline DCT-based JPEG, and specifies the width, height, number of components, and component subsampling (e.g., 4:2:0). |
| **SOF2** | 0xFFC2 | *variable size* | Start Of Frame (Progressive DCT) | Indicates that this is a progressive DCT-based JPEG, and specifies the width, height, number of components, and component subsampling (e.g., 4:2:0). |

[1] JPEG Standards
[2] JPEG Header Information.

| | | | | |
|---|---|---|---|---|
| **DHT** | 0xFFC4 | *variable size* | Define Huffman Table(s) | Specifies one or more Huffman tables. |
| **DQT** | 0xFFDB | *variable size* | Define Quantization Table(s) | Specifies one or more quantization tables. |
| **DRI** | 0xFFDD | 2 bytes | Define Restart Interval | Specifies the interval between RST*n* markers, in macroblocks. |
| **SOS** | 0xFFDA | *variable size* | Start Of Scan | Begins a top-to-bottom scan of the image. In baseline DCT JPEG images, there is generally a single scan. Progressive DCT JPEG images usually contain multiple scans. This marker specifies which slice of data it will contain, and is immediately followed by entropy-coded data. |
| **RST*n*** | 0xFFD0 … | *none* | Restart | Inserted every *r* macroblocks, where *r* is the restart |
| **APP*n*** | 0xFFE*n* | *variable size* | Application-specific | For example, an Exif JPEG file uses an APP1 marker to store metadata, laid out in a structure based closely on |
| **COM** | 0xFFFE | *variable size* | Comment | Contains a text comment. |
| **EOI** | 0xFFD9 | *none* | End Of Image | |

**FIGURE I - BASIC JPEG MARKER LAYOUT**[3]

In order to compress the image the following steps are taken:

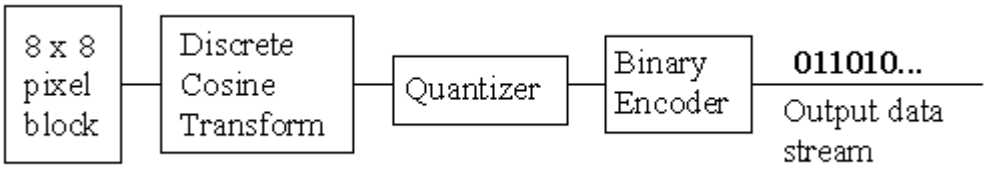


**FIGURE II – JPEG COMPRESSION STAGES**[4]

The JPEG codec divides the image into 8 by 8 pixel blocks. Each block is broken down and the codec calculates the Discrete Cosine Transform (DCT) of each block. This is obtained by the following formula:

[3] Marker Code Assignments
[4] JPEG Tutorial

$$B(k_1, k_2) = \sum_{i=0}^{N_1 - 1} \sum_{j=0}^{N_2 - 1} 4 \cdot A(i,j) \cdot \cos\left[\frac{\pi \cdot k_1}{2 \cdot N_1} \cdot (2 \cdot i + 1)\right] \cdot \cos\left[\frac{\pi \cdot k_2}{2 \cdot N_2} \cdot (2 \cdot j + 1)\right]$$

Where A = Initial Image
B = Final Output Image
$N_1$ & $N_2$ = Ranges for Pixel Height and Width respectively.

The Quantizer then rounds off the DCT coefficients according to an 8 x 8 Matrix. This is the step that generated the "lossy" aspect of JPEG, but allows for large compression ratios. Now that the process is described, techniques for image manipulation detection are possible.

## Detecting Manipulated JPEG Images

There are basically two principle methods of investigating the potential of a manipulated JPEG, they involve either:

- Active Protection
- Passive Detection

*Active Protection*

Active protection involves the application of digital watermarks and signatures to JPEG files. These are removed/modified as soon as the JPEG itself is tampered with in any way. This is a great tool to protect an existing JPEG file, but is useless in determining manipulation after the fact if it was not implemented the suspected alteration. For the purposes of this paper, this type of protection (although very good indeed) will not be discussed here.

*Passive Detection*

This methodology involves the analysis of two types of data from within the JPEG itself: the EXIF Data and the JPEG algorithm used to encode the original raw photographic data. This paper will discuss BAG, or Block Artifacts Grid mismatch. It must be noted, that there are indeed several other methods that utilize mathematical deviation to detect potential image manipulation, however they will not be discussed in this herein.[5]

[5] Image forgery Identification Using JPEG Intrinsic Fingerprints

BAG Mismatch

Synthetic images can be created with a copy and paste operation to either remove items or duplicate them. However when manipulation of the JPEG file is done to incorporate these changes, block artifacts are generated within a grid. These artifacts can be detected and shows not only that copy/paste transformations have occurred, but where they have occurred.[6,7]

In the following figure, the top circle is removed from the JPEG (a), by cutting and pasting from the side, creating JPEG (b) the 'Doctored Image'

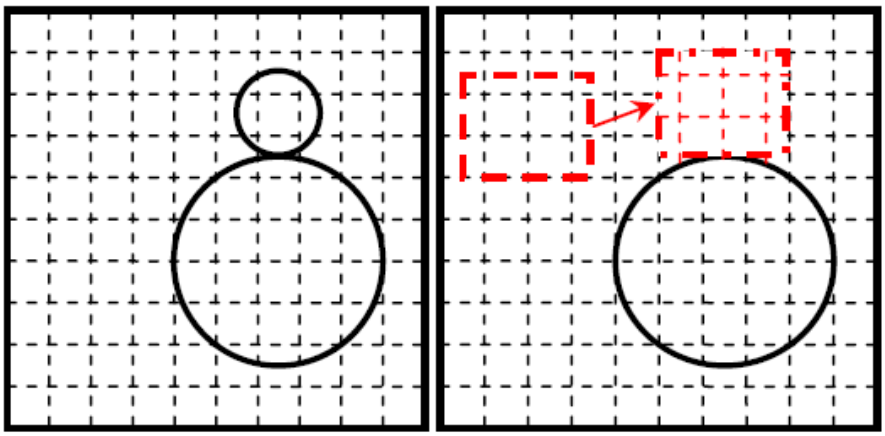


**FIGURE III(a) ORIGINAL VS. DOCTORED IMAGE**

This process is rather simple, but very difficult to detect with the naked eye if done properly. So, how can block artifacts allow the detection of this manipulation?

*BAG Extraction*

An interesting aspect of the DCT or Discrete Cosine Transform that is part of the compression process of the JPEG is that the high frequency AC coefficients are usually zero after quantifications when compressing. However, this is not the case when an image has been modified via cut/paste.

[6] Detecting Copy-Paste Forgery Of JPEG Images Via Block Artifact Grid Extraction
[7] Detecting Doctored JPEG Images

To locate a BAG, a Local Effect (LE) must be found. The LE is represented by

$$LE_i = \left| \frac{S_7}{S_0} \right|$$

Where the LE is the local effect of the i+7 signal, or from i = 0..7 (recall the 8 x 8 matrix). The Signal value itself is normalize via the following equation:

$$S_j = \sqrt{\frac{\alpha_j}{8}} \sum_{n=0}^{7} s_{i+n} \cos \frac{j(2n+1)\pi}{16} = 0 \quad (j = 0,1,\cdots 7)$$

The Local Effect, is then calculated from the following:

$$LE = \sqrt{\frac{\sum_{i=7 \text{ and / or } j=7} S_{ij}^{\ 2}}{S_{00}^2}}$$

The local effects represent the boundaries of the 'modifications' and have a inverse relation to the signal strength of the image (Figure III(b))

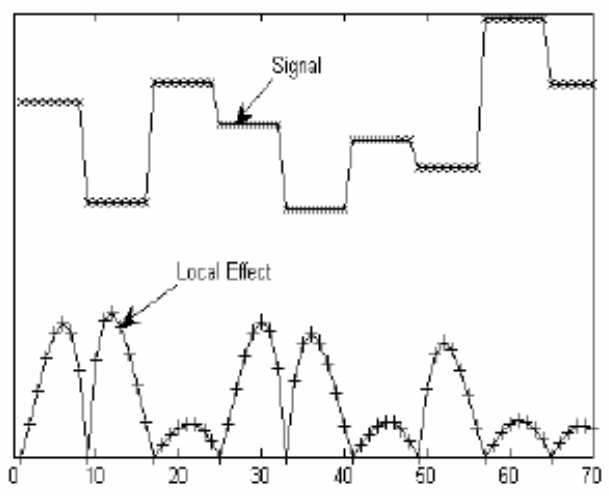


**FIGURE III(b)**

Once all the LE values are collected, a map can be provided showing the BAG.[8]

[8] Detecting Copy-Paste Forgery Of JPEG Images Via Block Artifact Grid Extraction

As an example of how this technique is applied, Figure IV(a) represents is a JPEG photograph of a man with a camera on a tripod with buildings off in the distance:

**FIGURE IV(a)**[9]

The image itself (Figure IV(a)) looks authentic at first glace (with a few exceptions), however if the tripod were properly superimposed, detection of the modification may not be apparent.

**FIGURE IV(b)**[10]

[9] Detecting Copy-Paste Forgery Of JPEG Images Via Block Artifact Grid Extraction

The figure above (Figure IV(b)) is the combination of the small LE (dark) and the large LE (bright). In order to facilitate comprehension of the photo, the local minimum value points of the LEs are obtained, and a grid form is created, resulting in:

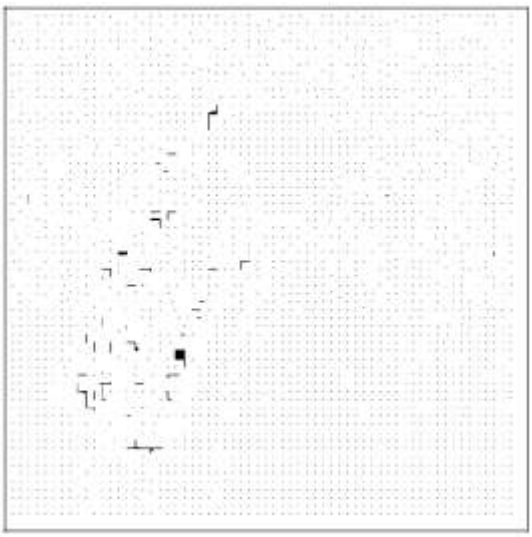

**FIGURE IV(c)**[11]

As can be seen in Figure IV(c), the basic outline of the man is visible as being manipulated. Although the tripod itself isn't shown, it can be assumed to be part of the doctored image as the man is interacting with it in the image.

This technique provides a valuable tool in the detection of what may be apparently real and authentic images. The mathematical support of this technique allows for the introduction of what used to be purely human observational factors into the determination of a potentially doctored image.

## EXIF JPEG Header Information

Every JPEG made from a camera has a lot of information held within the data in the form of JPEG headers. This data, called EXIF (EXchangeable Image File format) contains (among other things):

- Time and date picture was taken
- Camera make and model
- Integral low-res EXIF thumbnail
- Shutter speed
- Camera F-stop number

[10, 11] Detecting Copy-Paste Forgery Of JPEG Images Via Block Artifact Grid Extraction

- Flash used (yes/no)
- Distance camera was focused at
- Focal length and calculate 35 mm equivalent focal length
- Image resolution
- GPS info, if stored in image
- IPTC header
- XMP data [12]

EXIF was first published in October of 1996 as version 1.0. It was mainly due to the desire for a uniform file format standard for image data stored by digital cameras, as well as the uniformity of data stored within a file.[13]

This information is very useful, for the simple fact that most doctor's images will no longer contain the 'correct' data from the reported camera, and actually have the name of the application used to fabricate the image (such as Photoshop for example).

There are numerous applications that can read (and modify) the image data. Thus, although they certainly do not reflect a safe means of identifying an altered image, the lack of any information (or presence of any alien data) certainly does provide proof that the image has been altered.

## JPEG Ghosts

Digital manipulation involving cloning, splicing copy/paste and re-sampling are all very effective ways to alter a JPEG from its original composition.

In standard JPEG compression algorithms, a colour image (RGB) is converted into luminance/chrominance space called YCbCr. The two chrominance levels, denoted by CbCr are usually re-sampled by a factor of 2 relative to the luminescence Y.

When a JPEG image is modified, the resampling of the JPEG into YCbCr – and usually, the sampling of spliced information is different than the rest of the image.

Although it may not be apparent at first, but subsequently re-encoding the JPEG at different ratios will show the modified portion of the image, as the difference will be amplified (by a factor of two) for each subsequent iteration.[14]

[12] EXIF JPEG Header Manipulation Tool
[13] Digital Still Camera Image File Format Standard
[14] Exposing Digital Forgeries from JPEG Ghosts

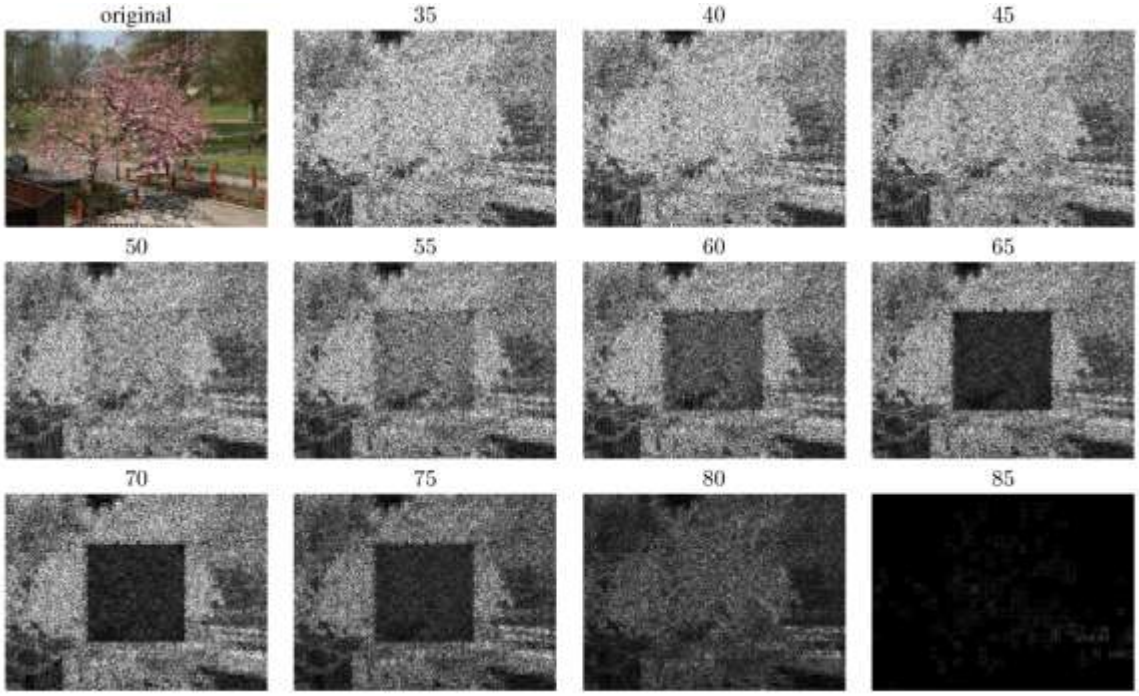


**FIGURE V**[15]

The above figure (Figure V) shows how the central 'square' visible in later images was originally undistinguishable from its surroundings, until the image was repeatedly saved at increasing JPEG quality (from 35% to 85%).

Although this technique does still require a person to determine an optical difference, once again, the mathematics behind the algorithms does provide a very solid foundation for any modifications discovered.

## Conclusion

There are many ways to detect photographic or image forgeries, both using visual cues and other more mathematically oriented means. As has been discussed, there are several advantages to knowing the exact structure and function of the JPEG codec. In the case of image manipulation and doctoring detection, this is certainly the case. The information provided in this paper is intended to provide a brief overview of the various options available to any investigator from casual amateur to a professional.

[15] Exposing Digital Forgeries from JPEG Ghosts

References

*Digital Still Camera Image File Format Standard*. Retrieved March 20, 2009, from: http://www.exif.org/Exif2-1.PDF

*Detecting Doctored JPEG Images.* Retrieved March 20, 2009, from: http://www.patents.com/Detecting-doctored-JPEG-images/US7439989/en-US/

Garg, A., Hailu, A., Sridharan, R. (2008) *Image forgery Identification Using JPEG Intrinsic Fingerprints*. Retrieved March 20, 2009, from: http://www.stanford.edu/~divad/mentorship/GargHailuSridharan.pdf

*EXIF JPEG Header Manipulation Tool*. Retrieved March 20, 2009, from: http://www.sentex.net/~mwandel/jhead/

*Farid, H., (2007) Exposing Digital Forgeries from JPEG Ghosts*. Retrieved March 20, 2009, from: http://www.cs.dartmouth.edu/farid/publications/tifs09.pdf

*JPEG Header Information*. Retrieved March 20, 2009, from: http://www.obrador.com/essentialjpeg/headerinfo.htm

*JPEG Standards*. Retrieved March 20, 2009, from: http://www.jpeg.org/faq.phtml

*JPEG Tutorial.* Retrieved March 20, 2009, from: http://cobweb.ecn.purdue.edu/~ace/jpeg-tut/jpegtut1.html

Li, W., Yaun, Y., Yu, N. (2008) Detecting Copy-Paste Forgery of JPEG Images Via Block Artifact Grid Extraction. Retrieved March 20, 2009, from: http://www.eurasip.org/Proceedings/Ext/LNLA2008/papers/cr1006.pdf

*Marker Code Assignments*. Retrieved March 20, 2009, from: http://www.digicamsoft.com/itu/itu-t81-36.html