File Forensics for RAW Camera Image Formats

Matthias Kalms[1], Thomas Gloe[1], Christopher Laing[2]

[1]Institute of Systems Architecture, Technische Universität Dresden, 01602 Dresden, Germany
[2]School of Computing, Engineering and Information Sciences,
Northumbria University, NE2 1XE Newcastle upon Tyne, U.K.

***Abstract*—Recent research in multimedia forensics has developed a variety of methods to detect image tampering and to identify the origin of image files. Many of these techniques are based on characteristics in the JPEG format, as it is the most used file format for digital images. In recent years RAW image formats have gained popularity among amateur and professional photographers. This increase in their use and possible misuse makes these file formats an important subject to file forensic examinations. The aim of this paper is to explore to which extend methods previously developed for images in JPEG format can be applied to RAW image formats.**

***Index Terms*—digital image forensics, image file forensics, RAW image formats, tamper detection**

I. Introduction

In digital photography, JPEG is the most commonly used file format for digital images. Especially as storage format in digital cameras, it has been used by most manufacturers since the beginning of commercial digital photography in the late 1990s. With higher demands on image quality and growing importance of digital post-processing, raw file formats come into focus, providing access to never processed sensor data. These are generally referred to as RAW image formats. Although not used on most compact cameras, these formats are now widely available as an option in digital single lens refractor (DSLR) cameras. Just as negatives in analogue photography they provide a high quality version with a wider colour range and higher resolution, from which the final image can be developed and have therefore sometimes been referred to as 'digital negatives'. In contrast to JPEG files, RAW images can only be decoded by special software and codecs that are not pre-installed on common operating systems. Consequently RAW file formats can be found as backup file on a local hard drive rather than being published online. Common image processing software do not allow to save images in these formats. RAW images are therefore regarded as much more trustworthy as a JPEG compressed version. For images in a research context, the guidelines by Cromey [1] even suggest RAW image formats as reference files that can later be compared to a processed version. It is nevertheless possible to manipulate RAW image files, although special software is required to do so. Consequently it is desirable to detect whether or not it has been manipulated. It has been shown by Kee et al. [2] that extracting a signature from header parameters can effectively be used for image authentication in JPEG images. Building on their method we show that a similar approach can also be used on three of the most common RAW image formats.

II. Recent Research on JPEG Files

Multimedia forensic techniques on JPEG files can mainly be divided into two categories. Both categories try to identify characteristics in the file that can give clues on devices and software, used to create it. The first analysing the information stored in the file header for characteristics of the encoding software. The other focusing on a statistical analysis of image data using manipulation artefacts and device characteristics.

A. JPEG File Information

The JPEG file format allows to store the compressed image data together with all necessary parameters for decompression. It is also possible to store metadata including information of camera settings, identifying serial numbers and time and location of image acquisition. Recent research has shown that this information stored in JPEG file headers can help to uncover the creation and processing history of an image. The file header consists of a series of segments, each tagged with a specific marker. Although the JFIF standard defines exactly how the information is stored in these segments, there are vendor specific segment markers. The APP14 segment for example is specifically used by Adobe, to store information about the software version and the compression quality that was used for post-processing. Gloe [3] showed that the sequence of all JPEG marker segments in a file can be camera manufacturer or software specific. Apart from that the characteristics of the data stored in the segments and the combination of these characteristics, can be used very effectively to identify the source camera or whether an image has been altered by software.

Common formats to store metadata are EXIF, IPTC and XMP. Also manufacturer-specific formats are used by camera and software manufacturers. Almost all digital cameras store their metadata in the EXIF format as part of the JPEG file. This format contains a variety of tags, unique byte signatures specified in the EXIF standard [4], that are used to identify the information in the binary file. Using these tags information about the camera, technical details of the photograph and the date and time it was shot can be stored in the APP1 segment. This includes information about the camera manufacturer, model and

time of acquisition. Sometimes, even serial numbers of the camera body or a interchangeable lens are stored in this segment. Has this information been deleted or altered in the file, other metadata can also give clues on the source device. To give an example, image dimensions dependent on the chip size and processing algorithm are specific to one manufacturer, small group of camera models or even a single model. The marker notes tag also provides a segment where a manufacturer specific set of tags and therefore more detailed information about the camera and shot can be stored. Alvarez [5] discussed the use of EXIF information in a computer forensic examination. He stated that this information can never stand on its own and must be examined together with the photo's context.

As a part of JPEG compression, the quantization stage depends on a set of parameter tables, known as Define Quantization Tables (DQT). Two or more tables are stored in the header of every JPEG file. The use of these tables in the detection of image forgery was discussed in a paper by Kornblum [6], following a study by Farid [7]. Camera manufacturers and software companies often use custom quantization tables, suitable to identify groups of camera models using the same quantisation table. Also a separation between authentic image files and post-processed image files is possible, as software vendors employ their own quantisation tables. Source devices and programmes that use the standard quantization tables proposed by Independent JPEG Group (IJG) in 1998 cannot be determined by the tables alone, as they are not manufacturer specific. In some cases, more than two quantization tables are used, which can be another characteristic parameter. Define Huffman Tables (DHT), another set of parameters that is needed for JPEG compression can be used in the same manor. In 2008, Farid [8] did a follow up study on his paper of 2006, concluding, that analysing quantization tables "is reasonably effective at narrowing the source of an image to a single camera make and model or to a small set of possible cameras" (2008).

JPEG file headers also include a number of thumbnail images, used for previewing an image. The creation of a thumbnail inside a camera consists of a series of processing steps, including filtering, adjustments and compression. Kee and Farid [9] have shown that these parameters vary significantly between camera manufacturers and photo-editing software. As thumbnails are JPEG compressed themselves they store compression details such as DQT and DHT, which can be used in the same way as in a regular image file. Their dimensions are also a significant parameter. Furthermore not every software will update every thumbnail when saving an image. In these cases a low quality version of the deleted areas might exist, to give, combined with the remaining photo segment, a general idea about the original content.

Kee et al. [2] suggested a method using a combination of all these features, concluding: "Specifically, 62% of images have a signature that is unique to a single camera, 80% of images have a signature that is shared by three or fewer cameras, and 99% of images have a signature that is unique to a single manufacturer." (2011). Their findings also indicate that it is still hard to distinguish manipulated images from e.g. RAW Images that have been converted to JPEG by software. In this case the software can influence the Quantization tables, image dimensions and the EXIF segment. These files might than have the same characteristics as a JPEG file, processed with that specific software.

EXIF information is not inherent to each image and can easily be edited or replaced. To avoid detection, the whole header can be replaced, altered or faked. But, apart from editing EXIF information, this is not a feature of modern image processing software. Also the findings of Kee et al. [2] show, that it takes more than changing a single feature of the file header, when faking another image source

III. RAW Image Files Forensics

A. Structure of RAW File Formats

In this section we will examine the structure of the two most commonly used proprietary RAW formats: the Nikon Electronic Format (NEF) and CR2, the second version of the Camera Image File Format (CIFF) [10]. Additionally, we will take a closer look on Adobe's Digital Negative (DNG) [11], as it not only promises to be the format for future archiving, but also gets increasingly used in high-end middle format cameras. It is also the only RAW format in this examination, for which a full documentation is available. Therefore the examination of the structure of RAW files has to be based on observable rules in the general file structure. All three of these formats, like most RAW image formats are based on the Tagged Image File (TIFF) Standard. In the first section in every TIFF based file, the header, a magic number to mark it as a TIFF file, information about the byte order and a pointer to the following section are given. CR2 files have an extended header, including also a magic number, version and subversion for CR2 and an additional pointer to the raw image data.

The next segment is the first of a number of Image File Directory (IFD) segments. Each of these segments represents a sub file, an image in most cases. It contains information about the image and points to the binary image data in the file. The first segment (IFD#0), contains not only most of the metadata, the EXIF and Makernotes IFD, but also information about a preview or thumbnail image it represents. In total, mostly there are four versions of a camera image in all three RAW formats: a high resolution JPEG compressed preview image, a low resolution JPEG compressed thumbnail, an uncompressed low resolution image and finally lossless compressed raw image data without any post-processing applied. These are stored in separate IFD segments. NEF as well as DNG files embed all following segments as sub-IFDs in IFD#0 while the format CR2 employs individual major IFDs to store information.

B. Counter Forensic Techniques

There are several software packages available, that are capable of modifying or deleting segments in RAW image files. ExifTool [12] provides a wide range of alteration functionalities. It allows to modify, copy and delete metadata by entry, segment or as a whole. Using this function, information about the image that is saved in the file, e.g. timestamps, the camera model and the camera manufacturer

Table I
STRUCTURE OF COMMON RAW FILE FORMATS

Structure	TIFF	CR2	NEF	DNG
Header	0-1: Byte order 2-3: TIFF magic number 4-7: Offset to 1st IFD	0-1: Byte order 2-3: TIFF magic number 4-7: Offset to 1st IFD 8-9: CR2 magic number 10: CR2 major version 11: CR2 minor version 12-15: RAW IFD Offset	0-1: Byte order 2-3: TIFF magic number 4-7: Offset to 1st IFD	0-1: Byte order 2-3: TIFF magic number 4-7: Offset to 1st IFD
0th IFD	**Sub File (e.g. Image)** + basic image Information	**Preview Image** (JPEG compressed, RGB, ¼ of original resolution) + basic image information	**Thumbnail Image** (uncompressed, RGB, 160x120) + basic image information	**Small Thumbnail Image** (uncompressed, RGB) + basic image information
EXIF IFD		**EXIF Metadata** + Canon Makernotes	**EXIF Metadata** Nikon Makernotes (including JPEG compressed preview image)	**EXIF Metadata** + Makernotes
0th Sub IFD			**Preview Image** (JPEG compressed, RGB, full resolution) + basic image information	**Raw Image Data** (CFA, full resolution) + basic image information
1st Sub IFD			**Raw Image Data** (Nikon NEF compressed, CFA, full resolution) + basic image information	**Thumbnail image** (JPEG compressed, RGB) + basic image information
2nd Sub IFD			***Preview Image*** *(rare) (JPEG compressed, RGB,* 1632×1080*)* *+ basic image information*	***Preview Image*** *(Adobe DNG Converter only) (JPEG compressed, RGB)* *+ basic image information*
1st IFD		**Thumbnail image** (JPEG compressed, RGB, 160x120) + basic image information		
2nd IFD		**Small Thumbnail Image** (JPEG or uncompressed, RGB) + basic image information		
3rd IFD		**Raw Image Data** (lossless JPEG compressed, CFA, full resolution) + basic image information		

can be manipulated. Furthermore preview images of CR2 files can be extracted from or embedded in the file. Making any of these changes normally includes resaving the file, which will update the 'modified date' entry in the file. ExifTool offers a function to synchronize the modified date with other dates in the files metadata. Therefore modifications such as exchanging preview images or modifying the 'model' entry cannot be detected by a difference between the created and the modified date.

C. Examination

For this examination we collected a number of parameters from a total of 225 sample images in the three different RAW file formats, whose structure we have discussed in this paper. These images were created by 51 different camera models from three different manufacturers. Specifically 22 Canon, 24 Nikon and 5 Pentax camera models were used. In order to examine the DNG format we also converted CR2 and NEF files using Adobe's DNG Converter [13]. The proposed method does not aim at identifying whether a single entry, such as the date and time information, has been altered. It will however try to authenticate the camera maker and model entries by analysing the file information and general structure. Apart from DNG, RAW file formats are already manufacturer specific. Based on the approach on JPEG files by Kee et al [8] we examined how a combination of metadata parameters and characteristics in preview and thumbnail images stored in RAW files can be used to identify a group of cameras or even a single model. For this matter ExifTool was used to analyse the structure and metadata of each file. Thumbnail and preview images were then extracted and analysed using JPEGSnoop. Finally we also examined RAW files in which the date and time entries were altered using ExifTool.

1) Thumbnail, Preview and Raw Image Parameters : The first two parameters extracted are the dimensions of the raw image data and of the converted raw image. The raw image data has the exact resolution as the image sensor, while the converted image depends on border

Table II
VARIATIONS IN NEF FILE STRUCTURE

NEF basic structure	class 0	class 1	class2	class3
Header	x	x	x	x
IFD#0 + picture#0	x	x	x	x
SubIFD#0 + picture#1			x	x
SubIFD#1 + picture#2	x	x	x	x
EXIF	x	x	x	x
Makernotes + picture#3		x	x	x
SubIFD#2 + picture#4				x
cameras in class	Nikon D1	Nikon D100, D1X, ...	Nikon D3, D40, ...	Nikon D4, D3200

Table III
EXAMPLES OF RAW HEADER SIGNATURES

Maker/Model	**Canon 350D**	**Nikon D4**	**Pentax K-5**
Format	CR2	NEF	DNG
Metadata entry count	14 28 24 2 2 11 0 6	25 31 51 0 7 8 1 17 25 32 51 0 7 8 1 17	37 20 100 0 0 19 0 25
Sensor dimensions	3516×2328	4992×3292	4992×3284
Image dimensions	3456×2304	4928×3280	4928×3264
Preview dimensions	384×256	160×120	160×120
Thumbnail dim.	160×120	570×375	640×480
Thumbnail DQT	static tables	created dynamically	static tables
Quantization table (Y)	3 2 2 3 5 8 10 12 2 2 3 4 5 11 11 13 3 2 3 5 8 11 13 11 3 3 4 6 10 17 15 12 3 4 7 11 13 21 20 15 5 7 10 12 15 20 21 17 9 12 15 17 20 23 23 19 14 17 18 19 21 19 20 19		28 19 17 28 41 69 88 105 21 21 24 33 45 100 103 95 24 22 28 41 69 98 119 96 24 29 38 50 88 150 138 107 31 38 64 96 117 187 177 132 60 60 95 110 139 179 194 158 110 110 134 150 177 208 206 174 124 158 163 169 193 172 177 170
Quantization table (Cb/Cr)	3 3 5 9 19 19 19 19 3 4 5 13 19 19 19 19 5 5 11 19 19 19 19 19 9 13 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19		29 31 41 81 170 170 170 170 31 36 45 114 170 170 170 170 41 45 96 170 170 170 170 170 81 114 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170 170
Preview DHT	static tables	created dynamically	static tables
DC (Y)	2 1 3 3 2 4 3 5 5 4 4 0 0 1 125		0 1 5 1 1 1 1 1 1 0 0 0 0 0 0 0
DC (Cb)	3 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0		0 2 1 3 3 2 4 3 5 5 4 4 0 1 125
DC (Cr)	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
AC (Y)	2 1 3 3 2 4 3 5 5 4 4 0 0 1 125		2 1 3 3 2 4 3 5 5 4 4 0 0 1 125
AC (Cb)	2 1 2 4 4 3 4 7 5 4 4 0 1 2 119		2 1 2 4 4 3 4 7 5 4 4 0 1 2 119
AC (Cr)	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Preview dimensions	1536×1024	4928×3280	4928×3264
Preview DQT	static tables	created dynamically	static tables
Quantization table (Y)	3 2 2 3 5 8 10 12 2 2 3 4 5 11 11 13 3 2 3 5 8 11 13 11 3 3 4 6 10 17 15 12 3 4 7 11 13 21 20 15 5 7 10 12 15 20 21 17 9 12 15 17 20 23 23 19 14 17 18 19 21 19 20 19		46 32 29 46 69 116 147 176 35 35 40 55 75 168 173 159 40 38 46 69 116 165 199 162 40 49 64 84 147 251 231 179 52 64 107 162 197 255 255 223 69 101 159 185 234 255 255 255 142 185 225 251 255 255 255 255 208 255 255 255 255 255 255 255
Quantization table (Cb/Cr)	3 3 5 9 19 19 19 19 3 4 5 13 19 19 19 19 5 5 11 19 19 19 19 19 9 13 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19 19		49 52 69 136 255 255 255 255 52 61 75 191 255 255 255 255 69 75 162 255 255 255 255 255 136 191 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255
Preview DHT	static tables	created dynamically	static tables
DC (Y)	2 1 3 3 2 4 3 5 5 4 4 0 0 1 125		0 1 5 1 1 1 1 1 1 0 0 0 0 0 0 0
DC (Cb)	3 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0		0 2 1 3 3 2 4 3 5 5 4 4 0 1 125
DC (Cr)	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
AC (Y)	2 1 3 3 2 4 3 5 5 4 4 0 0 1 125		2 1 3 3 2 4 3 5 5 4 4 0 0 1 125
AC (Cb)	2 1 2 4 4 3 4 7 5 4 4 0 1 2 119		2 1 2 4 4 3 4 7 5 4 4 0 1 2 119
AC (Cr)	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

parameters that are stored in the metadata. The two JPEG compressed preview or thumbnail images were analysed in the same manner as JPEG preview images by Kee et al. [2]. From each image the dimensions as well as the quantization and Huffman table parameters were collected. From the uncompressed thumbnail image only the dimensions were collected. Not every camera creates all preview or thumbnail images. In this case the parameters of the missing images are set to 0.

2) Metadata Parameters : From the metadata in the IFD#0 segment we collect the count of all 6 IFD segments. From the EXIF segment, EXIF metadata and Makernotes are counted separately. Additionally we count the number of additional image IFDs.

(1) IFD#0
(2) EXIF IFD
(3) Makernotes
(4) Interoperability IFD
(5) thumbnail/preview image IFD
(6) thumbnail/preview image IFD
(7) additional image IFDs
(8) raw image data IFD

As the IFD#0 segment itself contains a thumbnail or preview image, (6) and (7) represent one of the other images in the order they appear in the file. Missing segments in this sequence and images that are not stored in a sperate IFD segment are set to 0.

D. Examination Results

Canon cameras proof to be the most consistent in the general structure of the RAW files they produce. Only the compression format of one of the thumbnail images varies between uncompressed and JPEG compression in different camera models. The other JPEG compressed thumbnail image has a constant size of 160×120. All Canon camera models have a static set of quantization and Huffman tables for each JPEG compressed thumbnail and preview image. The Huffman Table is identical throughout Canons camera range. In their higher priced camera range Canon has introduced the M-Raw and S-Raw formats as options to regular RAW images. In order to enhance the time and memory space these RAW images need for being stored, they only have a medium or small file size compared to the original. Consequently there are different signatures for different RAW types from every of these camera models. The main difference of these formats lies in the resolution of the raw image, other parameters are the same.

The general structure of NEF files is less consistent throughout the files created by different Nikon camera models. Not every Nikon camera creates every preview and thumbnail IFD. Nikon D800E and D4 cameras even add an additional preview image IFD to the structure. The uncompressed thumbnail image has a constant size of 160×120. The JPEG compressed thumbnail image has in most cases a size of 570×375. Nikon cameras adapt their quantization and Huffman tables with every image. A variation in whether the 'ISO' entry in the EXIF segment is used, depending on the ISO settings creates two different metadata signatures for some Nikon camera models. These varying parameters lead to a number of different possible signatures for one single camera model.

Except for the K-01 model, Pentax cameras examined are as consistent as Canon cameras. Just as Nikon cameras they create uncompressed thumbnail images with a size of 160×120. The other JPEG compressed thumbnail image has a static size of 640×480. Quantization and Huffman tables are, except from the K-01 model, static. All Pentax camera models examined even use the same Huffman table. Once converted to DNG format, RAW files will loose their original signature. The metadata structure changes, thumbnail and preview images get recreated with different dimensions, quantization and Huffman tables. The only characteristic properties unaltered are the dimensions of the raw image and the Makernotes count. Although the signature of RAW files converted to DNG depends on the original file, some parameters, such as the quantization and Huffman tables are characteristic to DNG Converter.

All cameras examined create a unique parameter signature. Metadata proves to be the most significant property of RAW images, closely followed by the sensor and thumbnail/preview dimensions. 63% of the Canon cameras examined have a unique combination of all 8 metadata parameters, 37% are in a class of size 2. All Nikon cameras create unique metadata signatures. From the metadata entries the Makernotes count is the most distinct.

NEF images, in which date and time entries have been altered using ExifTool, can still be detected as the 'OriginalDate' entry in the EXIF segment is deleted in the process. When resaving NEF files, ExifTool also changes the sequence of the files segments. In altered files the EXIF IFD including the Makernotes is put at the end of the file. Although a change in the segment sequence is not detectable by the method proposed in this paper, it indicates detectability by the method proposed by Gloe [3]. In CR2 files, altered with ExifTool could not be detected by our method.

E. Forensic Software

Most software packages that can be used to alter RAW images also provide functionalities to analyse them. ExifTool can visualize the file structure and reasonable number of entries in the different segments. Furthermore allows to extract preview and thumbnail images from CR2 and NEF files. JPEG preview and thumbnail images can also be extracted and then analysed using JPEGSnoop. It can extract all header information and provide a list of possible source devices, based on the files characteristics. But as Kornblum [6] mentioned in his paper, it's prediction abilities are limited to static cases. Using static DQT and DHT with a database of characteristics it takes a guess on the source camera or processing software. This database is fed by users of JPEGSnoop, by committing the characteristics of unknown camera models. For most preview images, extracted from CR2 images, JPEGSnoop listed the camera model used in a list of possible source devices. Dave Coffin's open source library DCRAW [14] offers a variety of functions. A command line based on DCRAW can be used to decode a RAW image file, save them as an JPEG or TIFF files and extract metadata or preview images.

F. Forensic Databases

To increase the effectivety of the techniques discussed and to decrease the costs of an investigation trustworthy databases, that store the characteristics and sample images of various cameras or software packages are needed. Fortunately, several multimedia forensic groups are building such databases for research purposes. One of these is the 'Dresden Image Database' [15], which provides sample images in different formats.

IV. Conclusion

Taking a closer look at their structure, this paper identified characteristics in common RAW image files that can be used in a file forensic analysis. Results of the examination indicate that an authentication based on CR2, NEF or DNG file information can be as effective as it is based JPEG file headers. We have also shown that there are still alterations undetectable by this method. Modifying already existing metadata entries such as date and time does not in all cases leave characteristic traces in the file structure.

Appendix

Definitions

JPEG — is commonly used to refer to the JPEG Image File Format (JFIF) and its compression algorithm proposed by the JPEG commission.

RAW — is a general term that refers to a huge variety of lossless image file formats used by manufacturers of digital photo cameras.

References

[1] D. W. Cromey, "Avoiding twisted pixels: Ethical guidelines for the appropriate use and manipulation of scientific digital images," *Science and Engineering Ethics*, vol. 16, no. 4, pp. 639–667, 2010. I

[2] E. Kee, M. Johnson, and H. Farid, "Digital image authentication from jpeg headers," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 1066 –1075, sept. 2011. I, II-A, III-C1

[3] T. Gloe, "Forensic analysis of ordered data structures on the example of JPEG files," in *submitted to WIFS'2012, December, 2-5, 2012, Tenerife, Spain*, 2012. II-A, III-D

[4] JEITA, *Exchangeable image file format for digital still cameras: Exif Version 2.2*, April 2002. [Online]. Available: http://www.exif.org/Exif2-2.PDF II-A

[5] P. Alvarez, "Using extended file information (exif) file headers in digital evidence analysis," *International Journal of Digital Evidencen*, vol. 2, no. 3, pp. 1–5, 2004. II-A

[6] J. D. Kornblum, "Using JPEG quantization tables to identify imagery processed by software," *Digital Investigation*, vol. 5, no. Supplement 1, The Proceedings of the Eight Annual DFRWS Conference, pp. 21–25, 2008. II-A, III-E

[7] H. Farid, *Digital Image Ballistics from JPEG Quantization*, 2006. II-A

[8] H. Farid, *Digital Image Ballistics from JPEG Quantization: A Followup Study*, 2008. II-A

[9] E. Kee and H. Farid, "Digital image authentication from thumbnails," in *SPIE Symposium on Electronic Imaging*, San Jose, CA, 2010. [Online]. Available: www.cs.dartmouth.edu/~erickee/papers/spie10.pdf II-A

[10] Canon, *CIFF - Specification on Image Data File*, December 1997. III-A

[11] Adobe, *Digital Negative (DNG) Specification, Version 1.3.0.0*, June 2009. [Online]. Available: http://www.adobe.com/content/dam/Adobe/en/products/photoshop/pdfs/dng_spec.pdf III-A

[12] P. Harvey, "Exiftool - read, write and edit meta information," 2012. [Online]. Available: http://www.sno.phy.queensu.ca/~phil/exiftool/ III-B

[13] Adobe, "Adobe dng converter 7.1," 2012. [Online]. Available: http://www.adobe.com/support/downloads/detail.jsp?ftpID=5389&promoid=DTEHR III-C

[14] D. Coffin, "Dcraw, decoding raw digital photos in linux," 2011. [Online]. Available: http://www.cybercom.net/~dcoffin/dcraw/ III-E

[15] T. Gloe and R. Böhme, "The dresden image database for benchmarking digital image forensics," *Journal of Digital Forensic Practice*, vol. 3, no. 2-4, pp. 150–159, 2010. [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/15567281.2010.531500 III-F