B13 Utility of Quantization Tables for Digital Image Authentication

Amanda E. Broyles, MAM, Federal Bureau of Investigaion, Building 27958A, Quantico, VA 22135; and Richard W. Vorder Bruegge, PhD, Federal Bureau of Investigaion, OTD-FAVIAU, Building 27958A, Pod E, Quantico, VA 22135*

After attending this presentation, attendees will understand what a JPEG quantization table is, how they differ among manufacturers, and how this information can be used in image authentication examinations.

This presentation will impact the forensic science community by reinforcing the value of metadata analysis in digital image authentication and providing another avenue through which claims of image manipulation can be addressed.

The process of digital image authentication usually incorporates an assessment of the metadata contained within the digital image file. This can include information on the make and model of the camera used to take a picture, as well as other information such as date and time or camera settings like shutter speed, aperture, or image size (in pixels). This type of metadata often serves to provide circumstantial evidence regarding the source of a questioned image. For example, if image files depicting child pornography are found on a suspect's computer and the files contain metadata indicating the same make and model as the camera found next to the computer, then this provides compelling evidence that the camera was used to record those image files. Likewise, if the time and date indicated in the metadata correspond to a time when the suspect had access to the camera and victim, this provides additional circumstantial evidence. The mere presence of camera metadata in a digital image file is often cited as support for the authenticity of the file and the scene depicted therein.

However, because there is the potential that such metadata can be falsified (or "spoofed"), the value of such analysis in these cases may be limited, depending upon the specific type of metadata in question. For example, it is a relatively straightforward process to manually modify the time and date metadata using a hex editor, while leaving no trace of this modification. On the other hand, other types of metadata may be very difficult to falsify. This paper addresses one such type of metadata – JPEG quantization tables.

Quantization tables are used to define the amount of compression an image file will undergo when subjected to JPEG compression. A quantization table includes a total of 192 values, broken out into three sets of 64 values. The first set affects the luminance of the image, while the second and third sets affect the chrominance. When a digital camera user selects an image quality setting such as "Fine," "Normal," or "Basic," they are typically selecting a specific quantization table that has been predefined by the camera manufacturer. In some cases, the manufacturer will also use a different quantization table for images of different size (or resolution). Based on an analysis of approximately 200 cameras, Farid[1] suggested that the quantization table could be used to narrow the source of an image to a small subset of camera makes and models. Subsequently, after examining 1,000,000 images, Farid[2] identified a total of 10,153 combinations ("classes") of camera make, model, resolution, and quantization table. The fact that a given camera make and model can generate files of the same size with different quantization tables typically reflects variations in the quality setting. Therefore, in order to completely spoof a digital camera image, the manipulated file must also include the correct quantization table.

The work described in this paper extends the analysis of quantization tables contained in digital images to the "thumbnail" images included within many digital image files. "Thumbnail" images are reduced size versions of images that are used for ease of display either on a camera monitor or within a computer browser. They are complete digital image files in and of themselves, so they can have their own quantization tables. As a result, digital camera image files can have more than one set of quantization tables – one for the thumbnail and one for the full size image. The quantization tables for the full size image and the thumbnail image usually are different, which means that any spoofing attempt must utilize two quantization tables, making it more difficult.

Further complicating spoofing attempts is the fact that one cannot simply modify the quantization tables using a hex editor, since this can result in dramatic modifications to the image quality. Likewise, commercially available image processing applications such Adobe Photoshop will typically utilize a small set of quantization tables that differ from those of camera manufacturers, meaning that any manipulated image will have to be reprocessed outside of Photoshop to create a falsified quantization table if the proper quantization tables are to be generated. Finally, additional properties of thumbnail images generated by digital cameras as opposed to image processing will be described, such as size, orientation, and framing.

References:

1 Farid, H. Digital Image Ballistics from JPEG Quantization, Technical Report TR2006-583, Dartmouth College, Computer Science, 6 pp, 2006. Accessed July 27, 2009. (www.cs.dartmouth.edu/farid/publications/tr06a.html)

2 Farid, H. Digital Image Ballistics from JPEG Quantization: A

 ** Presenting Author*