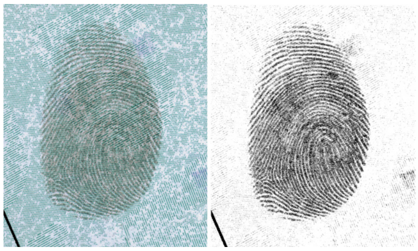
Digital Image Integrity

TABLE OF CONTENTS

The integrity of a digital image is paramount in fields such as forensic, medical imaging, military, and industrial photography. Courts make decisions affecting an individual's liberty based, in part, on images presented as evidence. Physicians and researchers make diagnoses based on imaging—holding people's lives in the balance. Military photographs may be used to determine target locations based on their content and interpretation. Industrial photographs depict defects in materials that could lead to faulty and dangerous consumer products if not discovered.

Because it is frequently necessary to make corrections and adjustments to images (for example, to separate one type of cell from another, or to enhance a fingerprint), it is important to maintain the integrity of images from capture through final usage. To address this issue, the creator of an image can follow best practices that maintain an archive image, restrict access to the archive image, require work to be done only on copies of the archive image, and then provide an audit trail of any adjustments made to the image.

In the case of nonraw file formats, the archive file is the original file itself. In the case of raw files, the DNG format with an embedded raw file is an excellent solution for the archive file—providing an archive of the raw file plus the information associated with any image adjustments made in Adobe® Camera Raw or another raw image processor.



The image on the left shows a fingerprint on a check.
The image on the right shows a fingerprint that has been bleached and altered for clarity.

Viability of digital images

Are digital images intrinsically viable in the above-mentioned fields? Comparing digital imaging to silver-based photography puts many issues into perspective. The question is whether digital imaging technology prevents this medium from use in fields in which image integrity is paramount. If not, what methods must be employed to meet the requirements of the fields?

Silver-based photographic images have been manipulated, altered, and faked for over 150 years. Dino Brugioni's *Photo Fakery* (published by Brassey's Inc., 1999) shows images from the 1850s to the late 20th century in which multiple negatives were used to create scenes that never existed, or were otherwise manipulated. Throughout history silver-based images have been manipulated—often for political reasons.

Digital imaging doesn't create the possibility of image manipulation; it merely provides an additional technology for image manipulation, and for the detection of it. Therefore, the potential of image manipulation is not unique to digital images. With digital-imaging technology and a film original, you can scan a roll of negatives, manipulate the images and output them to a film recorder, and create a new set of negatives. There is no metadata stored with an analog image as there is with a digital photograph. If a digital photograph is altered, the associated metadata will reveal the alteration; any break or inconsistency in the metadata will be a clue to the manipulation, making digital originals more difficult to manipulate than film originals.

Digital imaging is as viable as any other imaging technology and is perhaps even better than analog photography for showing the provenance of an image. In forensic, scientific, military, and industrial applications, those who create and work with images should utilize best practices with all imaging media.

Best practices

Best practices are policies or rules that provide guidelines for procedures and workflow, and should incorporate (and may go beyond) any industry-side standards. You can use best practices to maintain the integrity of a digital imaging workflow.

A typical best-practices policy incorporates maintaining an archive image, only working on copies of the archive image, maintaining an audit trail, and employing only valid image processing procedures.

Archive images

Maintaining an unaltered archive image is essential to the workflow in most technical, medical, forensic, and military applications. A viewer can compare the archive image and the final image to determine if the image content or quality has been altered. Maintaining an archive image also ensures that any user can verify that the procedures used to make adjustments to it are reproducible and valid.

The Federal Bureau of Investigation (FBI) formed the Scientific Working Group on Imaging Technologies (SWGIT) in the mid 1990s to address some of the issues surrounding the use of digital imaging in forensics, among other issues. The SWGIT guidelines (www.fdiai.org/images/SWGIT guidelines.pdf) provide recommendations for photography and digital imaging in forensics. SWGIT recommends maintaining an archive image, and defines the archive image as "Either the primary or original image stored on media suitable for long-term storage." The primary image is defined as "…the first instance in which an image is recorded onto any media that is a separate, identifiable object or objects. Examples include a digital image recorded on a flash card or a digital image downloaded from the Internet." In other words, an archive image is an exact copy of what the camera recorded onto its original media.

If the original image was captured as a JPEG or TIFF file, the archive image will be an exact copy of it in the same format. TIFF and JPEG captures have distinct limitations—they are processed within the camera and are limited to 8 bits per channel during their camera processing. In addition, recovering highlights is impossible, and adjustments to color balance, contrast, and brightness can quickly deteriorate the image quality.

If the original was captured in a raw format, it is important to also retain information on any image adjustments made when the raw image is opened or converted. Raw files are, by definition, read-only, and contain unprocessed data from the digital camera that must be processed when opened. Raw files opened with the Camera Raw plug-in may contain a hidden sidecar file, or this information may be placed in a database on the host computer—depending on user preferences. In either case, it is important (but not intuitive) to keep this information with the file when the file is moved or archived. With raw file formats, the archive image includes the raw file plus the sidecar file.

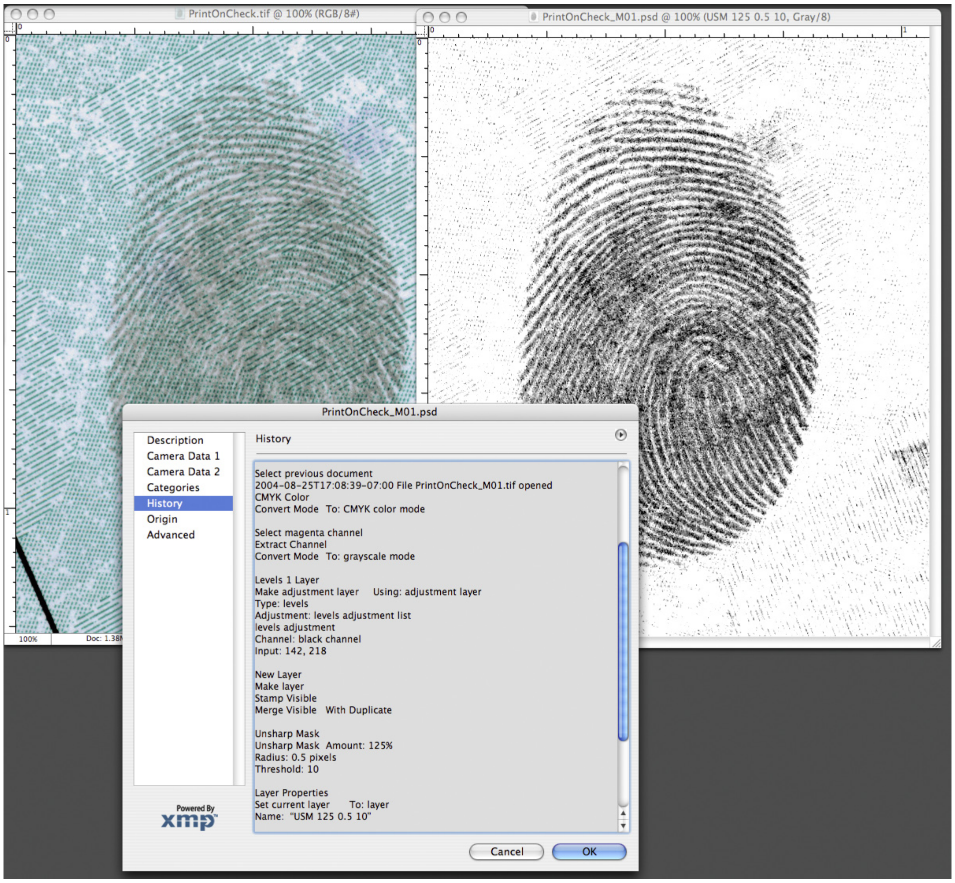
Raw formats can provide images with greater bit depth (10, 12, or more, depending on the camera). When opened using the Camera Raw plug-in, raw images provide many advantages in addition to their higher bit depth, such as color balance, brightness, and contrast adjustments that are nearly lossless.

Taking advantage of raw file formats is essential to getting the best image, and this is where the DNG format comes into play. Without the DNG file format, there is no guarantee that the settings used when opening the file are archived with the raw file. Using the DNG format with the raw file embedded provides the quality improvements of the raw format and the maintenance of the image adjustments as part of a single archive file.

Audit trail

In most fields, it's often necessary to make adjustments to images. For example, an image presented in court or analyzed for medical evaluation may have gone through several adjustments after it was captured. A question may arise as to whether the adjustments made were valid for the application, or if the adjustments resulted in a misrepresentation of the image.

In forensics, an image that was taken under fluorescent lighting may need color correction to eliminate the green cast, or a fingerprint image may benefit from a contrast boost and image sharpening. In medical imaging, applying false colors to the tonal range may help isolate, identify, and quantify a specific type of bacteria. Various methods of image processing used to identify product defects are important tools in industrial photography.



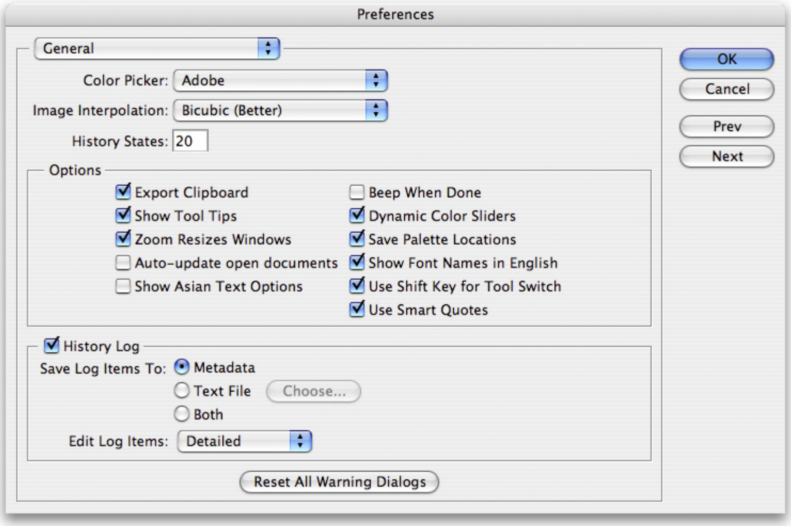
History

```
Select previous document
2004-08-25T17:08:39-07:00 File PrintOnCheck_M01.tif opened
CMYK Color
Convert Mode  To: CMYK color mode

Select magenta channel
Extract Channel
Convert Mode  To: grayscale mode

Levels 1 Layer
Make adjustment layer    Using: adjustment layer
Type: levels
Adjustment: levels adjustment list
levels adjustment
Channel: black channel
Input: 142, 218

New Layer
Make layer
Stamp Visible
Merge Visible  With Duplicate

Unsharp Mask
Unsharp Mask  Amount: 125%
Radius: 0.5 pixels
Threshold: 10

Layer Properties
Set current layer     To: layer
Name:  "USM 125 0.5 10"
```

This figure shows the history of modification to an image of a fingerprint.

Using a method of tracking changes to create an audit trail shows whether valid procedures were used, how each procedure affected the image, and allows the procedures to be repeated with similar results. In Adobe Photoshop® CS and later, an image creator can automatically record an audit trail by turning on the History Log feature in the Preferences panel. Each tool and feature used can be recorded, along with the parameters used for the given tool, filter, or adjustment. There are some exceptions, however, including the exact shape of Lasso tool selections and the paths of brush strokes of any of the painting or dodging/burning tools.

The History Log can be recorded directly into the image's metadata or as a separate text file, depending on the preference set in the General Preferences panel. If the log is stored in metadata, it can be viewed in the File Info panel, or in the Metadata window in the File Browser.



Preferences

General

Color Picker: Adobe

Image Interpolation: Bicubic (Better)

History States: 20

Options

☑ Export Clipboard
☑ Show Tool Tips
☑ Zoom Resizes Windows
☐ Auto-update open documents
☐ Show Asian Text Options
☐ Beep When Done
☑ Dynamic Color Sliders
☑ Save Palette Locations
☑ Show Font Names in English
☑ Use Shift Key for Tool Switch
☑ Use Smart Quotes

☑ History Log

Save Log Items To: ● Metadata
○ Text File Choose...
○ Both

Edit Log Items: Detailed

You can select the History Log in the General Preferences panel.

In earlier versions of Photoshop, recording an audit trail required a plug-in or had to be done manually. To store the audit trail in the file's metadata, the image creator could have typed the information in one of the fields in the File Info panel.

Repeatability of image adjustments

When a technology is challenged in court, a Kelly-Frye or a Daubert hearing may be called to determine if the technology is valid. Digital imaging technology has gone through three such hearings since 1991. In his paper About Forensic Digital Imaging (www.imagingforensics.com/forensic.pdf) Erik Berg states, "State of Washington vs. Eric Hayden serves as an affirmation of the conclusion reached in the Commonwealth of Virginia vs. Robert Douglas Knight case. It also imposes the same requirements for digital images as those placed upon other types of evidence. …Any enhancement techniques must be reproducible, so that notes about the enhancement process, as well as who did the work should be maintained."

The need for image processing techniques to be repeatable and produce similar results is a cornerstone in forensics applications. For any technique to be reproducible, the technique must be performed on the same image or an exact copy of that image. With raw files, it is essential that experts open the images using the same settings in order to have the same starting point. If one expert opens the image in Adobe RGB color space, with a color temperature setting of 5500 in 16-bit mode, and another opens the same raw file in the sRGB color space with a color temperature setting of 4500 in 8-bit mode, it is like starting with two different images.

The DNG format with embedded raw files resolves this problem by creating a single image that contains the raw file along with the information about any adjustments made in the raw file conversion process.

History of tools to address issues of archive images

Since the early 1990s, camera and software companies have created products to provide various sorts of archive images, audit trails, and image authentication systems. Some of these products have provided the basis for the present raw files and audit trails.

Perhaps the earliest attempt to create a proprietary archive image format was the Kodak KDC file format. This format required either Kodak software or a Kodak plug-in to open the image. Like current raw formats, it was an unchangeable format, meaning that you couldn't save an image to KDC format. It also contained some metadata, including camera make and model, shutter speed and f-stop. The drawback to this format was that it wasn't universal and had limited bit depth—but it led the way to more powerful raw file formats.

In 1999, Olympus developed the Image Authentication System for use with two of its point-and-shoot digital cameras. This system required software to be installed in both the camera and the computer. Running the software would verify if an image had been altered.

Canon currently has a Data Verification Kit for the EOS 1Ds and EOS 1D Mark II cameras, which functions much like the Olympus system, but requires a dedicated memory card as well. Canon states that its system will detect any changes to the image, even as small as 1 bit.

Lexar has announced its Locktight security system, which can prevent a memory card from being used in an unauthorized camera or downloaded onto an unauthorized computer.

Most camera manufacturers now offer a raw file format from digital cameras. The benefit of raw formats, as related to digital image integrity, is that they are virtually unalterable. Raw file formats are read-only, which makes them difficult to alter without leaving traces that experts can detect. With the DNG format, one can now take that raw file and embed it, plus any adjustments made to it in a raw file processor, and archive this as a single file. The DNG file format provides an open source format that meets the needs of the forensics, medical, military, and industrial fields for archiving. As more software and hardware manufacturers support the DNG format, it will become the standard for archiving raw files in a secure manner that will meet the needs in fields in which image integrity is essential.

ABOUT THE AUTHOR

George Reis is the owner of Imaging Forensics Inc., which provides consulting and training services in forensic applications of imaging technologies, and image analysis support for court cases. He has testified as an expert in photography and in image analysis in courts in California and Hawaii.

He has been a Crime Scene Investigator, Forensic Photographer, and Fingerprint Technician with the Newport Beach (CA) Police Department from 1989 to 2006 and introduced digital imaging technology to that agency in 1992.

Imaging Forensics has provided training and consulting services to thousands of individuals, and represented hundreds of police and government agencies since 1995. These agencies include the US Secret Service, US Army Crime Lab, Missouri State Crime Lab Supervisors, Arkansas Criminal Justice Institute, Colorado Bureau of Investigation, San Francisco Police Department, Los Angeles Sheriff's Office, St. Louis County Police Department, and numerous state, county, and municipal agencies throughout the country.

Adobe Systems Incorporated
345 Park Avenue, San Jose, CA 95110-2704 USA
www.adobe.com