

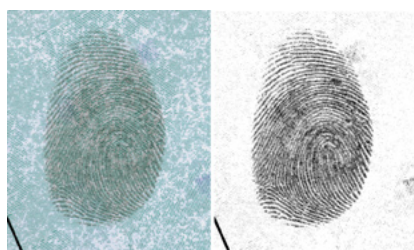
Digital Image Integrity

TABLE OF CONTENTS

- 1 Viability of digital images
- 2 Best practices
- 2 Archive image
- 3 Audit trail
- 4 Repeatability of image adjustments
- 5 History of tools to address issues of archive images

The integrity of a digital image is paramount in fields such as forensics, medical imaging, and 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 determine target locations based on their content and interpretation. Industrial photographs depict defects in materials that could lead to faulty and dangerous consumer products.

Because making corrections and adjustments to images is frequently necessary—whether to separate one type of cell from another or to enhance a fingerprint—it is important to maintain the integrity of all 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 others to work only on copies of the archive image, and provide an audit trail of any adjustments made to the image.



The image on the left shows a fingerprint on a check.

The image on the right shows a fingerprint that has been bleached/alterd for clarity.

Viability of digital images

Are digital images intrinsically viable in these fields? Comparing digital imaging to silver-based photography often brings up surprises and puts many issues into perspective.

Silver-based photographic images have been manipulated, altered, and faked for over 150 years. And, it is probably easier to get away with falsifying an image that was originally recorded on film.

“Are digital images intrinsically viable in these fields?” With film, someone can scan a roll of negatives, manipulate the images, output them to a film recorder, and create a new set of negatives. Unlike a digital photograph, there is no metadata stored with an analog image. 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. Another advantage of a digital image is that the tools to analyze a digital image enable the viewer to look at very fine edge detail and find resolution mismatches, differences in noise signatures, and other clues.

Regarding the history of image manipulation, Dino Brugioni's *Photo Fakery* (published by Brassey's Inc., 1999) shows images from the 1850s that used multiple negatives to create scenes that never existed. And, throughout history silver-based images have been manipulated—often for political reasons. Digital imaging doesn't create the possibility of image manipulation; digital imaging merely provides an additional technology for it, and for the detection of it.

Digital imaging is as viable as any other imaging technology and is perhaps even better than analog photography. However, in forensic, scientific, military, and industrial applications, people 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. Best practices should incorporate any industry-wide standards or requirements, and may go beyond them. Best practices help maintain the integrity of a digital imaging workflow.

A typical best-practices policy incorporates the items discussed below.

Archive image

Maintaining an unaltered archive image is essential to the workflow in most technical and medical fields, forensics, 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 (<http://www.fdiai.org/images/SWGIT%20guidelines.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 in the JPEG or TIFF format, the archive image will be that file (or an exact copy of it) in that 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, brightness, and so on can quickly deteriorate the image quality.

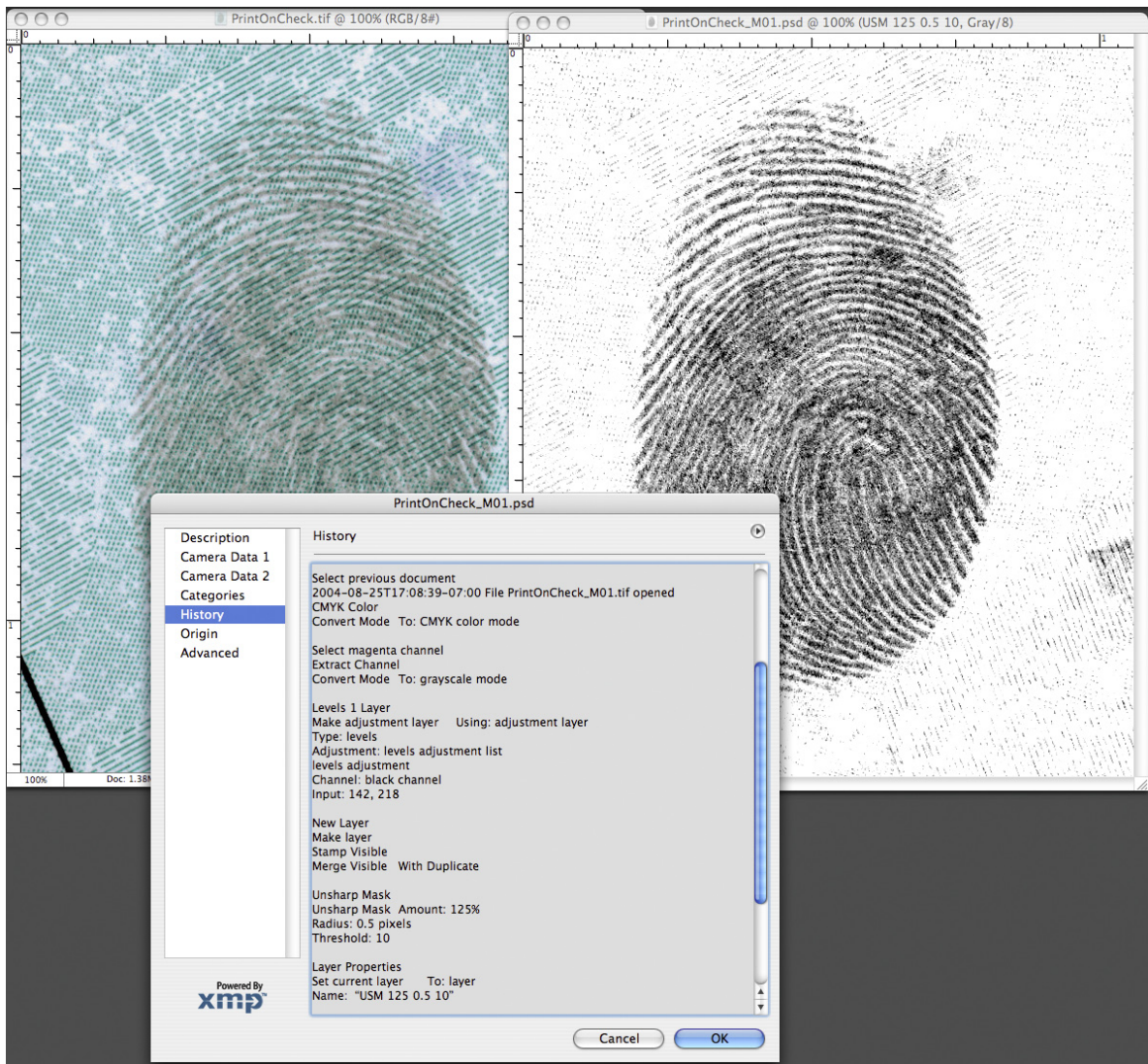
If the original was captured in a raw format, it is important to also retain the information on any image adjustments that are made when the raw image is opened or converted. Raw files are, by definition, unalterable (read-only) file formats. These files contain the unprocessed data from the digital camera and must be processed upon opening. Raw files opened with the Adobe® 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 the 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 is the raw file plus the sidecar file.

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

Audit trail

In some fields, making adjustments to images is often required. 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.

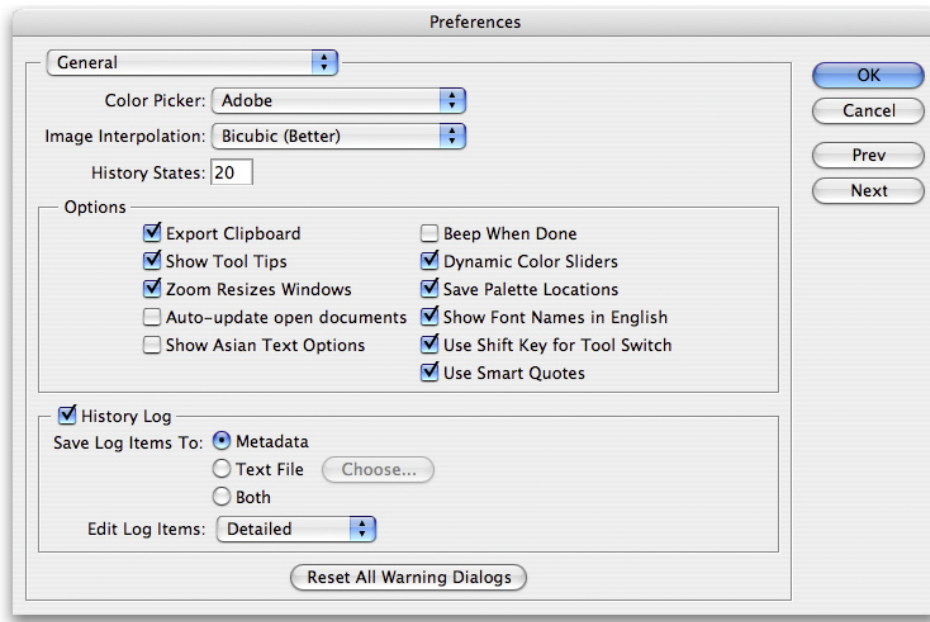
In forensics, an image that was taken under fluorescent lighting may need color correction to eliminate the green cast for courtroom use, or a fingerprint image may benefit from a contrast boost and image sharpening. In medical imaging, restricting the tonal range may help isolate, identify, and quantify a specific type of bacteria. Infrared imaging, and image processing algorithms to identify product defects, provide important tools in industrial photography.



This figure shows the history of modification of a fingerprint.

Utilizing a method of tracking changes to create an audit trail will show if valid procedures were used and how each procedure affected the image, and will allow the procedures to be repeated with similar results. In Adobe Photoshop CS, an image creator can automatically record an audit trail by invoking the History Log feature in the Preferences pane. Each tool and feature used can be recorded, along with the parameters used for the given tool, filter, or adjustment. There are some exceptions to this, 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 user preference set in General Preferences. If the log is stored in metadata, it can be viewed in the File Info pane, or in the Metadata window in the File Browser.



You can select the History Log in General Preferences.

In earlier versions of Photoshop, recording an audit trail either 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 pane.

Repeatability of image adjustments

When a technology is challenged in court, a Kelly-Frye hearing 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* (<http://www.pcprosus.com/About%20Forensic%20Digital%20Imaging.pdf>), Erik Berg describes a significant case that occurred in 1995 (*State of Washington v. Eric Hayden*). 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 by using the same settings in order to have the same starting point. If one expert opens the image in the 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. This creates a potential problem and shows the importance of carefully retaining the sidecar files with the raw files.

History of tools to address issues of archive images

Since the early 1990s, camera and software companies have introduced 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 images. Like current raw formats, it was an unchangeable format, meaning that you couldn't save an image in the 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 on the computer would verify if the image had been altered.

Canon currently has a Data Verification Kit for the EOS-1Ds and EOS-1D Mark II cameras. This 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.

Watermarks have also been used to authenticate digital images. An image creator can embed watermarks into a digital image; then, if the image is changed, software cannot only show that the image was altered, but also show where it was altered.

Many 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. This is a benefit for archival purposes and for forensics experts, but at the same time it leads to one of raw's greatest limitations. When a raw file is opened, the raw data is read from disk and processed into a file that can be viewed on a computer monitor. This completely transforms it from its raw state, and the data cannot then be resaved in a raw format. The processing information used when a raw file is opened cannot ever become part of the original archive file. So although the raw file largely retains its integrity as an unaltered file, it doesn't include processing information that is frequently crucial to forensics.



George Reis

George Reis is the owner of Imaging Forensics Inc., providing 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 2004 and introduced digital imaging technology to that agency in 1992.

Imaging Forensics has provided training and/or consulting services to thousands of individuals, representing 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.

<http://www.imagingforensics.com>