Washington University Journal of Law & Policy

Volume 10 *Access to Justice: The Social Responsibility of Lawyers*

January 2002

Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images

Jill Witkowski
Washington University School of Law

Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images

Jill Witkowski*

I. INTRODUCTION

The dawn of the new millennium has revealed the electronic revolution that is sweeping the globe. Computers and the Internet now dominate the 21st century global culture. New computer-related technology emerges daily and the falling costs of such technology make it increasingly available to the average consumer. As computer technology makes its way into the courtroom, it is important to ensure that the underlying principles of law are not lost in the embrace of new technology.

Digital imaging is one area in which the legal community may be too hastily adopting new technology without fully considering the ramifications of its use. While NASA and the military have used digital imaging for decades, skyrocketing law enforcement and consumer use of the technology should convince the legal community to examine the legal issues surrounding the use of digital images.[1]

This Note examines the legal community's current treatment of digital images. It discusses how authentication methods used for traditional photographs are inadequate to sufficiently answer the unique legal problems posed by digital images. This Note proposes a new method of authentication for digital images.

Part II of this Note emphasizes the differences between digital images and photographs, in both the image creation process and

* J.D., Washington University School of Law, 2002.

1. Herbert L. Blitzer, *Digital Imaging: Digital Imaging Can Be a Boon to Law Enforcement, if it's Done Right*, LAW ENFORCEMENT TECH., at 16 (Feb. 2000) [hereinafter, Blitzer, *Digital Imaging*].

susceptibility to manipulation. Part III introduces the multiple methods of authentication for photograph-like evidence, including sound recordings, video recordings, and computer-generated evidence. Part IV illustrates how the current system does not respond to concerns raised by the increased use of digital images. Finally, Part V proposes a new method for authentication of digital images.

II. DIGITAL IMAGES ARE NOT PHOTOGRAPHS

Digital imaging presents the most recent trend in photographic technology.[2] Digital cameras operate by principles similar to traditional cameras.[3] There are significant differences, however, between traditional photographs and digital images that may necessitate different evidentiary treatment than that normally given to

---

2. Advantages of digital imaging include convenience and versatility. Most digital cameras have an LCD screen that allows the user to view the image immediately after capture. If a user does not like the image, she can erase the image and take the shot again. The electronic nature of digital images allows for instant copying and transmission over the Internet, which may be especially advantageous for law enforcement agencies. Many cameras also come equipped with audio and/or video recorders that allow users to log important information about the details of the image captured.

Digital cameras also provide lower processing costs and therefore may be cheaper than traditional photography in the long run. Unlike traditional photography, where development costs are high, digital photography allows a user to view images on a computer first and then choose which images to print. In addition, the lack of film developing chemicals makes digital photography more environmentally friendly. *See* Scientific Working Group on Imaging Technologies, *Guidelines for Field Applications of Imaging Technologies*, Version 2.0 (June 8, 1999), *reprinted in* 2 FORENSIC SCIENCE COMMUNICATIONS, (2000) *available at* http://www.fbi.gov/hq/lab/fsc/backissu/jan2000/swigit.htm (last visited Nov. 11, 2002).

3. Unlike traditional cameras, which store information on film, digital cameras store information on an image sensor. *See generally* Dennis P. Curtin, *A Short Course in Choosing a Digital Camera*, Short Courses Website, *at* http://www.shortcourses.com/choosing/contents.htm (last visited Nov. 11, 2002). An image sensor, either a Charge Coupled Device (CCD) or a Complementary Metal Oxide Semiconductor (CMOS), is a solid state device that contains hundreds of thousands or millions of photosensitive diodes called photosites. *Id*. § 3. Each photosite records a charge proportionate to the brightness of the light that falls on it. *Id*. When the shutter closes, the exposure is complete, and the image sensor "remembers" the charges. *Id*. The captured image is read one row at a time by either an interlaced scan, which processes every other row and then fills in the image by processing the remaining rows, or by a progressive scan, which processes one row after another. *Id*. The scanned image is transferred to a read out register, fed to an amplifier, and then sent to an analog-to-digital converter. *See* Curtin, *supra* § 3. Once the converter reads a row, it is deleted from the read-out register and the next row is read. *Id*.

traditional photographs.[4] The digital image creation process and the susceptibility of digital images to manipulation make digital images sufficiently different from photographs to necessitate different treatment under the Federal Rules of Evidence.[5]

A. Digital Image Creation Process

Two facets of the digital image creation process separate digital images from traditional photographs: initial image quality and compression.

The quality of the initial images produced by photographs and digital images distinguishes the two technologies. Images taken by a digital camera vary dramatically from those taken by a traditional film camera. Digital cameras produce lower quality images than those produced by 35mm film. Typically, 35mm film yields better resolution, a higher dynamic range, and better color range and fidelity than digital images.[6] In contrast, digital images tend to have relatively lower resolution, and therefore poor image quality in the brightest portions of the scene being recorded.[7]

Some digital cameras are not capable of producing images of a high enough quality to be useful in court.[8] In fact, experts in the digital imaging field warn that cameras with resolution of less than one megapixel will yield results of questionable quality.[9] Moreover, because traditional film images contain as much as sixteen times the

---

4. *See infra* Part IV.

5. *See infra* Part V.

6. Herb Blitzer, *Creating the Digital Image SOP*, LAW ENFORCEMENT TECH. 58, 61 (June 2000), *available at* http://www.ifi-indy.org/articles/287_20000jun_003673.pdf (last visited Nov. 11, 2002) [hereinafter Blitzer, *SOP*]. The average 35 mm photograph has a resolution of approximately 5500 x 3600 pixels; a digital camera with a resolution of 640 x 480, therefore, contains only 1.6 percent of the information recorded on a 35 mm negative. Scientific Working Group on Imaging Technologies, *supra* note 2. While each pixel of a digital image can produce 256 levels of the three primary colors, film can produce 500 levels per color. Herbert L. Blitzer, *Forensic Imaging Options, Institute of Forensic Imaging*, *at* http://www.ifi-indy.org/articles/fio.html, (last visited May 1, 2002) [hereinafter Blitzer, *Forensic*]. Additionally, most digital cameras employ a process of color interpolation in which the digital camera only records the original color of a portion of the pixels in the image. It then guesses the color of the missing pixels by examining the surrounding pixels. Curtin, *supra* note 3.

7. Blitzer, *SOP*, *supra* note 6, at 61.

8. *Id*. *See infra* notes 13-14 and accompanying text.

9. Blitzer, *SOP*, *supra* note 6, at 58.

information as digital images, film images make better enlargements than digital images and may, therefore, be more useful in court.[10]

The possibility of digital image compression also distinguishes digital images from photographs. Unlike a traditional camera that limits the number of photographs taken to the amount of film in the camera, digital cameras allow users to choose the number of images they want to capture and store on a storage medium. Through a process called "compression," users can choose to store a greater number of images of lesser quality by permanently discarding some of the information originally contained in the digital image.[11] When the user wants to view the image, the decompression process "guesses" what information was discarded to produce a complete image.[12]

Although compression may seem a convenient way to store more images per unit of storage medium, complications arise when a user wants to print the digital image. The larger the print desired, the larger the file necessary to preserve the image integrity and produce a useable image.[13] Even though certain types of removable storage media hold insufficient data to support even one five- by seven-inch print, some digital cameras allow the user to store between twenty and twenty-four images.[14] Such large compression ratios discard a significant amount of information so that the image viewing software must then "guess" the lost information during reversal. A very high compression ratio, which saves only a small portion of the information contained in the original image, limits the size of the

10. Blitzer, *Forensic*, *supra* note 6.

11. Blitzer, *SOP*, *supra* note 6, at 59. The JPEG system is both variable and "lossy," meaning it tends to permanently lose some information, although some cameras allow users to adjust the level of compression. *Id*.

12. *See id*.; Blitzer, *Digital Imaging*, *supra* note 1, at 18-19.

13. A 4.5 MB image file should support a five-inch by seven-inch print. Blitzer, *SOP*, *supra* note 6, at 59. While one popular storage medium, the "flash card," is generally capable of holding eight to ninety-six MB of information, another popular storage medium, the floppy disk, holds only 1.44 MB of information and therefore would not store enough information to produce a sufficient five- by seven-inch print. *Id*.

14. When twenty to twenty-four images are stored on one medium, significant amounts of information will be lost in the storage process. For example, in order to store twenty to twenty-four images on a floppy disk, a digital camera compresses the image at a 65:1 ratio, meaning that for every sixty-five pixels in the original image, only one is actually stored and the other sixty-four are permanently discarded. *Id*.

print a user can produce because there is not enough information within the image file; larger prints are too "grainy" to be useful.[15] A lower compression ratio still produces an image that is less accurate than a traditional photograph. For example, compression of a digital image of a wound could, by inserting artifacts and altering colors within the image, exaggerate the wound and "create" bruises or other wounds that did not exist.[16]

B. Digital Images are Highly Susceptible to Manipulation

Digital images are easier to manipulate than traditional photographs and digital manipulation is more difficult to detect.

Digital images are highly susceptible to manipulation. Manipulation, as distinct from enhancement, consists of changing the elements of a photograph or image by changing the colors, moving items from place to place on the image, or otherwise altering the original image.[17] Individuals without training or specialized equipment may easily manipulate digital images. In fact, users do not even need specialized software to manipulate images; the same programs that allow users to view images or adjust contrast also allow users to cut and paste items with a click of the mouse.[18] Digital camera users also have a greater opportunity to manipulate images than those using traditional cameras because digital camera users process the image themselves, while traditional camera users generally take the film to a professional developer to produce the

---

15. *See id*.

16. Blitzer, *SOP*, *supra* note 6, at 58, 59-60. *See also* Blitzer, *Digital Imaging*, *supra* note 1, at 18-19.

17. In general, both traditional photographs and digital images often need to be enhanced. Enhancing an image involves adjusting the contrast so that a picture is clearer. Penney Azcarate, *Digital Imaging Technology and the Prosecutor*, PROSECUTOR, Jan.-Feb. 2000, at 26, 27. Digital camera users can enhance an image without professional assistance by using one of many software programs; users can easily enhance digital images with just a few clicks of the mouse. *See id*. While photo enhancement is generally accepted practice, photo "manipulation" is not. *See id*.

18. Certain digital imaging processing tools can significantly alter an image. The "rubber stamp," or cloning tool in Photoshop takes designated parts of an image and copies them to a different location within the same image or another image. Blitzer, *Digital Imaging*, *supra* note 1, at 19. In this way, a user could put one person's face on another person's body. *Id*. Another tool, the "eyedropper," can be used to copy colors and insert them in other locations. *Id*.

prints.[19]

While manipulation tools are both accessible and easy to use for those without training, those who have training may make even more convincing manipulations.[20] Hollywood's increasing use of digital technology is an excellent illustration of the ease of manipulation and variety of alterations possible with digital imaging.[21]

The electronic nature of the image file makes undetectable manipulation of a digital image easy, in part because no traditional "original image" is made.[22] Unlike traditional cameras, which produce one negative, digital cameras create an electronic file from which the image can be generated.[23] Because the image file contains a finite set of ones and zeros, exact copies of the image file can be made with no loss of image quality between generations.[24] Thus, it is impossible to determine which image is a first generation image and is therefore the "original."[25] The lack of an "original" for comparison with the offered image reduces the opportunity to verify that the

---

19. Indeed, one of the advantages of digital cameras is that they reduce processing costs normally associated with traditional film cameras. *See generally* Blitzer, *Forensic*, *supra* note 6.

20. Budding filmmakers are learning how to manipulate images at the University of Southern California's Robert Zemeckis Center for the Digital Arts. *See* Rick Lyman, *Monument to the Filmless Future*, N.Y. TIMES, Mar. 1, 2001, at E1.

21. Director Robert Zemeckis notes that "with digital technology there is so much that you can do with the image after you shoot it. The whole notion that what was photographed in the camera is the final image is gone forever." *Id*. With digital technology, a director can "shift the perspective of a scene, add a fresh camera movement, alter an actor's performance, transfer the location from Red Square to Times Square, speed up time, [or] slow it down . . . ." *Id*. at E10. This Note does not deal explicitly with the problems presented by evidence produced by digital video cameras, although digital still and video cameras present many of the same evidentiary issues.

22. A digital image is just a visual representation of ones and zeros and therefore may be altered, deleted or copied at will, in the same way as any other computer program, leaving no trace of the alteration. HOUSE OF LORDS SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY–FIFTH REPORT, § 2.5, Feb. 21, 1998, *available at* http://www.parliament.the-stationery-office.co.uk/pa/Id199798/Idselect/Idsctech/064v/st0501.htm (last visited Nov. 11, 2002).

23. *Id*.

24. *Id*.

25. *See id*. Some digital image experts maintain "[t]he court considers any image that can be visually seen to be an original. A print from a digital file would be considered an original. An image on a monitor would be considered an original." Ronnie L. Paynter, *Shattering Myths: Digital Imaging is a Viable Option for Crime Scene and Evidence Photography if You Know the Truth About This Technology*, LAW ENFORCEMENT TECH., Nov. 1999, at 68 (quoting George Reis, digital imaging expert with Newport Beach, California Police Department). The lack of an "original" may possibly have legal implications under the Best Evidence Rule, but this Note will not explore that possibility.

image has not been altered or has only been altered in an acceptable manner, thereby increasing the likelihood that changes will not be discovered unless the proponent of the image reveals them.

Some proponents of digital images argue that it is just as easy to manipulate a photograph as it is to manipulate a digital image.[26] Although photographs may be manipulated, the potential for making subtle but significant alterations to digital images gives cause for concern that digital images may be unfit for use as evidence in a court of law.[27]

III. DIGITAL IMAGES AS EVIDENCE: AUTHENTICATION

According to the Federal Rules of Evidence, evidence must first be relevant before it is admissible.[28] An important aspect of relevance that must be met prior to admission is authentication.[29] With the exception of a small group of documents that are considered "self-

---

26. One Commentator suggests that "Anybody with the intent, knowledge of the technology, and the financial means can manipulate most forms of evidence at will." *Id*. at 70 (quoting Leonard Pratt, law enforcement program manager at Eastman Kodak). Like digital images, photographs are also susceptible to distortion and manipulation. Photographs may be distorted in many ways, including the use of false lighting or filters, choice of lens focal length, selections of viewing distance, or through use of techniques such as "dodging" and "burning." *See* ANDRE A. MOENSSENS ET AL., SCIENTIFIC EVIDENCE IN CIVIL AND CRIMINAL CASES § 2.11 (4th ed. 1995).

Currently, the technology exists by which an operator could scan a traditional photograph, alter the image, print a new negative and then develop a photograph from the negative such that the changes to the photograph are undetectable, even by experts. *See* HOUSE OF LORDS SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY–FIFTH REPORT, *supra* note 22, § 2.11. Such technology, however, is both costly and unavailable to the general public. Thus, undetectable manipulation of digital images is exponentially more likely than undetectable manipulation of a traditional photograph.

Some commentators suggest that the ease of digitally manipulating traditional photographs by digitizing them and representing them as digital images should make all images suspect to strict scrutiny. *See id*.

27. *See* HOUSE OF LORDS SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY, *supra* note 22, § 2.11. One commentator notes that in order to change an image, a person must be able to view the photo and have access to tools that can alter it. Blitzer, *SOP*, *supra* note 6, at 61. Digital cameras that have LCD displays for immediate viewing of images do not support image editing. *Id*. Thus, if the digital image is preserved before it is viewed on a device that enables image editing, concerns regarding manipulation may be overcome. *See id*.

28. FED. R. EVID. 401. Relevant evidence may be excluded if the probative value of the evidence is outweighed by prejudicial impact of the evidence. FED. R. EVID. 403. This aspect of relevancy, while important, will not be discussed in this Note.

29. *See* 29A AM. JUR. 2D *Evidence* § 945 (1997).

authenticating,"[30] the proponent of any writing or recording must authenticate the evidence, whether the evidence is substantive or demonstrative.[31] A proponent may fulfill the authentication requirement by producing evidence sufficient to support a finding that the matter in question is what its proponent claims.[32] This part addresses general foundational requirements under the Federal Rules

---

30. FED. R. EVID. 902. Documents such as domestic public documents under seal, certified copies of public records, newspapers, periodicals, and other official publications may be admitted into evidence without further proof of their authenticity. *Id*.

31. FED. R. EVID. 901(a); *See* Dean M. Harts, *Reel to Real: Should You Believe What You See? Keeping the Good and Eliminating the Bad of Computer-Generated Evidence Will be Accomplished Through Methods of Self-Authentication and Vigilance*, 66 DEF. COUNS. J. 514, 521-22 (1999). Relevant evidence may be admitted either as demonstrative of witness testimony or for its own independent probative value. Evidence admitted for its independent probative value is known as substantive evidence. The trial judge uses a preponderance of the evidence standard to determine the initial admissibility of substantive evidence. See FED. R. EVID. 104(a). Demonstrative evidence is evidence "addressed directly to the senses without intervention of testimony [but] which illustrate[s] some verbal testimony and has no probative value in itself." BLACK'S LAW DICTIONARY 432 (6th ed. 1990). The Federal Rules of Evidence address admissibility of real and demonstrative evidence in Rules 901, 902, 1001, 1002, 1003, 1004, 1005, 1006, and 1007.

Evidence that is merely illustrative of verbal testimony and carries no independent probative value may be used as demonstrative evidence to aid a witness' testimony or to help counsel in opening or closing arguments. *See* Harts, *supra* at 516. Demonstrative evidence has been an effective courtroom tool; litigators have used chalkboards, maps, diagrams, photographs, films, and videos to help the jury understand and remember witness testimony. *See id*.

Evidence that has independent probative value is deemed substantive evidence. The trial judge uses a preponderance of the evidence standard to determine the initial admissibility of substantive evidence. *See* FED. R. EVID. 104(a). Photographs have occasionally been offered as substantive evidence under the "silent witness" theory. *See infra* notes 58-58 and accompanying text. Under such theory, the photograph "speaks for itself," in that the reliability of the photographic process frees the photograph from authentication requirements.

32. *See* FED. R. EVID. 901(b). *See also* 29A AM. JUR. 2D *Evidence* § 945 (1997). Authenticity is a question of fact for the jury to decide via procedure set out in Rule 104(b). Rule 104(b) provides: "When the relevancy of evidence depends on the fulfillment of a condition of fact [i.e., the evidence is what the proponent claims it to be] the court shall admit it upon . . . the introduction of evidence sufficient to support a finding of the fulfillment of the condition." FED. R. EVID. 104(b). However, before the evidence may be submitted to the jury for consideration, the trial judge must determine whether the proponent has offered a satisfactory foundation from which the jury could reasonably find the evidence to be authentic. *See* FED. R. EVID. 104(b). Because the question of authenticity is ultimately a fact for the jury to decide, even after a trial court's *in camera* finding of authenticity, the evidence showing authenticity must still be presented to the jury before a recording may be admitted. *See* United States v. Branch, 970 F.2d 1368, 1371 (4th Cir. 1992).

of Evidence and common law foundational requirements for sound recordings, video recordings, photographs, computer-based evidence, and scientific evidence, as well as provides an explanation.

A. Federal Rules of Evidence

Federal Rule of Evidence 901 requires authentication of writings and recordings.[33] Rule 901 lists several ways in which writings and recordings may be authenticated.[34] Rule 901(b) specifies ten different methods of authentication, including testimony of a witness with knowledge, non-expert handwriting identification, and comparison by an expert.[35]

---

33. FED. R. EVID. 901.

34. *Id.*

35. Methods advocated by the Rule 901(b) include: (1) testimony of witness with knowledge; (2) non-expert opinion on handwriting; (3) comparison by trier or expert witness; (4) distinctive characteristics and the like; (5) voice identification; (6) telephone conversations; (7) public records or reports; (8) ancient documents or data; (9) process or system; and (10) methods provided by statute or rule. *See* FED. R. EVID. 901(b). While not every method listed herein would be appropriate to authenticate a photograph or digital image, commentators have advocated some of these methods. Some commentators assert that digital images should be treated like photographs; a witness may authenticate the image through testimony that the image is a "fair and accurate" portrayal of the scene at the time. *See* Paynter, *supra* note 25, at 68. Official commentary to Rule 901 suggests that courts should approach authentication requirements on a case-by-case basis and that they should require a more substantial foundation where circumstances create suspicion that evidence is altered, fabricated, or unreliable. Stephen A. Saltzburg, Daniel Capra, and Michael Martin, *Commentary to Rule 901*, FED R. EVID. 901 (2000).

There is little guidance as to what type of evidence requires explanation by expert witness testimony. Expert witness testimony is allowed under Rule 702 in order to explain evidence. However, Rule 702 deals solely with expert witness testimony necessary to explaining a piece of evidence. Rule 702 provides no guidance as to what types of real or demonstrative evidence would actually need expert witness testimony to explain the process used to create the evidence. Moreover, the use of the word "evidence" in Rule 702 may refer to real, demonstrative, and testimonial evidence. *See* BLACK'S LAW DICTIONARY 555-56 (6th ed. 1990). Nonetheless, before expert witness testimony can be admitted, it must first be shown to be "reliable." *See* FED. R. EVID. 702. "Reliability" usually depends on the reliability of the underlying scientific principle; the reliability of the technique or process that applies to the principle; the condition of the instrument used in the process; adherence to proper procedures; the qualifications of the person who performs the test; and the qualifications of the person who interprets the results. Michael H. Graham, *The Expert Witness Predicament: Determining "Reliable" Under the Gatekeeping Test of Daubert, Kumho, and Proposed Amended Rule 702 of the Federal Rules of Evidence*, 54 U. MIAMI L. REV. 317, 336-37 (2000).

Expert witness testimony may be considered reliable under either the *Frye* or the *Daubert* test. Since the 1923 case *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923), a scientific process or technique was deemed reliable and scientific evidence and testimony was therefore

In addition to the methods of authentication listed in Rule 901(b), the common law sets forth various authentication procedures. By examining common law authentication tests for types of evidence similar in nature to digital images, focusing on trends in the courts and the explanations for those trends, we might better judge the nature of the authentication requirements to which digital images may be subjected.

B. Sound Recordings

In the earliest cases that admitted sound recordings, the courts established the strictest authentication requirement ever applied to a recording or photograph-like piece of evidence. In *United States v. McKeever*, the defendants attempted to use a tape recording of an alleged conversation between a witness and the defendant to impeach

---

admissible if it passed "general acceptance" test. The *Frye* court held that if experts in the field generally accept a scientific principle or technique, the evidence is considered reliable and is admissible. *Id*. at 1014. The court explained:

> Just when a scientific principle or discovery crosses the line between the experimental and demonstrable stages is difficult to define. Somewhere in this twilight zone the evidential force of the principle must be recognized, and while courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs.

Id.

In the 1993 decision *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), the U.S. Supreme Court held that the Federal Rules of Evidence superceded the *Frye* test. *Id*. at 595-96. The Court explained that nothing in the Federal Rules of Evidence establishes "general acceptance" as an absolute prerequisite to admissibility of scientific testimony or evidence. *Id*. at 589. The Court reaffirmed that under the Federal Rules of Evidence a trial judge must ensure that admitted scientific evidence or testimony must be both relevant and reliable. *Id*. at 594. The Court then recognized that "general admissibility" is not the sole admissibility factor for scientific evidence; trial courts should also look to peer review and publication, the known or potential rate of error of the process or technique, and whether the process or technique has been tested. *Id*. The Court stressed the importance of "testing [scientific techniques] to see if they can be falsified" and mentioned that "the criterion of the scientific status of a theory is its falsifiability . . . ." *Id*. (quoting K. POPPER, CONJECTURES AND REFUTATIONS: THE GROWTH OF SCIENTIFIC KNOWLEDGE 37 (5th ed. 1989)).

The factors the Court set forth in *Daubert* are meant to be helpful, but not definitive. The primary focus of the test is the scientific validity of the principles that underlie the proposed evidence. *See* Kumho Tire Co. v. Carmichael, 526 U.S. 137, 151 (1999).

the witness' testimony.[36] The court held that, prior to admission of the tape recording, the proponents of the recording must establish a foundation of admissibility during an *in camera* hearing. At this hearing, the proponent must show the competency of the recording device; the competency of the operator; the authenticity and correctness of the recording; that no changes, additions or deletions have been made; that the recording has been preserved; that the speakers are identified; and that the conversation was made voluntarily. [37] The test, which addresses accuracy, authenticity, chain of custody, relevance, and competency, is known as the "seven-part" or *McKeever* test.[38]

---

36. 169 F. Supp. 426, 426 (S.D.N.Y., 1958), *rev'd on other grounds*, 271 F.2d 669 (2d Cir. 1959).

37. The court articulated that the proponent must show:

> (1) That the recording device was capable of taking the conversation . . . offered into evidence.
>
> (2) That the operator of the device was competent to operate the device.
>
> (3) That the recording is authentic and correct.
>
> (4) That changes, additions or deletions have not been made to the recording.
>
> (5) That the recording has been preserved in a manner that is shown to the court.
>
> (6) That the speakers are identified.
>
> (7) That the conversation elicited was made voluntarily and in good faith, without any kind of inducement.

169 F. Supp. at 430.

At first glance, it may seem strange that in order to authenticate a recording, a proponent must show it to be authentic. Indeed, Webster's Third New International dictionary defines "authenticate" as "to make authentic." Webster's Third New International Dictionary 146 (1993). The apparent redundancy in terms can be explained by an alternate definition of "authentication." Black's Law Dictionary defines "authentication" as "the act of proving that something (as a document) is true or genuine . . . so that it may be admitted into evidence." BLACK'S LAW DICTIONARY 127 (7th ed. 1999). By such a definition, it makes sense that a writing should be shown to be authentic, or credible, before it may be authenticated, or accepted into evidence.

38. The court noted:

> Current advances in the technology of electronics and sound recordings make inevitable their increased use to obtain and preserve evidence possessing genuine probative value. Courts should deal with this class of evidence in a manner that will make available to litigants the benefits of this scientific development. Safeguards against fraud or other abuse are provided by judicial insistence that a proper foundation for such proof be laid.

169 F. Supp. at 431.

In 1992 the Fourth Circuit adopted a flexible variation of the *McKeever* test in *United States v. Branch*.[39] During an *in camera* hearing before trial, the Government had presented evidence authenticating recordings of Branch's conversations, after which the court concluded that the Government presented sufficient authenticating evidence but would still have to lay a proper foundation for the tapes during trial.[40] Branch argued that the Government had failed to present sufficient evidence at trial to support a finding that the recordings were authentic.[41] The court held that the proponent of a tape recording need not satisfy each of the *McKeever* factors in order for a jury to reasonably conclude that the recordings were authentic and properly admitted into evidence.[42] The court reasoned that while the *McKeever* factors would generally provide a sufficient foundation, the factors should only provide guidance for the district court in its determination of whether evidence was sufficient to support a finding by the jury of the recording's authenticity.[43] The court further explained that the district courts have wide latitude in determining whether a party has provided a proper foundation from which a jury could find the recording authentic and that the abuse of discretion standard governs review of the district court's decision.[44]

Just as the *Branch* court emphasized that the seven-part test should function as a guide rather than a rule, many courts have adopted more relaxed tests. The court in *United States v. Biggins* used a four-part authentication test.[45] The *Biggins* court required: proof as to the competency of the operator; the fidelity of the recording equipment; the absence of material deletions, additions, or

---

The comment is as germane today as it was over forty years ago. For further commentary on the *McKeever* authentication test, see JORDAN S. GRUBER, ELECTRONIC EVIDENCE 264 (1995).

39. 970 F. 2d 1368 (4th Cir. 1992). The Eighth Circuit also adopted the *McKeever* seven-part test, but in the context of electronic monitoring. United States v. McMillan, 508 F.2d 101, 104 (8th Cir. 1974), *cert. denied*, 421 U.S. 916 (1975).

40. United States v. Branch, 970 F.2d at 1369-70.

41. *Id*. at 1370.

42. *Id*. at 1371-2. *See supra* note 37 and accompanying text.

43. 970 F.2d at 1372.

44. *Id*.

45. 551 F.2d 64 (5th Cir. 1977).

alterations in the relevant portions of the recordings; and the identification of the relevant speakers.[46] Like the *Branch* court, the *Biggins* court was quick to note that the four parts are merely guidelines and should not be interpreted as a rigid test.[47] The court emphasized that the foundational standards must ultimately ensure the accuracy of the recording.[48]

C. Video Recordings

Authentication tests during the early years of video recordings mirrored the strict scrutiny required during the authentication of early audio recordings.[49] Over time, however, the courts replaced the strict foundational requirements concerning the process of taking motion pictures with the admission of witness testimony that the film was a fair and accurate representation of what actually happened.[50] With the advent of sound in moving pictures, courts applied the seven-part test for sound recordings, originally used in *McKeever,* to motion pictures.[51]

As time passed, the courts relaxed the requirements for admissibility of video evidence. In almost every jurisdiction, authentication of video evidence now requires a foundation that accounts for the following four factors: relevance, fairness and

---

46. *Id*. at 66. The *Branch* court also noted that, in a criminal trial, it is particularly important for the government to lay a proper foundation for the recording because a defendant will often hear the recording for the first time in court. *Id*. Because sound recordings are more susceptible to undetectable alterations than traditional photographs or other demonstrative evidence, the court found it imperative that the defendant be alerted to any possible uncertainties or distortions in the recording before it is introduced as evidence against him. *Id*.

47. *See supra* notes 43-44 and accompanying text.

48. *See* 551 F.2d at 66-67.

49. Judges often sustained objections to motion pictures, excluding them because of motion pictures' reputation as easy to fabricate, falsify, and distort. *See* Gruber, *supra* note 38, at 373. By the 1930's, courts held that it would be an abuse of discretion to exclude relevant video evidence that was otherwise properly identified and authenticated. *See id*. For more on the authentication requirements used in the early days of audio recordings, see *supra* notes 36-48 and accompanying text.

50. Gruber, *supra* note 38, at 374. As the "silent witness theory" gained popularity, an authenticating witness no longer had to see what actually happened, but merely was required to verify the accuracy of the recording. *See id*.

51. *Id*. at 374-75. For a detailed account of the seven-part foundation test, see *supra* note 37 and accompanying text.

accuracy, the exercise of discretion with respect to whether probative value outweighs prejudice or possible confusion, and issues of competence.[52] As long as recordings meet these four requirements, there is generally no need to adhere to the strict seven-part test.[53]

D. Traditional Photographs

Traditional photographs have even more relaxed foundational requirements than video evidence. Like video evidence, often all that is necessary to authenticate a photograph is witness testimony that the photo is a fair and accurate portrayal of the scene.[54] The Federal Rules of Evidence require a showing that there is no more than a remote chance that either the photograph is distorted or that the scene portrayed is materially different from the scene that is relevant to the trial.[55] Unless there is evidence of tampering, the court typically requires only witness testimony establishing that the photograph is a true and accurate representation.[56]

In some instances, a photograph may even be admissible without witness testimony that the photograph is a fair and accurate representation of the scene. Under the "silent witness" theory, a court may consider photographs offered for their independent probative

---

52. Gruber, *supra* note 38, at 387 (quoting Gregory P. Joseph, *Videotape Evidence in the Courts—1985*, 26 S. TEX. L. REV. 453, 453 (1985)). The four factors will hereinafter be referred to as the "video four-factors test."

53. *Id*. In fact, strict foundational requirements for video recordings "are now almost universally rejected as unnecessary." *Id*. at 408 (quoting 3 CHARLES C. SCOTT, PHOTOGRAPHIC EVIDENCE, § 1297 (2d ed. 1991)). This departure from the strict foundational requirements for video evidence is a product of "the judicial system's growing familiarity with video evidence, and the widespread social, cultural, and technological acceptance of the medium." *Id*. at 386. Four common ways in which video evidence is currently authenticated include: (1) testimony by photographic expert who determined that the video was not altered in any way; (2) testimony concerning the chain of custody of the recording; (3) testimony regarding the checking and use of the camera and adequate proof of the validity of the video recording process; (4) testimony that the video evidence introduced at trial was the same as what the witness viewed immediately after recording. State v. Luster, 295 S.E.2d 421 (N.C. 1982).

54. 29A AM. JUR. 2D, *Evidence* § 965 (2001).

55. *Id*. at § 945.

56. Courts often defer to witness testimony because photography is considered a tried-and-true, time-tested image capture tool. *See* Kodak, *Film or Digital? About Film* (on file with author); EPA, *Conducting Environmental Compliance Inspections: Inspector's K.I.S.S. Manual* 21 (7th ed. 1996). Hereinafter, this authentication method will be referred to as "fair and accurate portrayal" testimony.

value to be self-authenticating such that they do not require witness testimony as to their accuracy. [57] Prior to admission of a photograph under this theory, the court requires proof that the photograph has not been altered.[58]

E. Computer-generated Evidence

Clearly distinct from authentication requirements for photographic, audio, or video recording evidence but certainly germane to authentication of digital images is the common law approach to authenticating computer-generated evidence. Most early cases involving authentication of computer printouts imposed a substantial burden on the proponent of the evidence.[59] In 1968, the Mississippi Supreme Court set guidelines for admissibility of computer-generated business records requiring a showing that the computing equipment was standard; that the entries were made in the regular course of business; and that foundation testimony regarding the source of information, method, and time of preparation indicated the trustworthiness of the evidence.[60]

As computer usage became more common, courts began to employ more liberal authentication standards.[61] In *Hahneman University Hospital v. Dudnick*, the New Jersey Superior Court ruled that expert testimony regarding the reliability of computer programs or other technical aspects of a computer's operation is not necessary to find computer-generated records circumstantially reliable.[62]

Likewise, in *People v. Lugashi*, a California Court of Appeals held that testimony on acceptability, accuracy, maintenance and reliability of computer hardware and software, as well as testimony

---

57. 29A AM. JUR. 2D, *Evidence* § 967 (2001).

58. *See* Buck v. State, 453 N.E.2d 993, 996 (Ind. 1983).

59. Mark A. Johnson, Comment, *Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability?* 75 MARQ. L. REV. 439, 448 (1992). For example, in *Transport Indemnity Co. v. Seib*, 132 N.W.2d 871 (Neb. 1965), the Nebraska Supreme Court considered 141 pages of trial testimony in deciding whether the foundation for the evidence was properly laid. Johnson, Comment, *supra*, at 449.

60. Johnson, Comment, *supra* note 59, at 449 (quoting King v. *ex rel*. Murdock Acceptance Corp., 222 So.2d 393, 398 (Miss. 1969)).

61. *See* Johnson, Comment, *supra* note 59, at 450.

62. *See* Hahnemann Univ. Hosp. v. Dudnick, 678 A.2d 266, 269 (N.J. Super. Ct. App. Div. 1996).

from hardware and software designers, was not required to demonstrate the "trustworthiness" of computer-generated evidence in order to lay its foundation for admission.[63]

Finally, Illinois courts allow computer-generated business records to be admitted if: the computer equipment is standard; the input is entered in the regular course of business and reasonably close in time to happening of the event recorded; and foundation testimony establishes that sources of the information, as well as the method and time of its preparation, show that the information is trustworthy and justify its admission.[64]

IV. THE CURRENT EVIDENTIARY SYSTEM IS NOT EQUIPPED TO AUTHENTICATE DIGITAL IMAGES

Despite the fact that digital images are different than traditional photographs, courts often use the same methods to authenticate digital images that they use to authenticate traditional photographs.[65] Most law enforcement agencies that use digital image technology have developed procedures to authenticate digital images under the current evidentiary requirements for authentication of photographs.[66] In addition, many members of the law enforcement community have suggested that digital images have not and should not be subject to stricter requirements than traditional photographs.[67]

---

63. 252 Cal. Rptr. 434, 441 (Cal. App. 2 Dist. 1988).

64. *See* People v. Houston, 679 N.E.2d 1244, 1249 (Ill. App. 4 Dist., 1997); *see also*, People v. Morrow, 628 N.E.2d 550 (Ill. App. 1 Dist. 1993); People v. Hendricks, 495 N.E.2d 85 (Ill. App. 4 Dist. 1986).

65. Traditional photographs are usually authenticated by "fair and accurate portrayal" testimony. *See supra* Part III.D. The "fair and accurate portrayal" testimony is insufficient to counter the possibility of a subtle, yet significant change. For more on the possibility of subtle manipulation of digital images, see HOUSE OF LORDS SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY–FIFTH REPORT, *supra* note 22. Moreover, lawyers and judges need to be aware of the possibility of tampering with traditional photographs and may consider adopting more strict foundational requirements for all photograph-like evidence.

66. For more information regarding the law enforcement community's use of digital images, see Law Enforcement Technology Website, *at* http://www.letonline.com (last visited Nov. 11, 2002).

67. One commentator asserts, "The truth is digital imaging will hold up in court, without meeting higher standards than print photography." Paynter, *supra* note 25, at 68. Another insists that "[a]s long as you can go into court and say you haven't altered an image, it will stand up. It's the integrity of the person who presents the image that's at issue." LAW ENFORCEMENT

A. Federal Rules of Evidence

Federal Rule 901(b) does not provide significant guidance for authentication of digital images.[68] First, testimony of a witness with knowledge, often used to authenticate photographs via the "fair and accurate portrayal" testimony, is insufficient for authentication of digital images.[69] For example, the compression process may distort the image so that a bystander might think that the image was a fair portrayal, but the scene might be slightly exaggerated.[70] Witness testimony limited to fair and accurate portrayal testimony omits important information regarding the digital camera settings, including the compression ratio, storage medium, and opportunity for manipulation.[71] Second, the other authentication methods suggested in Rule 901(b), such as non-expert handwriting identification, voice identification, and expert comparison, are inappropriate for digital imaging.[72] Third, the "silent witness theory," permitted under the Federal Rules of Evidence, is unacceptable for digital images.[73]

TECH., Oct. 1998, at 94, 95 (quoting Lt. Gene Miller, of the Montgomery (Alabama) Police Department).

68. *See supra* note 35 and accompanying text.

69. *See supra* notes 54-56, 65 and accompanying text.

70. *See supra* notes 11-16 and accompanying text.

71. *See supra* Part II.

72. Handwriting identification and voice identification are clearly not applicable to digital imaging. Although expert witness comparison may seem appropriate, because digital cameras do not produce an "original" image, an expert witness would not be able to compare the image offered to the original image to determine whether or not the image had been manipulated.

If counsel believes that expert testimony is not required to explain the process or technique, however, the underlying process or technique is not subject to reliability scrutiny. Moreover, the current rules regarding expert testimony only inquire whether the underlying technique is reliable, not whether the particular use of the process or technique produced a reliable result. *See* FED. R. EVID. 702. Thus, in the case of a digital image, the images can "slip through the cracks" of expert witness testimony. Because of the general public's familiarity with digital cameras (through commercials, etc.), and because the end product "looks" like a photograph, which is generally considered reliable, digital images may not need expert witness testimony, and may not require a showing that the underlying process is reliable. Because digital images are so easily manipulated and image quality and accuracy varies depending on the use of the camera, however, digital images should not be admissible as mere photographs.

73. The nature of digital images makes them too susceptible to manipulation for them to be considered "reliable" without further proof that the image and the process are genuine. Moreover, because of the potential for fabrication of traditional photographs due to advances in digital technology, traditional photographs should themselves no longer be admissible under the "silent witness" theory.

The Federal Rules of Evidence also hint that the courts should treat digital images differently than photographs, but they do not explain how to do so.[74] The Best Evidence Rule, Federal Rules of Evidence 1001, requires that in order to prove the content of a writing, recording, or photograph in a trial, the proponent must offer the original writing or adequately explain its absence.[75] The rule, formulated to increase the probative value and reliability of the evidence, distinguishes "photographs" from other "writings and recordings" and defines them as "still photographs, X-ray films, video tapes, and motion pictures."[76] The Commentary to Rule 1001(1) acknowledges possible expansion of the Best Evidence Rule to include "computers, photographic systems, and other modern developments." Importantly, the Commentary categorizes "photographic systems" under "writings and recordings," not under "Photographs."[77] The exclusion of digital imaging—explicitly labeled a "photographic system" in the Commentary—from the category of "Photograph" indicates that the Advisory Committee may have recognized the difference between traditional photographs and digital "photographic systems."[78]

The Advisory Committee has not, as of this writing, taken the opportunity to comment on exactly how digital images should be treated differently under the Best Evidence Rule. Given that the Federal Rules of Evidence are constantly being amended and that digital imaging has been gaining popularity for a number of years, it is clear that the crafters of the Federal Rules of Evidence have chosen not to deal explicitly with digital imaging.[79]

---

74. *See* FED. R. EVID. 1001.
75. *Id*.
76. FED. R. EVID. 1001(2).
77. *See* Advisory Committee's Note, FED. R. EVID. 1001(1).
78. Digital imaging falls into the category of a "photographic system" because it produces photograph-like images and has, in many disciplines, begun to replace traditional photography.
79. Amendments to the Federal Rules of Evidence went into effect in December 2000. *See, e.g.,* FED R. EVID. 702.

B. Common Law Authentication Tests

The several common law authentication tests available, such as the *McKeever*, *Biggins*, and the video four-factor authentication tests, are tailored to the specific technology they authenticate.[80] While each of the tests is grounded on basic principles of authentication in order to ensure the reliability of the evidence, none of the tests in its current form responds to the nuances of digital photography that distinguish it from traditional photography.[81] An authentication test similar to the aforementioned tests but tailored to digital imaging, however, would respond to evidentiary concerns raised by digital imaging.[82]

C. The Failure of the Current System

The failure of the current authentication system, or lack thereof, is evident in the lack of challenges to the admissibility of digital images. Digital images are rarely challenged in court.[83] The infrequency of challenges to digital images begs the question of why this type of evidence is not more frequently challenged in court.[84] One possible explanation for the paucity of challenges is the legal

80. *See supra* Parts III.B, C, and E.

81. *See supra* Part II.

82. *See infra* Part V.

83. A recent study of police departments in two Indiana counties used digital cameras to document domestic violence. *See* Herb Blitzer et al., *A Picture Says it All: A Study Finds Digital Imaging Effective in the Fight Against Domestic Abuse*, LAW ENFORCEMENT TECH., at 52 (June 2000), *available at* http://www.ifi-indy.org/articles/287_2000jun_0003672.pdf (last visited Nov. 11, 2002). Of the more than 400 cases covered in the study, only a dozen defense lawyers raised objections to the photos. Blitzer, *Digital Imaging*, *supra* note 1, at 16. Even capital defense lawyers are not challenging the digital images produced by local police departments. Lt. Gene Miller, of the Montgomery, Alabama Police Department, reports that his department has "used the [digital] camera in capital murder cases, and so far no one has challenged the photos in court." Richard D. Morrison, *Digital-Point-and-Shoot Camera System*, LAW ENFORCEMENT TECH., at 88, 89 (June 1999).

84. There are several explanations for why digital images are not being challenged in court. First, lawyers and judges may not be familiar enough with the risks posed by digital images to challenge the images. Second, lawyers and judges may be familiar with the recreational use of digital cameras and therefore may not consider it a "new technology" that should be subject to increased scrutiny. Third, groups that routinely use digital imaging in litigation, such as law enforcement agencies, are more technologically sophisticated than the legal profession and have prevented opposition through the use of training and development of SOPs. Fourth, evidentiary rules have not caught up with the technology. The Federal Rules of Evidence do not adequately address concerns raised by digital imaging.

community's general lack of awareness of the characteristics of digital images that should make them less reliable as evidence than traditional photographs.[85] The general lack of awareness of differences between digital images and traditional photographs explains the few challenges and therefore the scarcity of case law on the subject, which in turn perpetuates the lack of awareness that digital images present unique evidentiary issues. Moreover, the few cases dealing with digital images as evidence actually deal with digital enhancement of a digital image, not the digital image itself.[86]

The acceptance of digital imaging by forensics and law enforcement communities may discourage lawyers and judges from challenging the use of digital images without considering the fact that the current evidentiary rules were not designed to deal with digital images. [87] Moreover, there is a trend in the legal community towards

---

85. *See supra* Part II.

86. In *State v. Hayden,* 950 P.2d 1024 (Wa. Ct. App. 1998), digital enhancement of a digital image survived a *Frye* hearing in Washington state court. Although the court found that neither digital photography nor the use of computer software to enhance images is a novel process, it nonetheless analyzed the admissibility of the forensic use of enhanced digital imaging under the *Frye* test. *Id*. at 1027. The evidence in question, an enhanced digital photograph of a bloody handprint left on a bed sheet, was created by using filters on the digital image to remove background detail so that a latent fingerprint could be taken from the fabric. *Id*. at 1028. Finding that there was not a significant dispute among qualified experts as to the validity of such enhanced digital imaging, the court concluded that the process passed the *Frye* general acceptance test and was therefore admissible. *Id*. The court's finding is not necessarily convincing proof that digital imaging will always be acceptable under *Frye*; the proponent of the evidence offered two expert witnesses and five articles from forensic journals to prove that the process was generally accepted in the relevant scientific community, while the opponent provided no evidence to the contrary. *Id*. at 1027. Moreover, the actual bed sheet that was photographed and digitally enhanced was available to the court for examination, thereby allowing the court to verify that nothing had been added to the image that was not present on the sheet. *Id*. The court also supported its holding with findings that the specific enhancement technique used had a reliability factor of one hundred percent and a zero percent margin of error, the results were visually verifiable, and the results could be duplicated easily by another expert using her own digital camera and software. *Id*. at 1028.

87. Digital imaging has been subject to peer review and publication and has been deemed generally accepted technology. The court in *State v. Hayden* found that digital photography and manipulation of digital images using computer software were generally accepted in the relevant scientific community. *Id*. at 1027. Law enforcement agencies are increasingly using digital imaging during crime scene investigations. According to George Reis, a forensic digital photography expert employed by the Newport Beach Police Department, over 2,000 law enforcement agencies are currently using digital cameras during crime scene investigation. Telephone interview with George Reis, Forensic Digital Photography Expert, Newport Beach Police Department (July 14, 2000) (on file with author). Moreover, consumer use of digital

electronic-based litigation.[88] This trend may discourage lawyers and judges from objecting to electronic images for fear that to do so would be counter-productive to the movement towards convenience promised by increased computer use in litigation.

V. PROPOSAL FOR DIGITAL IMAGE AUTHENTICATION

A. Digital Image Authentication

Changes should be made to the current evidentiary system so that it is more responsive to concerns raised by digital images. The new comprehensive system should address camera capability, operator competency, compression ratios, preservation of an "original" image, safeguards against changes, additions, and deletions, and identification of the subject matter.

---

cameras has skyrocketed in the past five years. Reasons for this increase include the decreased cost of digital cameras, the increased prevalence of computer systems necessary to process the digital images, the ability to enhance, manipulate or re-size images without professional training, and the low processing cost. The strong acceptance of digital imaging technology by scientists, law enforcement officers, and consumers, combined with the legal profession's acknowledgment of the technology, is likely to convince a trial judge to allow digital images as evidence. The increased use of digital images by consumers increases the probability that jurors will be aware of how the technology works and how it can be manipulated. Jurors who do not own digital cameras will nonetheless be familiar with the potential manipulation of digital images. In 1997, the International Association for Identification officially endorsed the use of digital imaging technology, calling it "a natural progression in the history of photography." Paynter, *supra* note 25, at 68 (internal quotations omitted). Moreover, not only has the technology been subject to peer review, but the actual use of digital images in court has also been subject to peer review and publication. *See* Blitzer, *Digital Imaging*, *supra* note 1, at 16; Paynter, *supra* note 25, at 68; Morrison, *supra* note 87, at 88; Scientific Working Group on Imaging Technologies, *Definitions and Guidelines for the use of Imaging Technologies in the Criminal Justice System*, Version 2.1, Jun. 8, 1999, *at* http://www.fbi.gov/hq/lab/fsc/backissu/oct1999/swgit1.htm (last visited Nov. 11, 2000) [hereinafter SWGIT, *Definitions*]; Herb Blitzer and Richard Kammen, *Ensure Admissibility of Digital Images*, IND. LAW. *at* http://www.ifi-indy.org/articles/indlaw.html (last visited Nov. 11, 2002). On the other hand, the use of digital imaging is suspect in professional photography circles. While digital photography as a discipline has come into its own, the undocumented use of digital techniques to enhance traditional photography is problematic. The photography world was scandalized when it realized that an amazing photograph of a herd of zebras printed on the cover of National Geographic was actually a photograph that was digitally enhanced to make only a few zebras look like an entire herd.

88. Courtroom 21 and other technology-based initiatives have pushed for more computer-friendly courtrooms. *See* William & Mary Law School Website, *at* http://www.wm.edu (last visited Apr. 28, 2002).

By modifying factors taken from the *McKeever* seven-part test, the *Biggins* test, and the video four-factors test, the new standard should address concerns regarding digital images. [89]

Congress should adopt the following new Digital Image Authentication factors:

(1) The camera and storage medium can technologically support the image offered into evidence;

(2) The operator was competent to operate the camera;

(3) The digital image is a true representation of the scene;

(4) An "original" image has been preserved for the court;

(5) Changes, additions or deletions have not been made to the digital image; and

(6) The subject matter of the digital image has been identified.[90]

---

89. The *McKeever* factors, modified to apply to digital images, are:

(1) The digital camera was capable of taking the image offered into evidence;

(2) The operator of the device was competent to operate the device;

(3) That the digital image is authentic and correct;

(4) Changes, additions or deletions have not been made to the digital image;

(5) The digital image has been preserved in a manner that is shown to the court;

(6) The subject matter of the digital image was identified; and

(7) The digital image was taken voluntarily and in good faith, without any kind of inducement.

See supra note 37 and accompanying text.

As applied to digital imaging, the *Biggins* four-part test would require:

(1) Proof as to the competency of the operator;

(2) Accuracy of the digital image based on the camera's specifications;

(3) Absence of material deletions, additions, or alterations in the image; and

(4) Identification of the scene shown.

See supra notes 45-48 and accompanying text.

The video four-factors authentication test as applied to digital images is:

(1) Relevance of the image;

(2) Fairness and accuracy of the image;

(3) Rule 403 prejudice concerns; and

(4) Competence of the digital camera operator.

See supra note 52 and accompanying text.

90. The proposed authentication procedure should be used only for digital images as demonstrative evidence. Digital images may someday be self-authenticating, but only when

B. Meeting the Foundational Requirements

This section explores the importance of each factor and how users can ensure the admissibility of a digital image under these factors.

First, the proponent must show that the camera and storage medium could technologically support the image offered. A digital image print must be supported by an image file large enough to preserve image integrity.[91] By showing that the camera and storage medium were capable of capturing and storing an image of the file size necessary to create a print of the image like the one offered into evidence, the proponent can show that the image did not need to be augmented in order to produce the print offered into evidence.[92]

To show that the camera was capable of taking the image, the party seeking to admit the image into evidence would offer proof that the camera's resolution was sufficient to produce an image of the size displayed.[93] In addition, the proponent would offer evidence that the storage medium used was capable of holding the entire image file as shown to the court.[94]

Second, the proponent must show that the operator was competent to operate the digital camera. Because digital cameras can potentially produce low quality images depending on camera settings, such as compression ratios, proof that the operator understood basic

---

digital image protection technology is as affordable and available as digital image manipulation technology. Epson has developed in-camera software that encrypts the digital image as it is captured. Such manipulation-prevention technology will play an increasingly important role in the future.

Digital imaging as a process should not be subject to either the *Frye* or *Daubert* reliability test because none of the foundational factors in the proposed test requires expert witness testimony. *See supra* note 32. Keeping in mind the technology explosion and the increasingly widespread use of digital imaging in scientific, professional, and recreational settings, it is possible that digital imaging may be considered a familiar technology even in the absence of preliminary litigation that would introduce the technology to the court. On the other hand, if a digital image was manipulated by a specific process and the manipulated image was to be admitted into evidence, expert witness testimony be necessary to explain how and why the specialized manipulation technique was used.

91. Blitzer, *Forensic*, *supra* note 6. *See also supra* notes 13-14 and accompanying text.

92. On the contrary, if a five-inch by seven-inch digital image offered into evidence was purportedly captured by a camera that could not actually produce a useable image larger than two-inch by three-inch, the opponent of the evidence would apparently have strong proof that information had been added to the original image file in order to produce the larger image.

93. *See supra* Part II.A.

94. *See supra* Part II.A.

principles of digital imaging reduces the possibility that the image was inadvertently manipulated or created from scratch.[95] Witness testimony by the operator of the camera would be an easy way to demonstrate her competence in its use.

Third, the proponent must show that the digital image is a true representation of the scene. Proof that the digital image is a true representation of the scene captured is critical to evaluating whether the image will have sufficient probative value to outweigh possible prejudice.[96]

In order to prove a digital image is a true representation of the scene, the proponent should show that the image was stored using little or no compression.[97] The party offering the image would also present information regarding the trustworthiness of the colors of the image, despite the color interpolation process used by digital cameras.[98]

A fourth authentication requirement is that an "original" image be preserved for the court. The value of having an "original" image preserved is that the court could compare any subsequent image offered by either party to the original preserved image.[99] The

---

95. *See supra* Part II.A.

96. An additional requirement prior to admission of all evidence is that the probative value of the evidence is not substantially outweighed by its prejudicial effect. *See* Fed. R. Evid. 403. If a digital image is not a true representation of the scene, the sheer power of the incorrect image may be prejudicial and unintentionally sway the jury.

97. Blitzer, *SOP, supra* note 6, at 59. The compression process involves "loss" of a portion of the image's information. *See supra* Part II.A. When the image is later reconstructed, part of the information visible was not actually recorded, but has been "guessed" by the camera. *See id*. This makes images with a high compression ratio less accurate than those with a low compression ratio. *See id*. This Note does not propose a threshold compression ratio above which images would not be considered "correct." If courts adopt this authentication test, however, such a question would need to be resolved by digital imaging experts.

98. Because the digital image is initially recorded in one of 256 tones of gray scale, a combination of sensors, filters, and color interpolation is used to produce color images. Curtin, *supra* note 3. Several combinations of chips and filters may be used, but most combinations involve a process where the original color of each pixel is not calculated. *Id*. The computer within the camera must then "interpolate" as to what color the missing pixels should be by examining the surrounding pixels. *Id*. This process of color interpolation thus subjects the image to objections that it is not a "true" representation of the actual scene. *Id*.

99. Because it is possible to make exact copies of a digital image, it is likely that a government agency conducting an inspection of a facility would leave a copy of the images captured with the facility. Likewise, in a civil case, a digital image would need to be produced during discovery. If adverse parties have the same digital image, it is possible that each party would enhance the image to its own advantage.

"original" functions like a film negative and would allow the court to perform its own enhancements on the image, if necessary.[100]

An "original" image can be preserved for the court by copying the unopened image file directly from the original storage medium to an archiveable, unalterable storage medium.[101] Showing the chain of custody could then protect the "original".[102]

A crucial aspect of authentication of digital images is a showing that changes, additions, or deletions have not been made to the digital image. Digital images are highly susceptible to undetectable manipulation; evidence that the image has not been manipulated is crucial to a showing that the image is authentic and that its probative value outweighs possible prejudice.[103]

There are several ways in which a proponent may show that an image has not been altered. One possible method, useful for law enforcement agencies, but less useful in the civil arena, is the establishment of a complete chain of custody.[104] Chain of custody is

---

100. Given the trend towards computers in the courtroom, it is likely a court could, with its own software, perform an impartial assessment of the digital images in question. For more on the problem of not having an "original" image, see *supra* Part II.B.

101. *See generally*, Blitzer, *SOP*, *supra* note 6, at 58. One possible method would be to copy the image file to a Compact Disk-Recordable (CD-R) engraved with a serial number. *Id*. at 58-59. The serial number can be logged and once saved to a particular CD-R, the image file cannot be altered on that disk. *Id*.

102. Chain of custody may be more important to show that no changes, additions, or deletions have been made. *See infra* notes 107-11 and accompanying text.

103. *See supra* Part II.B.

104. Chain of custody can be an acceptable method to show lack of manipulation, if the chain of custody was complete, well documented, and part of a Standard Operating Procedure. *See* Blitzer, *Forensic*, *supra* note 6; Blitzer, *SOP*, *supra* note 6, at 58. Many law enforcement agencies across the country currently have detailed, written SOPs that mandate a strict, protected chain of custody that adds credibility to the process. *See generally* SWGIT, *Definitions*, *supra* note 87; Paynter, *supra* note 25, at 68. According to George Reis, a forensic digital photography expert employed by Newport Beach Police Department, over 2,000 law enforcement agencies are currently using digital cameras during crime scene investigation. Telephone interview with George Reis, Forensic Digital Photography Expert, Newport Beach Police Department (July 14, 2000) (on file with author). Law enforcement professionals consistently tout the acceptance of digital images in court. In his article *Digital Point-and-Shoot Camera System*, Richard D. Morrison professed that "Kodak digital technology is widely used and generally accepted in the field, laboratory, and courtroom." Morrison, *supra* note 83. Additionally, a study in which two counties in Indiana gave digital cameras to patrol officers showed that only a dozen defense lawyers made objections to the admissibility of digital images in over 400 cases. Blitzer, *Digital Imaging*, *supra* note 1, at 16. Chain of custody, however, is unlikely to be a reliable method of authentication in most civil suits, which tend to utilize photographs taken by individuals other than trained professionals following strict procedures.

an approach to showing the court that the original image has been preserved, ideally by accounting for the image from the moment it was captured until its presentation in court.[105] Digital imaging experts recommend that law enforcement and government agencies create Standard Operating Procedures (SOPs) which detail the appropriate steps in the chain of custody.[106] A typical SOP involves copying and archiving the image to several locations without opening it, logging the steps used while processing the image for printing, saving the processed image to a secure zip drive, and duplicating the contents of the zip drive to an incorruptible medium.[107] Parties without SOPs may be able to demonstrate a chain of custody, but it will most likely carry less weight than those parties that have a written SOP.[108]

A second method of showing that images are free from manipulation is through encryption of the digital image.[109] Digital fingerprinting and watermarking are viable forms of encryption.[110] The main drawback of digital watermarks is that they are

105. *See generally* Blitzer, *SOP*, *supra* note 6, at 58; Blitzer, *Digital Imaging*, *supra* note 1, at 16.

106. Experts note that "[a]n agency that is operating without SOPs is treading on dangerous ground." Richard Kammen, quoted in Blitzer, *Digital Imaging*, *supra* note 1, at 19.

107. *See* Blitzer, *SOP*, *supra* note 6, at 58. The most popularly used incorruptible medium is the write-once-read-many times (WORM) disks that have embedded serial numbers. *Id*. Once an image is recorded on a WORM disk and its index is preserved in another location, there is a uniquely identifiable and virtually incorruptible record of images. *Id*. If the images are archived soon after they are taken, it is unlikely that a party could alter the image to fit their theory of the case because the original images would be preserved. Blitzer, *Digital Imaging*, *supra* note 1, at 19.

108. A chain of custody without original, unopened copies of the image, process logs, and files saved to unalterable media does little to show the court that the image has not been altered. While it was possible in the past to doctor a photograph, electronic manipulation of digital image is faster, easier, and more accessible than methods of altering photographs. *See* Christine A. Guilshan, Note, *A Picture is Worth a Thousand Lies: Electronic Imaging and the Future of the Admissibility of Photographs into Evidence*, 18 RUTGERS COMPUTER & TECH. L.J. 365, 374 (1992).

109. Encryption enables the possessor of the image to "hide" the image so that it is meaningless to anyone viewing it without the appropriate equipment and decryption key. *See* HOUSE OF LORDS SELECT COMMITTEE ON SCIENCE AND TECHNOLOGY–FIFTH REPORT, *supra* note 22, at § 3.8.

110. A digital watermark is information hidden within a document or digital image by using a form of encryption. There are two types of watermarks currently in development: permanent and fragile. A permanent watermark is like a digital "tattoo" and is generally foreseen as being used to help owners protect copyrighted material. *Id*. On the other hand, any process of modifying or altering the image other than merely viewing it destroys a fragile watermark. *Id*.

meaningless unless the camera itself applies them when the image is captured.[111]

A third way to show that an image is free from manipulation is through use of Cyclical Redundancy Checksums (CRCs).[112] CRCs deter manipulation by providing a way to detect changes to the image.[113] While CRCs have been used to authenticate documents and are being used currently to authenticate images, CRCs are not foolproof.[114] Nevertheless, they do provide extra protection against manipulation and should be included whenever digital images are involved.

A final requirement for authentication of a digital image is identification of the subject matter captured in the image. Because visual evidence such as digital images can be a powerful persuasive tool, it is important to prove that the perpetrator "caught in the act" is actually who the proponent claims it is.

Parties may meet this requirement by inclusion of certain identifying "markers" within the image or by witness testimony that the picture was taken at a certain location on a certain date.[115]

VI. CONCLUSION

Digital imaging is a useful and attractive technology that is here to stay. The legal community should not condemn the use of digital cameras or digital images for fear of legal issues surrounding the

111. If a camera does not apply a watermark upon capture of the image, a user could capture an image, alter it, and then insert the watermark. Currently, there are no such cameras on the market.

112. CRCs are often referred to as "hashing algorithms" or "hash marks."

113. The CRC software calculates a unique number (the actual CRC) for the image by using a complicated algorithm based on the pixels in the image. Currently both 64-and 128-number algorithms are available. Since each pixel shade is given a number, it is likely that if the image were altered, the CRC would change as well. The larger the original algorithm, the less likely it is the algorithm would produce the same sequence of numbers if the evidence was manipulated. If a CRC is calculated and recorded immediately upon saving the image to CD-R, it is effective as a part of an audit trail to show that the image has not been altered. Also, the algorithm can be executed in court to show that the image presented is the original image.

114. Digital images contain significantly more bits and bytes of information than a normal document would. The question then remains as to how large an algorithm must to be to adequately ensure to a degree of certainty that no manipulation has taken place.

115. A witness may be able to testify that she took the picture while standing at a certain address and then offering proof that the business in question is located at the address.

technology. Instead, the legal community should recognize the evidentiary dangers posed by digital images and should recognize that current methods of authentication are insufficient to extinguish the concerns presented by digital images. The legal community should adopt new authentication standards tailored to compensate for the susceptibilities inherent in digital imaging technology.[116]

116. It is possible that the rampant opportunities available for falsification of every form of evidentiary media discussed here–audio, video, digital, and film–through use of digital technology may launch a trend toward more strict foundational requirements for all types of evidence, or at least those most vulnerable to falsification. While at some point strict foundational requirements for all forms of real or demonstrative evidence may be necessary, if new digital image authentication measures are adopted, juries should be able to believe what they see.