DIGITAL MANIPULATION AND PHOTOGRAPHIC EVIDENCE: DEFRAUDING THE COURTS ONE THOUSAND WORDS AT A TIME

Zachariah B. Parry[*]

I. INTRODUCTION

A picture is worth a thousand words. Photos do not lie. These clichés have been around since time immemorial, and, until recently, there has been little reason to question the veracity of a photograph's thousand words. Only lately have digital cameras and scanners capable of producing high-resolution digital images been available to more than large corporations and wealthy individuals. Now, for less than $100,[1] any consumer can purchase a digital camera capable of producing prints whose quality is indistinguishable from those derived from a 35mm negative.[2] Additionally, image-manipulation software is readily available: although some of the more sophisticated software, like Adobe Photoshop, comes at a moderate price;[3] other programs, like Google's Picasa, are capable of simple but effective enhancement

[*] J.D., University of Illinois, 2009; B.S., Psychology, Brigham Young University, 2006. I wish to extend my sincere and plenary thanks to a number of people who in some way or another contributed to this Note. First and foremost, I wish to thank my eternal companion and wife, Amber, whose keen eye caught errors and inconsistencies that were invisible to me. I also wish to show my gratitude to my family, including my parents, David and Rebecca, who taught me to speak; my siblings Eliza, Jessica, Jacob, Audrey, and Michael, who have always encouraged my love of Adobe Photoshop; my two perfect children, Cadence and Jack, who were exceedingly patient while their dad was clinking away at the computer for far too long; and my mother-in law, Rebecca, who kept my wife occupied while I was researching and writing. Thank you also to my very thorough editor, Katherine Croswell, and my good friends Jamshid Ghazi Askar, Daniel Lewis Orr III, Jeffrey Wallace Ellsworth, Christopher Russell Near, and William Kent Pyne. Much appreciation goes to my legal-writing professor, Professor Schulte, Judge Magistrate Robert Jake Johnston, and the exemplary partners at Woodbury, Morris & Brown, whose constructive input of my writing in general has proved invaluable. And thank you, Marilyn Kurz, who taught me I shouldn't send out anything I've written if it is not aesthetically pleasing.

1. RadioShack.com, GE A735 7.0MP Digital Camera (Red), http://www.radioshack.com/product/index.jsp?productId=3082700 (last visited Mar. 5, 2009) (selling a 7.0 megapixel camera for $79.99).

2. *See* Design215.com, Megapixels Chart, http://www.design215.com/toolbox/megapixels.php (last visited Feb. 6, 2009) (explaining the number of megapixels required to get true photo-quality prints from a digital camera).

3. *See* Adobe.com, Photoshop CS3 Editions, http://www.adobe.com/products/photoshop/ index.html (last visited Mar. 5, 2009) (selling the latest version of Adobe Photoshop for $699).

techniques and are available for download free of cost.[4] Despite the virtually universal availability of tools for the capture and manipulation of digital images, and the difficulty, sometimes impossibility, of detecting digital manipulations—there is no statute, rule, or case law that guarantees that false-positives (photos that have been authenticated but are not in fact what they purport to be)—will not be admitted as evidence in court.

Part II of this Note discusses the evolution of photography and what role photographs have played as evidence in court. Further, it will demonstrate how the standards for authentication are susceptible to doctored digital images. Part III details the evidentiary implications of the digital movement, and explores how rule-making bodies have reacted, as well as some of the common-law solutions implemented. Moreover, Part III evaluates the adequacy of these attempts to assure that authenticated photographs are in fact authentic. Part IV proposes an authentication scheme adapted to the new paradigm of digital photography that will provide courts with a reason to trust, instead of doubt, digital photographs.

II. BACKGROUND

Pictures persuade people powerfully.[5] Photos communicate more convincingly than do words alone by evoking an emotional and cognitive arousal that the same information, without the pictures, does not.[6] A picture is a more effective conveyor of information than its verbal and written counterparts alone[7] in that the communication of its message occurs in less time,[8] requires less mental effort on the part of the observer,[9] incites less counterargument,[10] and creates more confidence in the conclusions it proffers.[11]

People, including jurors, trust photographs.[12] So do courts.[13] Yet it has never been easier for photos to misrepresent the truth than it is now.[14] So great

4. Picasa.Google.com, Picasa 3: Free Download from Google, http://picasa.google.com/ (last visited Mar. 5, 2009).

5. *See* Richard K. Sherwin et al., *Law in the Digital Age: How Visual Communication Technologies Are Transforming the Practice, Theory, and Teaching of Law*, 12 B.U. J. SCI. & TECH. L. 227, 241–42 (2006) (discussing the cognitive affect of visual expressions).

6. *Id.*

7. *Id.*

8. *Id.* at 243.

9. *Id.*

10. *Id.* at 244.

11. *Id.*

12. Dean M. Harts, *Reel to Real: Should You Believe What You See?*, 66 DEF. COUNS. J. 514, 517 (1999); George Paul, *Fabrication of Evidence: A Click Away*, NAT'L L.J., Feb. 21, 2000, at B10 [hereinafter Paul, *Fabrication of Evidence*]; Art Golab, *Picture Perfect? Don't Be So Sure*, CHICAGO SUN-TIMES, Mar. 3, 1996, at 32.

13. *See* MCCORMICK ON EVIDENCE 214 (5th ed., 2003 Pocket Part) (explaining that the Federal Rules do not currently set forth admissibility requirements for digital photographs); George L. Paul, *The "Authenticity Crisis" in Real Evidence*, PRAC. LITIGATOR, Nov. 2006, at 46, 48 [hereinafter Paul, *The "Authenticity Crisis"*], *available at* http://www.lrlaw.com//files/uploads/documents/Paul_TheAuthenticityCrisisInReal Evidence_Practicallitigator_2004.pdf (noting that the current rules seem to assume that *ex post facto* examinations will detect manipulation of photographs).

14. Emily Nelson, *Claims of PhotoFakery Get Lots of Exposure in Court*, WALL ST. J., Feb. 7, 1997, at

is the risk of a photograph misrepresenting the truth that an international leader in digital imaging was compelled to declare, "photographs, as evidence of reality, are dead."[15] If photographs are so untrustworthy, why are they still considered the ultimate proof? Why are aphorisms like "photos don't lie" and "I'll believe it when I see it" so pervasive? The answer has to do with how technology has affected a paradigm shift in the methods used to take pictures. To comprehend how the fidelity of the photograph has been forfeited, it is first necessary to understand the previous picture paradigm and juxtapose it with the modern domain of digital images.

A. Traditional, Analog Photography

Traditional photography is an analog science.[16] Light enters through a camera's lens and the image the camera "views" is faithfully recorded onto a negative.[17] This negative is then printed into a recognizable image.[18] Although the images represented in the photograph have typically been faithful to the image "seen" by the camera, photographic trickery and distortion have long existed.[19]

Several variables affect how a photo turns out, all of which can either subtly or drastically change the story a photo tells.[20] A low-angle shot,[21] for instance, can make a human subject seem much taller than she is in reality.[22] "[S]potting, cropping, color balancing, brightness and contrast adjustment, burning, and dodging,"[23] and adjusting exposure time[24] are also very common

---

B2.

15. Paul, *The "Authenticity Crisis," supra* note 13, at 49 (quoting Jean Borda, the European coordinator for the Digital Imaging Group, a seventy-member international consortium of imaging companies). In fact, in at least one newspaper, almost all of the published pictures have been altered in some way. Stewart Wavell, *Exposed: The Cameras' White Lies*, SUNDAY TIMES (LONDON), June 27, 1999, at 14 ("One broadsheet picture editor admitted that up to 90% of photographs are now digitally enhanced or manipulated.").

16. Paul, *The "Authenticity Crisis," supra* note 13, at 46. The definition of "analog" is: "of a device that represents numerical quantities in terms of physical variables, e.g., in terms of voltages where resistance represents mechanical loss, or space in a slide rule, or rotation in a gear system." THE NEW LEXICON WEBSTER'S DICTIONARY OF THE ENGLISH LANGUAGE 32 (Encyclopedic ed. 1987). This is the complement of "digital," which is: "of an instrument that accepts data and produces output in the form of characters or digits." *Id.* at 266.

17. Victor E. Bianchini & Harvey Bass, *A Paradigm for the Authentication of Photographic Evidence in the Digital Age*, 20 T. JEFFERSON L. REV. 303, 306–07 (1998). The details of the process are considerably complicated and beyond the scope of this Note.

18. *Id.* at 307–08.

19. James Keane, *Prestidigitalization: Magic, Evidence and Ethics in Forensic Digital Photography*, 25 OHIO N.U. L. REV. 585, 585 (1999); Bianchini & Bass, *supra* note 17, at 308; Golab, *supra* note 12, at 32.

20. *See* David Beckman & David Hirsch, *Developing Evidence: Imaging Software Can Help your Pictures Tell the Story*, A.B.A. J., Aug. 2003, at 62, 62 ("Lighting, position of the camera relative to the subject, type of film, lens and any number of camera settings are just some of the variables that can affect the truth shown by any photograph.").

21. Wavell, *supra* note 15, at 14.

22. *See, e.g.*, Angelfire.com, The Power of the Camera, http://www.angelfire.com/ms/MediaLiteracy/Camera.html (last visited Mar. 5, 2009) (explaining that a basketball player can be made to seem much taller if a picture is taken from below).

23. Catherine Guthrie & Brittan Mitchell, *The* Swinton *Six: The Impact of* State v. Swinton *on the Authentication of Digital Images*, 36 STETSON L. REV. 661, 664 (2007). Spotting is "retouching a processed print with a pencil or brush (with watercolors or dyes) to eliminate spots left by dust or scratches on the negative." Kodak.com, A Glossary of Photographic Terms: Q-S, http://www.kodak.com/global/en/

ways to manipulate the story told by a photograph.[25]

For decades, books, newspapers, and magazines have used photographs to tell fantastic and impossible stories, from self-propelled, flying men to "proof" of the existence of jackelopes.[26] And yet, analog photographs maintain their integrity[27] because alterations and manipulations to an analog print have always been very easy to detect.[28] In fact, by looking for four different types of clues—density,[29] shadows,[30] splice lines,[31] and image continuity[32]—it becomes simple to finger a fraudulent analog photograph.[33] Moreover, making alterations to analog photographs is a complicated and costly ordeal.[34]

When the Federal Rules of Evidence were enacted in 1975, the fidelity of photographs was presumed,[35] which did not present a problem because the ease with which modifications and manipulations could be identified made it a very manageable matter for courts to protect themselves from fraudulent photographs.[36] Since then, however, digital technology has permeated society, making it more costly for courts to be cavalier about what images are

---

consumer/glossary/termsQ_S.shtml#S (last visited on Feb. 8, 2009). Cropping is "printing only part of the image that is in the negative or slide, usually for a more pleasing composition." Kodak.com, A Glossary of Photographic Terms: C, http://www.kodak.com/global/en/consumer/glossary/ termsC.shtml (last visited on Mar. 5, 2009). Color balancing is "how a color film reproduces the colors of a scene. Color films are made to be exposed by light of a certain color quality such as daylight or tungsten." *Id.* Burning is "[g]iving additional exposure to part of the image projected on an enlarger easel to make that area of the print darker." Kodak.com, A Glossary of Photographic Terms: B, http://www.kodak.com/global/en/consumer/ glossary/termsB.shtml (last visited on Feb. 8, 2009). Dodging is the "[h]olding back of image-forming light from a part of the image projected on an enlarger easel during part of the basic exposure time to make that area of the print lighter." Kodak.com, A Glossary of Photographic Terms: D, http://www.kodak.com/ global/en/consumer/glossary/ termsD.shtml (last visited on Feb. 8, 2009).

24. Bianchini & Bass, *supra* note 17, at 308.

25. *Id.*

26. *See* Wesley M. Baden, *Digital Photographs as Evidence in Utah Courts*, UTAH BAR J. Mar. 2004 at 28, 30 ("[a]ll kinds of manipulation—some artistic, others deliberately devious in nature—are possible in analog photography. Anyone who has spent time in the darkroom knows that picture sharpness, contrast, and even mood may be varied dramatically by simple changes in the type of developer, development time, and paper stock used. Undesirable objects may be removed by cropping. The physical appearance of individuals may be changed using techniques such as burning in and dodging. That is, hair may be darkened or lightened, a beauty mark highlighted, a mole removed, teeth whitened. Double exposure or cutting and splicing of negatives may be used to create prints of supposedly real objects like ghosts and flying saucers."); CNET.com.au, *Photos: Pictures that Lie*, Feb. 6, 2006, http://www.cnet.com.au/software/imaging/ print.htm?TYPE=story&AT=240060104-239035345t-230000052c [hereinafter CNET] (providing examples of digital manipulation).

27. Paul, *The "Authenticity Crisis," supra* note 13, at 46–47.

28. *Id.* at 46; Paul, *Fabrication of Evidence*, *supra* note 12, at B10.

29. The emulsion density based on the original exposures will differ among photos. Bianchini & Bass, *supra* note 17, at 310.

30. Different light sources in the components of a fusion of photographs will produce misaligned or missing shadows. *Id.*

31. Telltale signs of where an image has been cut are often left behind. *Id.*

32. This is a more holistic approach involving a subjective ascertainment of whether the image "looks" right. *Id.*

33. *Id.* at 309–10.

34. Paul, *The "Authenticity Crisis," supra* note 13, at 46; Paul, *Fabrication of Evidence*, *supra* note 12, at B10.

35. Paul, *The "Authenticity Crisis," supra* note 13, at 46; Paul, *Fabrication of Evidence*, *supra* note 12, at B10.

36. Bianchini & Bass, *supra* note 17, at 309–10; Paul, *Fabrication of Evidence*, *supra* note 12, at B10.

considered authentic. In fact, today it may be more accurate to say that a picture is worth a thousand lies.[37]

B. Modern, Digital Photography

Digital photography is the new norm for image capture.[38] Digital cameras, in contrast to their analog complements, do not store information in a continuous medium.[39] Instead, information is recorded in discrete bits of information called binary code,[40] which is a string of ones and zeroes[41] that makes up the storage language of hard drives, compact discs, computers, and all other digital devices.[42] By using a series of numbers, instead of the continuous crests and troughs characteristic of analog information,[43] digital image manipulation is much easier, cheaper, and infinitely more difficult to detect than an analog alteration.[44]

1. Advantages of Digital Photography

Whereas traditional film-based photography requires special photographic paper, processing time and costs, and malodorous and messy chemicals; digital, film-free photography does not have the same inherent drawbacks.[45] With digital photography, a photographer can check recently shot photos and re-shoot if necessary, make as many duplicates as desired without loss in image quality or a large lapse in time,[46] and immediately send pictures to anywhere in the world.[47] Additionally, digital photographs can be developed by the photographer who took them, and because they do not occupy any

37. Kimberly A. Wade et al., *A Picture Is Worth a Thousand Lies: Using False Photographs to Create False Childhood Memories*, PSYCHONOMIC BULL. & REV., Sept. 2002, at 597.

38. *See* Mike Musgrove, *Nikon Says It's Leaving Film-Camera Business*, WASH. POST, Jan. 12, 2006, at D1 ("A decade ago, digital cameras cost thousands of dollars, required technical proficiency to use and offered unclear images that took up large amounts of space on expensive memory cards. As prices for digital cameras and memory cards dropped year after year—and started to beat the prices and picture quality offered by film cameras—digital cameras rapidly took over the market").

39. Paul, *The "Authenticity Crisis," supra* note 13, at 46.

40. Guthrie & Mitchell, *supra* note 23, at 662.

41. *Binary Code*, MERRIAM WEBSTER'S COLLEGIATE DICTIONARY 114 (10th ed. 1993).

42. The Help Center: Answers to Computer Questions, What is the Difference Between Analog and Digital Technology?, http://www.sharpened.net/helpcenter/answer.php?62 (last visited Mar. 5, 2009).

43. *Id.*

44. Guthrie & Mitchell, *supra* note 23, at 673; Jill Witkowski, *Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images*, 10 WASH. U. J.L. & POL'Y 267 (2002); Douglas Page, *Forensics Focuses on Digital Photography*, FORENSIC MAG., Dec. 2006/Jan. 2007, http://www.forensicmag.com/articles.asp?pid=120; Rebecca Levy-Sachs & Melissa Sullivan, *Using Digital Photographs in the Courtroom: Considerations for Admissibility*, Aug. 2004, at 2, http://www.securitymanagement.com/archive/library/feature_August2004.pdf.

45. Keane, *supra* note 19, at 588; Christina Shaw, *Admissibility of Digital Photographic Evidence: Should It Be Any Different Than Traditional Photography?*, AM. PROSECUTORS RES. INST., 2002, *available at* http://www.thefreelibrary.com/The+admissibility+of+digital+photographs+in+criminal+cases-a0140790738; Page, *supra* note 44; Levy-Sachs & Sullivan, *supra* note 44, at 2.

46. Keane, *supra* note 19, at 588; Shaw, *supra* note 45; Page, *supra* note 44; Levy-Sachs & Sullivan, *supra* note 44, at 1.

47. Keane, *supra* note 19, at 588; Page, *supra* note 44; Levy-Sachs & Sullivan, *supra* note 44, at 1.

physical space, they are very easily stored.[48] Moreover, photographers no longer have to carry extra rolls of film because a single memory card, which can be smaller than a dime, is capable of storing thousands of pictures.[49]

All of the benefits of digital photography come at a price—a very low price.[50] By way of example, in 1999, a thirty-two-*mega*byte[51] memory card for a camera was priced at one thousand dollars.[52] Today, *one pair* of eight-*giga*byte[53] memory cards for a camera can be purchased for less than twenty-five dollars.[54] That is 512 times[55] the memory for one-fortieth[56] of the price. That means that sixteen gigabytes of memory today, at 1999 prices, would cost over half a million dollars.[57]

Digital cameras themselves have undergone a similar astronomical increase in caliber and plunge in price.[58] In 1991, Kodak introduced a 1.3-megapixel[59] digital camera that would hold 200 megabytes of data at a cost of $13,000.[60] Today, a 7.0-megapixel camera with a slot for memory cards, which allows for virtually unlimited image storage, can be purchased for less than ninety dollars.[61] On account of quality, cost, and convenience, digital cameras progressed from birth to ubiquity almost overnight.[62]

---

48. Levy-Sachs & Sullivan, *supra* note 44, at 1.

49. Renee Eng, *Hollywood Hoopla for SanDisk's New 8GB Memory Cards*, TGDAILY, Nov. 9, 2007, http://www.tgdaily.com/content/view/34798/97/.

50. *See* Paul, *The "Authenticity Crisis," supra* note 13, at 47 (explaining that in the 1990s, "digital cameras were esoteric devices costing many thousands of dollars. Suddenly they are everywhere, inexpensive, and of high quality.").

51. One megabyte is 1,048,576 bytes, or 8,388,608 bits of information. Megabyte – Definition from the Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/megabyte (last visited Feb. 8, 2009); *see* Byte – Definition from the Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/byte (last visited Mar. 5, 2009) (equating one byte with eight bits). A bit is the basic unit of information storage in a digital system; it is a binary digit, the one or zero in binary code. Bit – Definition from the Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/bit (last visited Mar. 5, 2009). Thirty-two megabytes is therefore 268,435,456 bits.

52. Keane, *supra* note 19, at 589.

53. One gigabyte is 1,073,741,824 bytes, Gigabyte – Definition from the Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/gigabyte (last visited Mar. 5, 2009); *see also* Byte – Definition from the Merriam-Webster Online Dictionary, *supra* note 51 (equating one byte with eight bits). Sixteen gigabytes is therefore 137,438,953,472 bits, or 512 times larger than thirty-two megabytes.

54. *See* amazon.com, SanDisk 8 GB SDHC Memory Card SDSDB-8192-A11(Retail Package), http://www.amazon.com/SanDisk-Memory-SDSDB-8192-A11-Retail-Package/dp/B000UZL0YU/ref=sr_1_3?ie=UTF8&s=electronics&qid=1239079278&sr=8-3(last visited Apr. 6, 2009) (selling one eight gigabyte memory card for $12.49, (two for $24.98) reduced from the original price of $44.99).

55. *See supra* text accompanying note 53 (calculations on sixteen gigabytes).

56. This number is derived from a simple calculation of 1000 divided by twenty-five.

57. If thirty-two megabytes cost $1000, then 512 times that would cost $512,000.

58. *See* Paul, *The "Authenticity Crisis," supra* note 13, at 47 ("Just 10 years ago digital cameras were esoteric devices costing many thousands of dollars. Suddenly they are everywhere, inexpensive, and high quality.").

59. A megapixel is a unit of measurement for an image containing one million discrete points of color, or pixels. The higher the megapixel count, the bigger the picture you can print without loss of quality. Kodak.com, Quick Review of Digital Terms, http://www.kodak.com/eknec/ PageQuerier.jhtml?pq-path=411&pq-locale=en_US (last visited Mar. 5, 2009).

60. Posting of Dan to Cheapshooter: Photography on a Budget, http://www.cheapshooter.com/2007/08/30/oh-how-far-weve-come-a-look-back-at-digital-camera-history/ (Aug. 30, 2007).

61. RadioShack.com, *supra* note 1.

62. Paul, *The "Authenticity Crisis," supra* note 13, at 47.

2. Digital Cameras Are Everywhere

It is estimated that by 2009, seventy percent of all households in the United States will have a digital camera.[63] In fact, so great has been the influx of digital cameras that Nikon, a major camera manufacturer, announced in early 2006 that it is leaving the business of selling film products to focus on the digital market.[64]

a. Police Use Digital Cameras

The criminal justice community first began using digital imaging in the early 1990s.[65] In 1997, the International Association for Identification ("IAI")[66] recognized in an official declaration that "electronic/digital imaging is a scientifically valid and proven technology for recording, enhancing, and printing images . . . ."[67]

At first, police agencies were disappointed in the caliber of digital images; however, as technology improved the quality and cost of the cameras, more and more film cameras were replaced by their digital counterparts.[68] Since then, digital cameras have become so pervasive in law enforcement that they are the preferred means of photo capture in nearly every major law enforcement agency in this country.[69] This has implications in the legal realm because police officers often submit photographs as evidence in court.[70]

b. Lawyers Use Digital Photographs

It should come as no surprise that lawyers have embraced digital technology. Increasing numbers of attorneys are lending support and illustrations to their arguments by using digital photographs.[71] This is true in both judicial and administrative settings.[72] Whereas a generation ago an attorney was likely to blow up a thirty-five millimeter picture for emphasis in the courtroom, now he is more likely to present an enhanced digital photograph to achieve the same, or arguably better, effect.[73] In fact, digital photographs

63. Ben Dobbin, *Aim, Shoot, Farm Out Prints*, SEATTLE TIMES, Feb. 23, 2006, at C1.

64. Musgrove, *supra* note 38, at D1.

65. Page, *supra* note 44.

66. The IAI is the oldest and largest forensic organization in the world. International Association for Identification, http://www.theiai.org (last visited Mar. 5, 2009).

67. Int'l Ass'n. for Ident. [IAI], *1997 Resolutions & Legislative Committee*, Res. 97-9 (1997), *available at* http://www.theiai.org/pdf/res97_9.pdf.

68. *Id.*

69. Erik C. Berg, *Legal Ramifications of Digital Imaging in Law Enforcement*, FORENSIC SCIENCE COMMUNICATIONS, Oct. 2000, http://www.fbi.gov/hq/lab/fsc/backissu/oct2000/berg.htm; *see* Witkowski, *supra* note 44 (noting that digital pictures are used much more in law enforcement now than they used to be); Shaw, *supra* note 45 (same).

70. *See, e.g.*, Brian Bergstein, *Digital Photos Pose Issues in Court*, CRN, Feb. 08, 2004, *available at* http://www.crn.com/digital-home/18831429 (relating some of the concerns law enforcement agencies have with presenting digital photographs in the courtroom).

71. Guthrie & Mitchell, *supra* note 23, at 669 n.54.

72. *Id.*

73. Edward J. Imwinkelried, *Can This Photo Be Trusted? Digital Photos Can Be Enhanced to Help*

used as exhibits at trial substantially outnumber those created from traditional film.[74]

3. Digital Images Are Easy to Manipulate

The National Aeronautics and Space Administration introduced digital image manipulation almost forty years ago in an effort to prevent the degradation of images captured in space.[75] The atrophy of the image quality of a photograph was anticipated mathematically and then preemptively counteracted by tweaking the image's sharpness, brightness, and contrast.[76] Since then, the manipulation of digital images has expanded beyond the exclusive realm of rocket scientists and übergeeks to become more of a household-level venture.[77] This is possible because the cost of manipulating photos has quickly plummeted.[78]

Tools for manipulating digital images can come at little or no cost to the consumer: image manipulation software is included free with operating system software[79] and is often included with a new digital camera.[80] Google's Picasa, a free image-cataloguing program, also comes with some rudimentary, yet very powerful, image enhancement tools.[81]

The millions of consumers who are willing to spend a moderate sum to purchase Adobe Photoshop[82] can create sophisticated alterations with ease.[83] Using Photoshop, anyone can crop images to either emphasize a portion of it or eliminate something unwanted, remove flash-induced red eye, modify the overall brightness and contrast of an image, and darken or lighten color tones.[84] An inexperienced layperson can perform these tasks with little effort.[85] With a moderate amount of expertise and experience, those with the

---

Jurors—or Manipulated to Mislead Them. Use your Digital Images Carefully, and Know When to Challenge your Opponent's, TRIAL, Oct. 1, 2005, at 48.

74. Michael Cherry & Edward Imwinkelried, *Forensics: A Cautionary Note About Fingerprint Analysis and Reliance on Digital Technology*, CHAMPION, Aug. 2006, at 27; *Case Blurb: Lorraine; Authenticating Digital Photographs*, Sept. 24, 2007, http://postprocess.wordpress.com/2007/09/24/ case-blurb-lorraine-authenticating-digital-photographs/.

75. Cherry & Imwinkelried, *supra* note 74, at 29.

76. *Id.*

77. Guthrie & Mitchell, *supra* note 23, at 673; Witkowski, *supra* note 44, at 271; Page, *supra* note 44; Levy-Sachs & Sullivan, *supra* note 44, at 2; *see also* Dean P. Davison, *What's the Verdict on Digital Evidence? The Canadian Experience Shows that Many Issues Related to the Admissibility of Digital Images in Court Proceedings Remain Unresolved*, SECURITY MGMT., May 1, 2005, at 142 (emphasizing the ease of manipulating digital images).

78. Paul, *Fabrication of Evidence*, *supra* note 12, at B10.

79. *See* Windows Vista Paint – Adobe Photoshop CS3 Killer, http://news.softpedia.com/ news/Windows-Vista-Paint-Adobe-Photoshop-CS3-Killer-63762.shtml (last visited Mar. 5, 2009) (discussing the paint feature included with Windows Vista).

80. *See* Keane, *supra* note 19, at 590 (explaining the features of PhotoStudio, software that came included with the author's camera).

81. Picasa, *supra* note 4.

82. Paul, *Fabrication of Evidence*, *supra* note 12, at B12; *see also* Beckman & Hirsh, *supra* note 20 (indicating that Adobe Photoshop is one of the most popular image-manipulation tools).

83. Beckman & Hirsh, *supra* note 20.

84. *Id.*

85. Paul, *Fabrication of Evidence*, *supra* note 12, at B12.

know-how can make infinitely more complicated alterations; opening a closed door,[86] adding water or snow where there was none,[87] aging the subject of a photo,[88] and changing what someone is wearing[89] are just a few of the things that a savvy user can do with Photoshop, some skill, and a little imagination.

4. Digital Manipulations Are Difficult to Detect

Digital manipulation is difficult to detect, plain and simple.[90] Unlike the artifacts left behind with an analog cut-and-paste job, digital alterations to an image do not, per se, leave any traces of change.[91] In fact, it is possible, and not difficult, to create a digital photograph with an empty pedigree—leaving no trace as to its origin.[92]

Because digital media consists entirely of ones and zeroes, it is a simple matter to chop the information into bits, manipulate it, and then put it back together without a trace.[93] But it does not always take skill, experience, or even cognizance to alter a digital photo; often, digital images are inadvertently changed.[94] Power surges, hardware failures, viruses, and human error can all be culprits in unintentional image manipulation.[95] Image compression, a very common and often unknowing way in which consumers store their pictures, also alters an image, thereby disturbing its integrity.[96]

5. Analog Prints Can Be Digitized

Converting an analog negative into a digital file was not feasible until recently. Similar to the trends in price and quality of memory cards and digital cameras, scanners have increased in quality and come down dramatically in price. Not long ago, a high-quality scan of a thirty-five millimeter negative required a $30,000 drum scanner.[97] Today, a negative scanner can be purchased for less than $150.[98] Lacking a negative, anybody can digitize a

86. STEVE CAPLIN, HOW TO CHEAT IN PHOTOSHOP: THE ART OF CREATING PHOTOREALISTIC MONTAGES 292-93 (3d ed. 2005).

87. *Id.* at 204–09.

88. *Id.* at 180–81.

89. *Id.* at 170–71.

90. Guthrie & Mitchell, *supra* note 23, at 673; Harts, *supra* note 12, at 521; Keane, *supra* note 19, at 587; Witkowski, *supra* note 44, at 271; Davison, *supra* note 77, at 142; Golab, *supra* note 12, at 32; Levy-Sachs & Sullivan, *supra* note 44, at 2; Page, *supra* note 45.

91. Paul, *The "Authenticity Crisis," supra* note 13, at 48; Paul, *Fabrication of Evidence*, *supra* note 12, at B12.

92. Bianchini & Bass, *supra* note 17, at 311.

93. Paul, *The "Authenticity Crisis," supra* note 13, at 48.

94. Cherry & Imwinkelried, *supra* note 74, at 29; Berg, *supra* note 69.

95. Berg, *supra* note 69.

96. Guthrie & Mitchell, *supra* note 23, at 665; Witkowski, *supra* note 44, at 270–71; Steven B. Staggs, *The Admissibility of Digital Photographs in Court*, CRIME SCENE INVESTIGATIOR, May 2, 2001, http://www.crime-scene-investigator.net/admissibilityofdigital.html.

97. Paul, *The "Authenticity Crisis," supra* note 13, at 46.

98. *See* Canon, CanoScan LiDE 600F Film and Negative Scanner, http://www.usa.canon.com/consumer/controller?act=ModelInfoAct&fcategoryid=120&modelid=14004 (last visited Mar. 5, 2009) (suggesting a retail price of $149.99 for this color image scanner).

35mm print with the use of a scanner.[99]

Digitizing an analog print or negative introduces another opportunity for inadvertent alteration.[100] Once digitized, the image derived from a photo or negative is susceptible to the same digital-manipulation tools that make alterations to digitally born photos.[101] Digital photography is not merely producing original digital images; it is reaching into the past and converting all images into binary bits, which then have the same potential for seamless and undetectable manipulation as those that have digital origins.

C. Photographs as Evidence

The ubiquity of tools for the digital capture and manipulation of images has created cause for concern in the courtroom.[102] The drafters of the Federal Rules of Evidence did not contemplate, much less anticipate, the kinds of changes that photography has undergone.[103] The Federal Rules do not differentiate between digital and analog photographs,[104] so relevance and authenticity are determined in the same manner for both.[105] Consequently, the Federal Rules, particularly those dealing with evidence, are maladapted to deal with digital images.[106]

1. The Problem with Photographs

A picture's power to persuade cannot be overemphasized.[107] The purpose of any trial is to persuade the finders of fact.[108] If the fact finders are going to give undue influence to pictures just because they can see them, this presents a panoply of problems because the ultimate purpose of a trial is to determine the truth.

Jurors often are bored, confused, and frustrated when attorneys or witnesses try to explain technical or complex material.[109] However, when attorneys present the same material with visual aids that simplify these

99. Bianchini & Bass, *supra* note 17, at 313; Guthrie & Mitchell, *supra* note 23, at 663; Golab, *supra* note 12, at 32.

100. Imwinkelried, *supra* note 73, at 49.

101. 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, 375 (1992); Levy-Sachs & Sullivan, *supra* note 44, at 2 (regarding prints); Beckman & Hirsh, *supra* note 20 (regarding negatives).

102. *See* Paul, *The "Authenticity Crisis," supra* note 13, at 46 ("digital technology has fundamentally changed the world of real evidence . . . .").

103. Bianchini & Bass, *supra* note 17, at 305–06.

104. MCCORMICK ON EVIDENCE, 214 (5th ed., 2003 Pocket Part).

105. FED. R. EVID. 1001(2) (defining photographs to include still photographs, X-ray films, video tapes, and motion pictures); Witkowski, *supra* note 44, at 282; Page, *supra* note 44; Levy-Sachs & Sullivan, *supra* note 44, at 2.

106. Witkowski, *supra* note 44, at 286.

107. *See* Guthrie & Mitchell, *supra* note 23, at 670–71 ("[J]urors tend to focus primarily on visual, rather than oral, evidence.").

108. Harts, *supra* note 12, at 520.

109. Roy Krieger, *Now Showing at a Courtroom Near You . . . Sophisticated Computer Graphics Come of Age—and Evidence Will Never Be the Same*, A.B.A.J., Dec. 1992, at 92, 93.

complex issues, the pendulum can swing too far in the other direction.[110] Because jurors may retain as much as 85% of what they learn visually and as little as 10% of the information they hear,[111] the verdict a jury renders may have more to do with how memorable a photograph is, rather than what the jury has heard from lawyers and witnesses.[112] Additionally, because of the fidelity of analog photographs, jurors trust all prints, even ones that have been digitally altered.[113]

Even if jurors were more skeptical, "[t]here is absolutely no way the average juror c[ould] tell the difference between a doctored and a pure photo."[114] The coupling of a juror's unwarranted trust in digital photographs and the ever-increasing possibility that counterfeit photos are being authenticated make it feasible to conclude that this spells "the end of photography as evidence of anything."[115] Even if the situation has not extended to that extreme, it is certain that digital technology has forever changed the world of evidence, especially with regard to photographs.[116] To preserve both digital and analog photographs as trustworthy and viable sources of evidence, the standards for authenticity must be such that they guarantee that the photos admitted into evidence are what they purport to be.

2. Admitting Photographs as Evidence

To be admitted into evidence, a photograph must first be deemed relevant[117] and authentic.[118] The purpose for which the picture is to be admitted determines the standard of authentication.[119] A photograph can be admitted as substantive or demonstrative evidence.[120] Substantive evidence is evidence that goes to prove a fact at issue.[121] Demonstrative evidence, on the other hand, is evidence that appeals directly to the senses and can help to

110. *See* Noelle C. Nelson, *A New Generation of Jurors?*, TRIAL, July 1997, at 54 (explaining that a generation accustomed to fast-paced visual aids like movies and video games have attention spans much more compatible with high-tech visual aids in the courtroom).

111. *See* Robert F. Seltzer, *Preparation and Trial of a Toxic Tort Case 1990: Evidence and Exhibits at Trial*, 387 PRAC. L. I. LITIG. 371, 375 (1990) (claiming that people in general retain 87% of visual information but only about 10% of what they hear).

112. It only makes sense that jurors will make decisions based on what they remember. Other studies have looked at how much jurors remember after three days have passed. John Selbak, Comment, *Digital Litigation: The Prejudicial Effects of Computer-Generated Animation in the Courtroom*, 9 HIGH TECH. L. J. 337, 360 (1994). The study suggested that when information is presented visually and orally, 65% of that information is retained after three days, while they can only remember 10% of the information presented without accompanying visual aids. *Id.*

113. Paul, *The "Authenticity Crisis," supra* note 13, at 46–47.

114. Nelson, *supra* note 14, at B2 (quoting Bob Jennings, head of the Evidence Photographers International Council).

115. Stewart Brand et al., *Digital Retouching: The End of Photography as Evidence of Anything*, WHOLE EARTH REV., July 1985, at 42.

116. Paul, *supra* note 12, at B10.

117. FED. R. EVID. 401.

118. FED. R. EVID. 901.

119. Harts, *supra* note 12, at 514; Guthrie & Mitchell, *supra* note 23, at 697.

120. Harts, *supra* note 12, at 514–17.

121. *Id.*

explain or illustrate difficult-to-understand concepts in the case.[122] Examples of demonstrative evidence include charts, maps, x-rays, and models.[123] With demonstrative evidence, the standard for authentication is somewhat relaxed,[124] but as will be shown below, neither standard suffices to prevent altered photographs from becoming evidence that a jury will trust.

a. Authenticating Substantive Evidence

When admitting any object as substantive evidence in connection with the commission of a crime, it is necessary as part of the authentication process for the propounding attorney to prove that the object is in substantially the same condition as it was at the time the crime was committed.[125] If the judge is satisfied that the object has not been tampered with, or otherwise altered in a way that is relevant to ascertain the defendant's guilt or innocence, she may permit its admittance.[126]

The standard is similar for photographs. To authenticate a photograph, a witness need only testify that the photo fairly and accurately portrays the scene.[127] If there is only a remote chance that the photograph is materially different from the original scene, or has been distorted, nothing more is required.[128] However, due to the ease with which digital photographs are manipulated,[129] and the expanding scope of the public's use and reliance upon them,[130] the scrutiny with which digital photographs are considered before being admitted into evidence should be heightened.[131]

In essence, the courts today simply take the witness's word that a digital photograph has not been tampered with. Neither the photographer, nor anyone subsequently handling the picture, nor a witness who was present when the picture was taken, is required to testify.[132] If a dissembling witness were to take the stand and intend to use a doctored photograph to deceive the court, ascertaining the truth would be difficult at best.[133] Even more common, if the witness is testifying to a photograph he does not know has been changed, or

122. Kenneth S. Brown et al., MCCORMICK ON EVIDENCE, 212 (5th ed. 1999).

123. *Id.* at 213.

124. *Id.*

125. United States v. S. B. Penick & Co., 136 F.2d 413, 415 (2d Cir. 1943).

126. Gallego v. United States, 276 F.2d 914, 917 (9th Cir. 1960); *see also* McEntyre v. State, 717 S.W.2d 140, 147 (Tex. App. 1986) (explaining, in the context of tapes, that the record of preservation must indicate that the trustworthiness and reliability of what the tapes contain has not been compromised).

127. Brown, *supra* note 122 at 214.

128. *Id.* at 966.

129. Page, *supra* note 44.

130. Levy-Sachs & Sullivan, *supra* note 44, at 2.

131. Beckman & Hirsh, *supra* note 20; Page, *supra* note 44.

132. 29A AM. JUR. 2D *Evidence* § 966 (2007); Paul, *The "Authenticity Crisis," supra* note 13, at 47; Bianchini & Bass, *supra* note 17, at 319–20.

133. Bianchini & Bass, *supra* note 17, at 309. Some law enforcement agencies take the stance that digital photographs should not be treated any different than traditional ones. They believe that the issue should be the integrity of the person on the stand, not the integrity of the photograph. Witkowski, *supra* note 44, at 282. This is shortsighted, however. Even if we were to put complete trust in an unimpeached witness, the fact that a witness is being honest does not mean that the picture accurately depicts the scene pictured. A witness can tell the truth and still be wrong.

has inadvertently changed it himself, uncovering the truth would be even more problematic.[134] This is not inconceivable considering that witnesses are usually testifying about pictures years after they were present at the scene.[135]

Until recently, any deliberate or unintentional alterations in a photograph were very easy to detect, so the courts have only just become vulnerable to these issues in approximately the last decade.[136] Even more disconcerting is that sometimes the court's only check against fraudulent photographs is the cross-examining attorney, who is expected to ferret out the fakes, usually without the aid of extrinsic evidence.[137]

i. Chain of Custody

Sometimes, proof of chain of custody is required to authenticate an image.[138] Chain-of-custody requirements include either showing that the image is an unedited original, or providing a log of all the possessors of the image and all the changes that have been made.[139] Although chain-of-custody requirements are a good way to ensure that the photos entered into evidence are accurate representations of the images they depict, they are only rarely required.[140]

ii. Best-Evidence Rule

The Federal Rules of Evidence require that any photograph submitted to prove the truth of the matter it asserts (i.e. substantive evidence) should be an original.[141] This is known as the best-evidence rule.[142] However, digital photographs prove to be a proverbial wrench in this set of gears, and trying to define an original digital image becomes wrought with problems.[143] Some legal experts consider that a digital image should be limited to the version of the image contained on the disk drive of the camera, before being uploaded;[144] others consider the image on the floppy drive or compact flash card good enough.[145] In practice, however, almost any digital image, no matter how many generations down the family tree from the "original," is considered an

134. *See supra* text accompanying notes 94–96 (citing examples of how photos can be inadvertently altered).

135. Paul, *The "Authenticity Crisis," supra* note 13, at 47.

136. *See supra* text accompanying notes 28–34 (explaining how easy it is to detect analog manipulations to photographs).

137. Paul, *The "Authenticity Crisis," supra* note 13, at 47.

138. M. L. Cross, Annotation, *Authentication or Verification of Photograph as Basis for Introduction in Evidence*, 9 A.L.R.2d 899, 901 (1950).

139. Page, *supra* note 44; Levy-Sachs & Sullivan, *supra* note 44, at 4.

140. Cross, *supra* note 138, at 901.

141. FED. R. EVID. 1001–04.

142. 29A AM. JUR. *Evidence* § 1083 (2008).

143. *Id.* (emphasizing that JPEG metadata may help avoid the complexities associated with digital photographic evidence).

144. Page, *supra* note 44; Levy-Sachs & Sullivan, *supra* note 44, at 4. You can imagine, however, how problematic it would be trying to use the LCD viewfinder of a camera in a courtroom, often measuring smaller than two inches, if such a limited notion of "original" were adopted.

145. Keane, *supra* note 19, at 591.

original for purposes of the best-evidence rule[146] because exact copies can be made of digital files without any loss of quality between generations.[147] As a result of these difficulties, it may be true that the notion of an original is obsolete.[148] The best-evidence rule illustrates another instance where the Federal Rules, as they stand, are ill-equipped to ensure the authenticity of digital images accepted as evidence in a courtroom.

b. Authenticating Photographs as Demonstrative Evidence

Demonstrative evidence can be a powerful tool to help the factfinders understand a difficult concept, reinforce their beliefs, or even persuade them to, or dissuade them from, believing something.[149] The rules for admitting demonstrative evidence are more relaxed than they are for substantive evidence,[150] which creates even greater potential for admittance of false positives. Demonstrative evidence implicates neither the best-evidence rule,[151] nor chain-of-custody requirements.[152]

The danger of fraudulent photographs being admitted as reliable, authentic evidence "presents a looming and perplexing dilemma for the legal system. One for which there is no easy answer."[153] Indeed, "the computer . . . presents a real danger of being the vehicle of introducing erroneous, misleading, or unreliable evidence."[154] To substantiate this fact, more than ever before, photographic evidence is being challenged in court, in both the criminal and civil arenas.[155] And forensic photographers are being called in with more frequency to prove that photos are phony.[156] And yet, even taking these increased precautions regarding digital photographs, so great is the extent to which lawyers and courts trust digital images that they only rarely challenge them.[157] In other words, challenges to photographs in court went from non-existent to very rare. As awareness of photographic chicanery increases, so too will the challenges to them in court. If neither the legislature nor the Supreme Court establishes a reliable standard for authentication, the responsibility will be relegated to the opposing counsel to ensure the authenticity of images. Because lawyers will lack the legal tools to do so, the thousand words of a photo will be untrustworthy.

---

146. *See* FED. R. EVID. 1001(3) ("[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'").

147. Witkowski, *supra* note 44, at 272; Levy-Sachs & Sullivan, *supra* note 44, at 1.

148. 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.

149. Harts, *supra* note 12, at 516.

150. Shaw, *supra* note 45.

151. *Id.*

152. Paul, *Fabrication of Evidence*, *supra* note 12, at B10.

153. Bianchini & Bass, *supra* note 17, at 313.

154. Perma Research & Dev. v. Singer Co., 542 F.2d 111, 125 (2d. Cir. 1976) (Van Graafeiland, J., dissenting).

155. Nelson, *supra* note 14, at B2.

156. *Id.*

157. Witkowski, *supra* note 44, at 285.

III. ANALYSIS

Due at least in part to the growing concern that digital images cannot, and should not, be trusted, both Congress and sundry courts have drafted rules and opinions to mitigate some of the ill effects thereby generated.[158] Although the intents of these legislative and judicial entities are aimed true, the results of their efforts have fallen short of a legitimate solution. This is likely because the problem is merely narrowed in scope. Moreover, none of these solutions applies across the board.[159] Furthermore, the Supreme Court has never directly addressed the issue.

A. The Common–Law Digital Dilemma

In most cases, for a photograph to be authenticated—digital or analog—a witness need only testify that it fairly and accurately depicts the scene.[160] This is problematic for several reasons: often the witness is questioned about the photograph years after it was taken,[161] frequently the witness would not notice if the photograph had been changed,[162] and too often the witness is lying.[163]

Police officers are among those who most often lie.[164] In fact, lying among police officers has become so pervasive, that in some jurisdictions, the officers themselves have given it a nickname: testilying.[165] In one study, it is estimated that on Fourth Amendment issues alone, police commit perjury between twenty and fifty percent of the time.[166] This dishonesty is especially fraught with negative implications in the authenticity of digital photographs when coupled with the fact that courts presume too much in regards to photographs provided by police and other government officials: these officers and officials are presumed to have followed proper procedure in taking the

158. *See infra* text accompanying notes 185–297 (discussing court-created standards of evidence and their relevance to verifying photograph authenticity).

159. As will be explained later, the FRCP amendment of 2006 does not completely solve the problem because false positives can still get through the metadata provision. In addition, the FRCP does not apply to criminal cases. As for the common-law attempts at a solution, these have not solved the problem either, and none of them apply to any more than the small jurisdiction under the purview of the court that wrote them.

160. FED. R. EVID. 901; 29A AM. JUR. 2D *Evidence* § 975 (2008).

161. Paul, *The "Authenticity Crisis," supra* note 13, at 47.

162. *See supra* text accompanying notes 94–96 (describing unintentional image manipulation). If the witness does not know the photograph has been digitally altered, there is no reason to believe she will be better equipped to detect this alteration than anyone else.

163. James C. McCloskey, Executive Dir. and Bd. President, Centurion Ministries, Address at the John Jay College of Criminal Justice: Commentary: Convicting the Innocent (Winter/Spring 1989) (excerpts available at http://www.truthinjustice.org/convicting.htm) ("The recent District Attorney of Philadelphia once said, 'In almost any factual hearing or trial, someone is committing perjury; and if we investigate all of those things, literally we would be doing nothing but prosecuting perjury cases.'").

164. *Id.*

165. Christopher Slobogin, *Testilying: Police Perjury and What to Do About It*, 67 U. COLO. L. REV. 1037, 1040 (1996).

166. Myron W. Orfield, Jr., *Deterrence, Perjury, and the Heater Factor: An Exclusionary Rule in the Chicago Criminal Courts*, 63 U. COLO. L. REV. 75, 83 (1992); *see also* McCloskey, *supra* note 163 ("The words of one twenty-five-year veteran senior officer of a northern New Jersey police force still ring in my ears: . . . 'I don't know one of my fellow officers who hasn't lied under oath.' Not too long ago a prominent New York judge, when asked if perjury by police was a problem, responded, 'Oh, sure, cops often lie on the stand.'").

photographs,[167] presumed not to have altered a scene before they photograph it,[168] and apparently are also presumed not to have altered a photo after taking it.

Even more problematic is the fact that lawyers themselves are sometimes prone to lie.[169] Some conjecture that many lawyers, even good lawyers, are untruthful in their profession.[170] Lawyer lying ranges from stretching points and arguing perverse interpretations of the facts,[171] and coaching witnesses, or suggesting "better" answers;[172] to padding timesheets to meet billable-hours requirements,[173] and putting a witness on the stand to lie, perhaps while "intentionally avoiding learning the facts of a case to avoid suborning perjury."[174]

The notion that lawyers are dishonest comes as no surprise to a large portion of the population; since 1976, no more than a quarter of the population has given lawyers "high" or "very high" "honesty and ethical standards" evaluations in Gallup polls.[175] In fact, about half of the public regards at least one-third of all lawyers as dishonest.[176] There are some practical consequences of a system full of dishonest lawyers. For instance, each state has a client protection fund, which reimburses clients who were victims of their lawyer's dishonesty.[177] Because lawyers play such an integral role in the justice system, a dishonest lawyer can frustrate the entire legal process and its truth-finding purpose.[178]

Despite the potential for dishonesty in many of the people involved, some believe that the solution to the use of falsely authenticated digital images as evidence should be the same as it always has been—let its authenticity hinge on the truthfulness of the witness.[179] However, sometimes a photograph can be admitted without witness testimony, under the "silent witness" theory, which permits authentication of photographs based on the trustworthiness of the

---

167. United States v. Mojica, 746 F.2d 242, 245 (5th Cir. 1984).

168. *Id.*

169. *See, e.g.*, MARK PERLMUTTER, WHY LAWYERS AND THE REST OF US LIE AND ENGAGE IN OTHER REPUGNANT BEHAVIOUR 19 (Bright Books, 1998) ("But what's truly pernicious in the American legal system is the daily dissembling about which most of us are unconscious.").

170. Dale R. Harris, *Do Lawyers Lie?*, COLO. LAW., Sept. 2000, at 19, 19, *available at* http://65.45.99.70/tcl/tcl_articles.cfm?ArticleID=802.

171. *See generally* Fred C. Zacharias, *Reconciling Professionalism and Client Interests*, 36 WM. & MARY L. REV. 1303 (1995) (analyzing the tensions between professional ethics and zealous client advocacy in regards to how far lawyers will stretch their personal ethics).

172. Franklin Strier, *Making Jury Trials More Truthful*, 30 U.C. DAVIS L. REV. 95, 118 (1996).

173. Harris, *supra* note 170, at 19.

174. *Criminal Law Notes*, ARMY LAW., July 1991, at 21, 23.

175. Chris Guthrie, *The Lawyer's Philosophical Map and the Disputant's Perceptual Map: Impediments to Facilitative Mediation and Lawyering*, 6 HARV. NEGOT. L. REV. 145, 169 (2001) (citing Amy E. Black & Stanley Rothman, *Shall We Kill All the Lawyers First?: Insider and Outside Views of the Legal Profession*, 21 HARV. J. L. & PUB. POL'Y 835, 852 t.6 (1997)).

176. Mark Galanter, *Predators and Parasites: Lawyer-Bashing and Civil Justice*, 28 GA. L. REV. 633, 663 (1994).

177. Carole R. Richelieu & Darryn Manuel, *Ethics & Issues*, HAW. B. J., July 10, 2006, at 16.

178. In re McGrath, 655 P.2d 232, 237 (Wash. 1982).

179. Witkowski, *supra* note 44, at 282 n.67; Brian Barakat & Bronwyn Miller, *Features: Authentication of Digital Photographs Under the "Pictorial Testimony" Theory: A Response to Critics*, 78 FLA. BAR J. 38 (2004).

process that created them.[180] Additionally, because digital manipulations are so difficult to detect,[181] because many witnesses actually commit perjury,[182] and because a photograph is deemed as good as the witness' word,[183] there must be better safeguards in place to protect the courts and the parties therein from this particular kind of fraud.

Not surprisingly, some courts have attempted to mitigate this problem.[184] As shown below, these efforts fall short of resolving the potential for this abuse.

1. Expert Testimony

Cases involving digitally enhanced photographs often rely on experts to give credence to the digital-enhancement process.[185] For seventy years, several circuit courts relied on *Frye v. United States*, 54 App. D.C. 46 (D.C. Cir. 1923), to determine whether the scientific processes or theories used to enhance the value of evidence was "generally accepted" in a given scientific field.[186]

In 1993, the Supreme Court overruled *Frye*, concluding that Federal Rule of Evidence 702, enacted in 1975, superseded the *Frye* standard.[187] Instead, it proposed a new standard, a four-factor test, which infused both a "reliable foundation" and "relevance" into an inquiry regarding expert testimony.[188] These *Daubert* factors included: (1) whether the evidence has been subjected to peer review, (2) whether the expert's theories and methods can be tested, (3) the error rates in studies and test results, and (4) the degree of acceptance of the expert's theories and methods.[189]

The *Daubert* standard and the *Frye* standard (insofar as the latter is still being used by state courts),[190] go a long way to ensure that evidence is not admitted that does not first successfully undergo scrutiny of the scientific community and measures of relevance by the judge. For example, the use of DNA, now almost universally accepted as a scientifically sound method of identification, under *Daubert*, is usually admitted as evidence so long as proper procedures are undertaken in the lab.[191]

---

180. 29A AM. JUR. 2D *Evidence* § 967 (2007).

181. *See supra* text accompanying notes 90–96 (describing the difficulties of identifying digital manipulation).

182. *See supra* text accompanying notes 163–66 (describing the prevalence of perjury).

183. FED. R. EVID. 901; 29A AM. JUR. 2D *Evidence* § 965 (2007).

184. *See infra* text accompanying notes 185–243 (describing case law involving digitally enhanced photography).

185. *See, e.g.*, State v. Hayden, 950 P.2d 1024, 1026 (Wash. Ct. App. 1998) (relying on an expert to explain what process was used to remove the fiber pattern from a bed sheet to isolate a bloody handprint for identification).

186. Elizabeth L. DeCoux, *The Admission of Unreliable Expert Testimony Offered by the Prosecution: What's Wrong with* Daubert *and How to Make It Right*, 2007 UTAH L. REV. 131, 142 (2007).

187. Daubert v. Merrell Dow Pharm., 509 U.S. 579, 591 (1993).

188. *Id.* at 597.

189. *Id.* at 593–95.

190. *See infra* text accompanying note 214 (describing the Washington Supreme Court's continued use of the *Frey* standard).

191. Karen Cormier et al., *Evolution of DNA Evidence for Crime Solving - A Judicial and Legislative*

Although these standards have significant utility concerning the admittance of testimony by an expert, they do not address a digitally altered photograph, submitted as evidence to the court, when the attorney is either unaware that it has been altered, or intentionally trying to defraud the court. This is true because in such cases experts are rarely, if ever, called.

2. Specific Cases Treating the Issue of Digital-Image Authentication

Although few courts doubt that a photo fails to depict accurately the image it portrays, there have been a number of cases where a photo's authenticity has been called into question, for various purposes and with varying degrees of success.

a. Kaps Transport v. Henry

The court in *Kaps Transport v. Henry*, 572 P.2d 72 (Alaska 1977), attempted to reconcile the concept of authenticity with photos that appeared to have been tampered with.[192] Though digital image manipulation was still only in use by scientists at this time, the simpler art of misrepresentation through analog photographs was not unheard of.[193]

Kaps Transport owned a big-rig truck and was sued after one of its trucks collided with a vehicle moving in the opposite direction on a two-lane highway. The truck jack-knifed, blocking the highway, and then was hit by another vehicle.[194]

In the subsequent lawsuit, the plaintiff hired "an expert in accident reconstruction and photographic interpretation" to analyze photos taken by the police on the scene.[195] He was to ascertain from the photos to what extent, if at all, the big rig had strayed into the opposite lane before the accident, and to testify to that effect.[196] His testimony was that the semi had been eighteen inches over the center line just prior to the accident.[197]

On cross-examination, the defendant submitted a photograph of two Ford Mustangs for his inspection and asked him, based on his expert opinion, to analyze the distance between them.[198] He did some calculations and rendered his opinion, but not before expressing doubt as to the authenticity of the photograph—in his opinion it was a "trick photograph."[199] It was indeed, a "trick photograph;" one of the Mustangs in the picture was a full-size car and one was a toy.[200] The defendant sought to impeach the expert witness by using

History, FORENSIC MAG., June/July 2005, http://www.forensicmag.com/articles.asp?pid=45.

192. Kaps Transport v. Henry, 572 P.2d 72 (Alaska 1977).
193. CNET, *supra* note 26.
194. *Kaps Transport*, 572 P.2d at 73.
195. *Id.* at 75.
196. *Id.*
197. *Id.*
198. *Id.*
199. *Id.*
200. *Id.* at 76, n.7.

two different sized cars to frustrate the perspective analysis.[201]

Although the court rejected this easily detected analog fraud, it ruled, "inaccuracies or defects in the photograph [do] not necessarily render it inadmissible as long as there is an explanation of these imperfections so that the jury is not misled."[202] In other words, the same photograph could have been admitted, but only insofar as the defendant disclosed the true nature of each of the cars depicted therein.

The standard pronounced by the court in *Kaps Transport* does little to mitigate the issue with regard to digitally manipulated photographs for at least two reasons: (1) digital alterations are not always intentional,[203] and (2) when a party wishes to defraud the court, it certainly will not disclose imperfections, or provide explanations for them. Additionally, unlike in 1977, when *Kaps Transport* was decided, today's "trick photographs" are not so easy to detect as to give themselves away after a quick look by a testifying witness.[204]

b. State v. Hayden

In 1998, the issue of digital enhancements once again surfaced in a courtroom setting.[205] Defendant Hayden was convicted of murdering a twenty-seven-year-old female student.[206] While committing the crime, Hayden left bloody handprints on the victim's bed sheets.[207]

A minimum of eight points of comparison is needed to make a positive identification from a handprint.[208] During the course of the investigation, a latent print examiner used dyes, alcohol, and water, using standard chemical processes to try extracting a handprint from the sheets in sufficient detail that identification would be possible.[209] Using only these "analog" techniques, the examiner was unsuccessful.[210]

An expert in enhanced digital imaging then took pictures of the prints and used a computer to remove the background texture of the sheet and otherwise fine-tune the image.[211] The computer enhancement produced twelve points of comparison on one print and more than forty on another, making it possible to match the handprints to their owner.[212] The defendant was thus identified.[213]

The court conducted a *Frye* hearing[214] to determine if the enhancement

201. *Id.* at 75.
202. *Id.* at 75–76 (citations omitted).
203. *See supra* text accompanying notes 94–96 (describing unintentional digital manipulation).
204. *See supra* text accompanying note 44 (describing why digital manipulation is more difficult to detect than analog alteration).
205. State v. Hayden, 950 P.2d 1024 (Wash. Ct. App. 1998).
206. *Id.* at 1025.
207. *Id.*
208. *Id.*
209. *Id.*
210. *Id.*
211. *Id.*
212. *Id.*
213. *Id.*
214. Though *Frye v. United States* was superceded by both the Federal Rules of Evidence and *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, the Supreme Court of Washington nonetheless declined to adopt *Daubert*,

process was scientific evidence that was "generally accepted in the relevant scientific community."[215] The court concluded that the "analog" chemical processes were generally accepted by forensic scientists and that the digital enhancement of images did not need to be subjected to a *Frye* hearing because it was not novel.[216] Nonetheless, they concluded that the digital enhancements satisfied the *Frye* test.[217]

On appeal, Hayden contended that the use of digital enhancements is novel as applied to forensic science and did not meet the strictures set forth in *Frye*.[218] The court analyzed the forensic digital imagine de novo and affirmed the lower court, concluding that the use of digital imaging in forensics is not novel and is generally accepted in the relevant scientific community.[219]

In *Hayden*, the question of authenticity is somewhat cloaked. At issue was whether the image of handprints, which matched the defendant's prints, had been enhanced in a way that was trustworthy.[220] The court did not directly consider in its opinion whether the photographs were what they purported to be (images of the handprints taken from the crime scene).[221] Interestingly, the court in this case did not have to rely on the witness's word that the original photographs actually depicted bloody prints taken from the scene, that the enhanced image was directly derived from those original images, or that nothing more had been changed at the scene or in the picture than what had been testified to at trial.[222] Because the actual bed sheet that was photographed and digitally enhanced was available to the court for examination, the court could verify that nothing had been added to the image that was not present on the sheet.[223] Although this would still leave open the possibility of the sheet being tampered with before being photographed, in rare cases like this, where courts can compare the object photographed with the photograph itself, courts can be more confident that the photographs truly are authentic.

c. Almond v. State

Only rarely does a civil case broach the topic of digital image authentication; the courts that do are usually conducting a criminal

preferring the time-tested *Frye* standard. *State v. Copeland*, 922 P.2d 1304, 1313–15 (Wash. 1996). The court also declined to interpret its own rule of evidence *in pari materia* to the parallel federal rule. *Id.* at 1314.

215. *Hayden*, 950 P.2d at 1026.

216. *Id.*

217. *Id.*

218. *Id.*

219. *Id.* at 1027–28.

220. The court couches the issue in terms of it being "generally accepted in the relevant scientific community" but the question it is really asking is whether it can trust the enhancement process enough to allow its fruits as evidence. *Id.* at 1027.

221. *See generally id.* at 1024 (focusing on the general acceptability of the enhancement process, rather than whether the picture actually depicted what it purported to depict).

222. *Id.* at 1028.

223. *Id.* Though the option was available to it, there is nothing in the record to indicate that the court took measures to ensure that the photographs matched the sheet. *Id.* Presumably this is something the opposing party would have done.

proceeding.[224] Most courts, by saying nothing, are in essence adopting the standard enunciated in *Almond v. State*, where the appellant, who had been convicted of malicious murder and the sale of cocaine, objected to the use of digital photographs as evidence.[225] The court held that for purposes of identification, digital photographs should be treated no differently than any other photograph.[226] To bolster its approach, the court indicated that it knew of no authority that suggested that digital photographs should be admitted on grounds any different than that of traditional photographs.[227] This is precisely why some sort of standard needs to be adopted for the authentication of digital images: there is no authority on the subject.

d. State v. Swinton

Perhaps the most significant of common-law approaches discussed thus far, *State v. Swinton*, 847 A.2d 921 (Conn. 2004) set a new standard for the authentication of digitally created or altered evidence.[228] Although the decision is only binding in the state of Connecticut, it could prove very useful as a guide for other courts as they confront the issues inherent in the authentication of digitally created evidence, particularly digital images.[229]

The defendant, Alfred Swinton, was convicted for the murder of a twenty-eight-year-old woman and sentenced to sixty years in prison.[230] In the course of the crime, among other things, he partially undressed her,[231] bit her breasts,[232] and strangled her to death.[233] Chief among the evidence used to convict him were photographs of bite marks on the victim's breasts[234] and molds taken of the defendant's teeth.[235] There was also a significant amount of corroborating circumstantial evidence that was not the subject of Swinton's appeal.[236]

The prosecution cleaned up the photographs of the bite marks with image-enhancing software called Lucis.[237] Then, images of the defendant's bite pattern (taken from the mold of his teeth) were superimposed over images of the bite marks using Adobe Photoshop.[238] It was these two actions of the prosecutor, the use of Lucis to enhance and the use of Adobe Photoshop to

224. Levy-Sachs & Sullivan, *supra* note 44, at 1.
225. Almond v. State, 553 S.E.2d 803, 803–05 (Ga. 2001).
226. *Id.* at 805 (indicating that the procedure for admitting digital pictures is neither different than nor heightened over the procedure for admitting traditional photos).
227. *Id.*
228. Catherine Guthrie & Brittan Mitchell, *The Swinton Six: The Impact of* State v. Swinton *on the Authentication of Digital Images*, 36 STETSON L. REV. 661, 689 (2007).
229. *Id.*
230. State v. Swinton, 847 A.2d 921, 927, 932 (Conn. 2004).
231. *Id.* at 927.
232. *Id.* at 928.
233. *Id.* at 927.
234. *Id.* at 932.
235. *Id.* at 928.
236. *Id.* at 928–32.
237. *Id.* at 934.
238. *Id.* at 946.

overlay, that were the basis of Swinton's appeal: he objected on the grounds that the prosecution had an inadequate foundation, concluding that the images were therefore improperly admitted.[239]

To analyze whether Swinton's claims had merit, the court adopted a six-factor test for the authentication of evidence generated or enhanced by a computer:[240]

> (1) the computer equipment is accepted in the field as standard and competent and was in good working order, (2) qualified computer operators were employed, (3) proper procedures were followed in connection with the input and output of information, (4) a reliable software program was utilized, (5) the equipment was programmed and operated correctly, and (6) the exhibit is properly identified as the output in question.[241]

In applying these factors, the court determined that the Lucis-enhanced photographs had been admitted on an adequate foundation and were therefore properly authenticated.[242] Conversely, the court found that the overlays created by Adobe Photoshop had not been properly authenticated because five of the six factors were not met, including whether the use of Adobe Photoshop was accepted as standard and competent among odontologists to create dental overlays.[243]

B. The Problem with the Common-Law Approaches

Except in the rare case where the subject of the photograph is available for comparison to the photograph presented to the court, each of these approaches relies on the testimony of a witness. Courts of yesteryear had protections against perjury, at least insofar as photographic evidence was concerned, because photographic trickery was much easier to detect.[244] Today, courts do not enjoy this protection.[245] Much of the burden of ensuring that evidence is authentic falls not on the court itself but on the attorney cross-examining a witness.[246] However when a defense attorney disputes expert testimony, he is most likely going to lose the challenge.[247] Indeed, prosecutors have a success rate of ninety-two and ninety-eight percent when fending off challenges of their experts in trial and appellate courts, respectively.[248] The meager protections courts have against falsely authenticated photographs are not enough.

---

239. *Id.* at 932.

240. *Id.* at 942.

241. *Id.* (citing CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, EVIDENCE: PRACTICE UNDER THE RULES § 9.16 (2d ed. 1999)).

242. *Id.* at 944.

243. *Id.* at 952.

244. Bianchini & Bass, *supra* note 17, at 309–10.

245. *See supra* text accompanying footnotes 90–96 (describing why it is harder to detect digital photographic trickery than analog photographic trickery).

246. Paul, *The "Authenticity Crisis," supra* note 13, at 47.

247. DeCoux, *supra* note 186, at 132.

248. *Id.*

C. Sundry Approaches to Solving the Digital Dilemma

The various approaches aimed at enhancing the trustworthiness of digital photographs include recent amendments to the Federal Rules of Civil Procedure,[249] implementation of hashing algorithms designed to detect alterations in an image,[250] and the use of self-authenticating cameras.[251]

1. 2006 Amendments Federal Rules of Civil Procedure

A new amendment to the Federal Rules of Civil Procedure took effect in December 2006 that requires the production of "electronically stored information."[252] Although not explicitly defined in the amendments, nor the committee notes, electronically stored information includes all information that requires computer hardware and software and is "created, manipulated, communicated, stored, and best utilized in digital form."[253] This would necessarily include digital images, along with their metadata.[254]

a. Electronically Stored Information, Metadata, and Authentication

The current Federal Rules of Civil Procedure empower a party to request electronically stored information in its native format, including its metadata.[255] Metadata is data about data.[256] For a typical document, it includes, *inter alia*, the name of a file, its location on the computer's hard drive, the file extension, dates of creation and modification, and names of users who have permission to open or alter a file.[257] Although metadata is generally not visible to the user, it is not difficult to find.[258] The deeper the levels of metadata sought, the more technically savvy the computer user must be to find it.[259] Additionally, metadata is not visible when the file or document is printed.[260] However, many levels of metadata can inadvertently become visible.[261]

---

249. *See infra* text accompanying notes 252–77 (discussing the 2006 amendments to the Federal Rules of Civil Procedure).

250. *See infra* text accompanying notes 278–85 (discussing hashing).

251. *See infra* text accompanying notes 286–97 (discussing self-authenticating cameras).

252. FED. R. CIV. P. 26(a)(1)(A)(ii); FED. R. CIV. P. 34(a).

253. Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. OF TECH. & INTELL. PROP. 171¶ 9 (2006), *available at* http://www.law.northwestern.edu/journals/njtip/v4/n2/3.

254. Joe Kashi, *Authenticating Digital Photographs as Evidence: A Practice Approach to Using JPEG Metadata*, L. PRAC. TODAY, June 2006, http://www.abanet.org/lpm/lpt/articles/tch06061.shtml.

255. Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 547–48 (D. Md. 2007).

256. *Case Blurb: Lorraine; Authenticating ESI Under FRE 901(b)(4) by Examining Metadata*, Sept. 18, 2007, http://postprocess.wordpress.com/2007/09/18/case-blurb-lorraine-authenticating-esi-under-fre-901b4-by-examining-metadata/ [hereinafter *Authenticating ESI*].

257. *Id.*

258. CATHERINE SANDERS REACH, DIRECTOR, LEGAL TECHNOLOGY RESOURCE CENTER AMERICAN BAR ASSOCIATION, DANGEROUS CURVES AHEAD: THE CROSSROADS OF ETHICS AND TECHNOLOGY 5 (2008), http://www.abanet.org/tech/ltrc/presentations/arkbarethicstech.pdf.

259. *Authenticating ESI*, *supra* note 256.

260. *Id.*

261. *See* Robert L. Kelly, *The Tech Side of E-Discovery: Understanding Electronically Stored Information*, BUS. L. TODAY, Sept.-Oct. 2007, *available at* http://www.abanet.org/buslaw/blt/2007-09-

The metadata of an image that a digital camera records can include the dimensions of the image, the file size and location, the make and model of the camera used to take the photograph, the focal length and ratio, exposure time, and the dates the photo was taken, last modified, and last opened.[262] Some cameras even have internal GPS chips that record the precise location the picture was taken.[263]

This new amendment to the Federal Rules of Civil Procedure has led some to postulate that the discovery rules regarding electronically stored information, including metadata, solves the problem of authenticating digital images.[264] Although metadata may be a useful tool for the authentication of digital images,[265] it by no means solves the problem, as illustrated below.

b. Disadvantages of Using Metadata to Authenticate

Using metadata as a means to guarantee that only genuinely authentic digital images are used as evidence is a proposition as problematic as it is fraught with misunderstanding. As useful as metadata can be, the danger of impetuously relying on it can be summed up in one sentence: metadata is not immutable.

There are a number of ways metadata can be altered—some of them inadvertent.[266] For example, the date the picture was taken, which could very conceivably play an important role in a case, is not necessarily going to be accurately reflected by the creation date in the metadata.[267] Various conditions must be met to ensure that the date is not inadvertently changed: first, the date on the camera must have been set correctly in the first place.[268] It would also have to be a camera that saves the date between battery charges and changes.[269] There are other difficulties as well. For example, in some cases, once the image is downloaded from a camera to a computer's hard drive, the

10/kelly.shtml (discussing metadata and when it is visible or invisible).

262. Electronic Discovery and Evidence: Digital Camera Metadata and GPS, http://arkfeld.blogs.com/ede/2004/12/digital_camera_.html (last visited Mar. 5, 2009).

263. Paul Miller, *GeoPic II Geotags your NikonSshots, Saves on Battery*, ENGADGET, Oct. 9, 2007, http://www.engadget.com/2007/10/09/geopic-ii-geotags-your-nikon-shots-saves-on-battery/.

264. *See, e.g.*, Kashi, *supra* note 154, at 14 ("[T]he metadata stored in any JPEG or RAW photographic file may help you authenticate that photograph and contradict the popular view that digital photographs can be easily and undetectably altered.").

265. *See* Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, B.U. J. SCI. & TECH. L., Winter 2007, at 1, 11 (describing the numerous benefits of metadata).

266. Kelly, *supra* note 261.

267. *See generally* Setting up a New Camera, http://h10025.www1.hp.com/ewfrf/wc/document?docname=c01056255&lc=en&cc=us&product=340344&dlc=en (last visited Feb. 13, 2009) (noting that the camera owner may set the date and time on the camera).

268. *Id.*

269. If the backup battery loses its charge, the camera will not remember the date when the primary battery is removed to be recharged, and the date must be reset manually. *See, e.g.*, Canon Professional Network, Batteries: Care of Batteries, http://cpn.canon-europe.com/content/infobank/batteries/care_of_batteries.do (last visited Mar. 5, 2009) ("[w]hen the battery runs down, you will need to replace it and then reset the date and time. If when you remove the main battery, the correct date and time is lost, you know it is also time to replace the back-up battery."); *and* Kodak KD40 Camera Manual, http://www.kodak.com/global/en/consumer/products/cameras/manuals/kd40Manual.shtml (last visited Mar.5, 2009) ("NOTE: After you replace the [backup] battery, you will need to reset the date and time.").

creation date visible in a file browser like Windows Explorer or Mac Finder changes to reflect the date the file was created on the computer, not the date the picture was taken.[270] Merely opening[271] or resaving[272] the image file also changes dates in the metadata of the image. These are all ways that the metadata is changed inadvertently.

Metadata can also very easily be purposefully changed. A free Microsoft Windows photo add-on makes it very easy to deliberately change metadata.[273] There are also programs that can completely remove, or scrub, a file's metadata.[274] If someone who is offering photographic evidence has an interest in the outcome of the case, and is willing to perjure herself, she can alter the contents of the photograph. This is particularly true where the current system assumes an image in evidence has not been even subtly doctored.[275]

Although it would be a sweeping error to rely on the Federal Rules of Civil Procedure to protect against photographs with undisclosed alterations, the biggest problem is not that metadata is not a sufficient safeguard, but that the Federal Rules of Civil Procedure only apply to *civil* suits in *federal* court.[276] Although state courts often have rules modeled from the federal rules,[277] this leaves state and federal criminal courts without even the meager protection offered by metadata.

2. Hashing

Hashing is a way to authenticate all manner of digital files and is widely used in both civil and criminal courts.[278] Hashing is an encryption algorithm that takes any kind of digital file and produces an alphanumeric value, called the "hash value," unique to that file.[279] If the same file, or an identical copy of that file, is run through the algorithm, the same hash value will result every time.[280] If even one comma is removed from a thousand-page document, the entire hash value will change.[281]

---

270. *See* Mac OS X Hints, http://www.macosxhints.com/article.php?story=20070104072657423 (explaining how to change a file's creation date to match the date the photo was taken) (last visited Mar. 5, 2009).

271. *See* Withers, *supra* note 253, ¶ 55 ("The simple act of opening a file on a computer changes the information . . . of that file's metadata . . . .").

272. *See generally* Picmeta Systems, Picture Information Extractor, http://www.picmeta.com/products/picture-information-extractor.htm (last visited Mar. 5, 2009) (noting that the program allows an individual to change the date or time in an image).

273. Microsoft Professional Photography: Microsoft Pro Photo Tools 2, http://www.microsoft.com/windowsxp/using/digitalphotography/prophoto/photoinfo.aspx (last visited Mar. 5, 2009).

274. REACH, *supra* note 258, at 12.

275. Paul, *Fabrication of Evidence*, *supra* note 12, at B10.

276. Legal Information Institute, Federal Rules of Civil Procedure, http://www.law.cornell.edu/rules/frcp/ (last visited Mar.5, 2009).

277. *Id.*

278. *See* Ralph C. Losey, *Hash: The New Bates Stamp*, J. TECH. L. & POL'Y, June 2007, at 1, 23–29 [hereinafter Losey, *The New Bates Stamp*] (discussing hashing's broad application in e-discovery and investigation).

279. Ralph Losey, *Hash*, E-DISCOVERY TEAM, http://ralphlosey.wordpress.com/computer-hash-5f0266c4c326b9a1ef9e39cb78c352dc/ (last visited Mar. 5, 2009) [hereinafter Losey, *Hash*].

280. Harts, *supra* note 12, at 522.

281. Losey, *Hash*, supra note 279.

Many courts already utilize hash marks or "digital fingerprints" to authenticate digital files.[282] The use of hash algorithms allows digital images and other electronic information to be stored indefinitely in a cryogenic state—frozen in time with a guarantee that any evidence of tampering will be markedly conspicuous and easily provable.[283]

If an original digital image were marked with a hash value at the time it was taken, opposing counsel at trial, or even an authenticating witness, could take the digital image produced for evidence and quickly extract a hash value, compare it to the original, and determine authenticity with certainty.[284]

The only caveat to this procedure is that any image authenticated in this manner must always have its hash value read while the image is still in its original state.[285] If police, lawyers, and other professionals who might anticipate the need to authenticate an image were to implement a hash-mark log of digital images as part of a standard operating procedure, the legitimacy of hash-mark comparisons would be preserved.

3. Self-Authenticating Cameras

There are some cameras whose images self-authenticate.[286] These cameras do so to differing degrees.[287] For example, any camera that stores images in RAW format can produce images that will stand up to even the strictest scrutiny.[288]

The RAW image file format is a read-only format that exists only on cameras.[289] Once the image is opened for viewing or printing on a computer, it loses its RAW status.[290] Using the increasingly available DNG format, a user can take a RAW file, along with a record of any adjustments made in a RAW file processor,[291] and embed them into a single file.[292] This open-source format is ideal for the legal field, where image integrity is paramount.[293] If a party at a trial can offer the image, still on the camera in its RAW format or archived as a DNG file, for comparison to the image being used for evidence,

---

282. *See* Losey, *The New Bates Stamp*, *supra* note 278, at 23–29 (detailing use in both civil and criminal cases).

283. Paul, *The "Authenticity Crisis," supra* note 13, at 49.

284. Losey, *The New Bates Stamp*, *supra* note 278, at 43.

285. If a hash value were provided without some sort of guarantee that it came from the image as taken by the camera, it would have no value. The lawyer or witness comparing the present hash value to the past one would not know at what point in the past the hash value was read and therefore could not be sure that the past hash value was not determined only after the picture had been altered.

286. *See supra* text accompanying notes 290–97 (discussing self-authentication).

287. *Id.*

288. Page, *supra* note 44.

289. *Id.*

290. *Id.*

291. When opening a RAW image in a photo-editing program, the user is offered several enhancement options, like adjusting the color balance or brightness and contrast. Introduction to Camera Raw, http://livedocs.adobe.com/en_US/Photoshop/10.0/help.html?content=WSBD0EDB3C-9472-48d2-A3B1-7C06FABF0A2B.html (last visited Feb. 13, 2009).

292. GEORGE REIS, DIGITAL IMAGE INTEGRITY 5 (2008), http://www.adobe.com/digitalimag/pdfs/phscs2ip_digintegr.pdf.

293. *Id.*

the two could be compared and the photographic exhibit authenticated.[294]

Additionally, at least two cameras utilize something similar to a hash algorithm to trace any changes made to a photo subsequent to its capture.[295] By installing software on both the computer and the camera, Olympus' Image Authentication System can trace any alterations to an image.[296] Similarly, but with the added requirement of a dedicated memory card for use on two of its cameras, Canon's Data Verification Kit will detect changes as small as one bit in a photograph.[297]

Because camera manufacturers are cognizant of a need for image integrity and the traceability of alterations, it is foreseeable that camera makers in the future will produce cameras, such as the aforementioned, that will make the authentication of images in the courtroom a more trustworthy process.

IV. RECOMMENDATION

It may be impractical to impose one strict requirement on attorneys for the authentication of digital photographs. However, because there are a number of ways to guarantee, with the participation of the attorney or police involved, that an image is authentic beyond question, the courts should require that at least one of these reliable methods be employed.

Using cameras with self-authenticating software would accomplish this end. The authenticity of a photograph offered into evidence would be incontrovertible if presented with proof that the image had run through the Image Authentication System or Data Verification Kit.

Alternatively, photos could be authenticated by a hash algorithm, which would serve as proof that the image taken by the camera is identical to the image seen by the court. This could be implemented either by using cameras that assign hash numbers when the pictures are taken, or by using third-party hash programs. Of course, there would also have to be standard operating procedures in place to guarantee that the hash algorithm is never applied to a photograph after it has been altered. For this reason, hash algorithms may be best suited for police departments and other highly regulated and structured entities.

Another alternative would be to have the RAW version of an image available for comparison to the one offered into evidence, or its DNG derivative. RAW photos are already very common and would leave no doubt as to the photo's authenticity.

Although none of these procedures should be universally compelled over another, as different forms of authentication could be implemented in different fields with differing levels of practicality, and any one of them would serve as a virtually foolproof form of authentication; relevant legislative, judicial, and regulatory bodies should require attorneys to prove the authenticity of a

294. Page, *supra* note 44.
295. REIS, *supra* note 292, at 5.
296. *Id.*
297. *Id.*

photograph in some manner. As a consequence, if the police, private investigators, and even civilians, understood that their photographs would be subject to higher scrutiny if offered as evidence, they would take greater pains to ensure their photographs meet muster. The creators of digital cameras would respond, creating more cameras that produce photographs with traceable lineage. Without implementing effective protection against digitally manipulated photographs, the fidelity of the justice system will be continually and critically compromised.

V. CONCLUSION

Using digital photographs as evidence in court is relatively new. Dishonest witnesses, however, are not. To protect against the ease with which dissembling witnesses can facilitate the admission of false evidence, a better method of authenticating images must be adopted. It is widely recognized, and widely ignored, that digital images are easy to create, easy to manipulate, and difficult to authenticate. There are a number of methods, with varying degrees of practicality and reliability that, if employed, would ensure that the photographs used in court to help ascertain the truth would be truthful themselves.

Any time lawyers, police officers, and others routinely involved in lawsuits predict that a photo could potentially be used as evidence, they should assure that their photos can be authenticated. As the law stands today, the court has no way of guaranteeing that one of these methods will be utilized. Only by adopting one or more of these methods will the primary purpose of the courts be achieved: that justice be served.