



A digital fingerprint scanner and an old-fashioned inked fingerprint card.

A cautionary note

about FINGERPRINT ANALYSIS and reliance on DIGITAL TECHNOLOGY

COGENT SYSTEMS

by MICHAEL CHERRY and
EDWARD IMWINKELRIED

Today the public is acutely aware of the importance of forensic science. Our morning papers regularly carry stories about the role of DNA evidence in both convicting the guilty and exonerating the wrongfully convicted. At night, the popular CSI television programs dramatize the role that forensic experts play in criminal investigations.

Although DNA evidence now attracts the greatest attention, for decades fingerprint analysis was the gold standard in forensic analysis. In fingerprint analysis, an examiner compares two images or representations of the friction ridge patterns on fingers. In the past, in criminal cases, one of the two images, often referred to as the “rolled” image, was typically produced when a person was arrested. As part of the booking process, the police rolled the arrestee’s fingertips in ink and then impressed them on a card. The card was subsequently stored in libraries of such cards maintained by local, state, and national government agencies. The data on the cards was classified on the basis of the type of ridge pattern.

The other image, usually termed the “latent,” is typically produced at a crime scene. If the police suspect that

a criminal might have left a fingerprint impression on a particular surface, such as a glass tabletop, they can use techniques such as the application of special powders to visualize the image. When they find an image, they photograph it for comparison

with the images in the library of fingerprint cards.

Again, in the old days, the police used conventional analog cameras and traditional chemical film to take the photographs. If those administering the library could classify the type of skin pattern displayed on the latent, they searched the library for cards of inked images with similar patterns. An examiner then compared the image of the latent to the fingerprint cards with the most similar patterns. Based on that comparison, the examiner might attribute the latent image and the image on a card to the same person. The fingerprint examiner frequently testified about the comparison at trial.

Thus, in the days of yore, living, breathing fingerprint examiners compared the images. Several aspects of that paradigm inspired confidence. To begin with, a human being made a meticulous comparison of the inked and latent impressions. Moreover, that person was working

Although there are advantages to digital fingerprint technology, we must be aware of the limitations.



with the best possible images. Admittedly, no image perfectly captures a person's fingerprint pattern, but some are more complete and therefore more reliable than others. For the most part, today, that paradigm is passe. We will not and should not return to the days of yore; but, as we shall see, we need to be far more aware of the pitfalls lurking in the new paradigm.

Computerized fingerprint analysis

To understand the profound differences between the old paradigm and the new reality, we must focus on two questions: who and what. Who conducts the analysis, and what is being analyzed?

Who conducts the analysis—a human being or a computer? During any given year today, government and business must conduct a huge number of fingerprint comparisons. Unfortunately, there are not enough examiners to conduct or verify even 10 percent of the fingerprint analyses that must be completed annually. Assume hypothetically that you have 1,000 experienced, certified examiners who do nothing but fingerprint analysis. If those examiners conduct 20 comparisons a day for 365 days, they will complete only 7,300,000 analyses per year. That number pales in comparison with the number of analyses that must be conducted.

One government agency alone, Homeland Security's US-Visit, has conducted fingerprint searches for over 40 million individuals since

March 2005. US-Visit conducts these searches in order to determine (1) whether the arrivee on American soil is the same person who earlier cleared the overseas departure customs and (2) whether that person is on the Watch List.

However, US-Visit is only part of the story. The FBI's Integrated Automated Fingerprint Information System (IAFIS) is another important piece of the picture. On a daily basis, approximately 130,000 employment background and criminal checks are completed by using IAFIS and its regional Automated Fingerprint Identification System (AFIS) counterparts.¹ During the course of a year, those checks could total over 40 million comparisons. Given the limited number of examiners in the United States, computers have to be routinely used to conduct the comparisons and determine whether two images should be attributed to the same person.

The FBI's IAFIS computerized fingerprint matcher was originally developed by Lockheed Corporation in the 1990s. In addition, many firms offer combination fingerprint scanning and enhancement systems that are the building blocks of our local and regional AFIS systems.

The U.S. Department of Commerce National Institute of Standards and Technology (NIST) is and has been the primary source for DOJ and Homeland's large scale testing of fingerprint matchers. NIST tests these proprietary matchers for speed and accuracy. The tests have shown instances where the matchers find more minutia matches than a human examiner could. NIST is currently contemplating testing the use of fingerprint matchers with latent fingerprints.

It is conceivable that NIST latent fingerprint testing could reveal that some of the popular matchers that are capable of matching single and multiple fingerprints lack the appropriate algorithms to accurately match

latent (partial) fingerprints. This would present a problem, since fingerprint experts have been using the untested matchers with latent fingerprints to provide them with suspects.

To be sure, in civil settings a computerized match frequently enjoys a major advantage over the analysis in a criminal case. In many criminal cases, the comparison is often between a solitary latent image and a ten-print card. In contrast, in civil cases the comparison is frequently made between two ten-print cards, decreasing the probability of a misidentification. However, even in a given civil case that advantage could be absent. The question thus arises in both civil and criminal cases: In general, does the cost/benefit analysis favor computerizing fingerprint analysis?

A major benefit of computerization is efficiency. Computerization enables the examiner to perform identification tasks that were virtually impossible under the old paradigm. For example, as previously stated, FBI certified matchers can often find more matches than human examiners.

But there is a price, and here is an example. In a recent interview, Thomas Bush III, the Assistant Director of Criminal Justice Information Services at the FBI, conceded that the FBI's system had missed a fingerprint attribution for Jeremy B. Jones on three occasions. Jones was a serial killer who was repeatedly released from custody. Even though the IAFIS library had included images of Jones' fingerprint patterns, the computer system failed to "match" those images to the new images produced each time Jones was re-arrested.

While acknowledging the repeated failures in the Jones case, Mr. Bush noted that "... Integrated Automated Fingerprint Information System [is] more than 98 percent accurate and a vast improvement over manually matching fingerprint cards, a process that used to take 15 to 25 days."² Although the time saving is desirable

1. NISTIR 7242 Summary of April 2005 ANSI/NIST Fingerprint Standard Update Workshop.

2. Shaila Dewan, *F.B.I. Apologizes for Failing to Identify Murder Suspect*, New York Times, May 5, 2005. www.nytimes.com/2005/05/05/national/05suspect.html?pagew.

and the 98 percent figure is impressive if it is true, even the 2 percent error figure is distressing. If a computerized system is involved in 40 million comparisons a year, a “mere” 2 percent error rate converts into 800,000 erroneous conclusions.

It is no surprise that there is a 2 percent error rate. No system, including human comparison, is foolproof, but IAFIS takes shortcuts in order to effect the time saving. For example, even when all 10 fingers of a suspect are available, in the early prescreening step IAFIS analyzes only the index fingers. If the prescreening yields a very low score, a non-match decision is made without analyzing the images of the other fingers.³ As a result, the system can fail to identify the person who is the source of the fingerprint patterns that produced the latent image. The Jeremy Jones debacle may have been caused by this deficiency in the process.

What is analyzed? The *who* question is only part of the problem; another key question is *what* is analyzed. Again, in the days of yore fingerprint examiners worked with the best possible images, such as the original inked exemplars and the original film photographs of the latent crime scene impressions. Today the original inked exemplars are digital, and the latent crime scene impressions could also be digital. The latent crime scene impressions have to be digitized to produce suspects. Once digitized, fingerprints are run through IAFIS or a regional Automated Fingerprint Information System (AFIS).

The law enforcement community is making extensive use of digitized technology in its fingerprint systems. In many cases, if the police succeed in visualizing a latent print at the crime scene, they use a digital camera to preserve the image. And we must never assume that once a person is taken into custody a traditional inked exemplar will be taken. In almost all cases, rather than preparing and preserving an old-fashioned inked fingerprint card, the police now employ digital scanners. The suspect places his or her fingers directly on the

instrument’s screen, and the instrument scans the fingers to produce a digital image that can be printed out later. In subsequent litigation, an inked fingerprint card will be unavailable because one was never created.

Litigants are not the only persons who might mistakenly assume that they are dealing with the best possible images of the fingerprint patterns. If an image has been digitized, it can of course be printed out. Even a fingerprint examiner might conduct an analysis without realizing that he or she was working with a digital image. It is almost impossible to differentiate between traditional inked fingerprint cards and cards produced by the best available printers.⁴

Limitations

Simply stated, the reality is that digital evidence is the new paradigm. But what difference does it make? Although digital photography is in widespread use, it has its limitations. Digitized images are incomplete. Digitized fingerprint impressions included in databases are represented by only 500 by 500 pixels per inch out of a minimum 6,000 by 6,000 pixels.⁵ In contrast, conventional 35 mm black and white forensic film employs at least 6,000 pixels per inch (ppi).

Digital printers and screen displays use interpolation⁶ techniques to approximate the appearance of images with 6,000 by 6,000 pixels. Interpolation is unnecessary when a computer is comparing two images; a computer does not need to “view” an image in order to compare it. In contrast, a human examiner does have to view images to compare them, and that almost always results in interpolated views. Computer experts realize that the final product of digital photography is not a complete, detailed reproduction of a 6,000 by 6,000 image; rather, it is an approximation—nothing less but nothing more.

It is true that database fingerprints of 500 x 500 ppi are thought by some to contain sufficient information to identify each row and valley of a full fingerprint. However, images of latent

fingerprints are frequently captured with more detail such as 1,000 x 1,000. Often latent fingerprints of 1,000 x 1000 are matched against AFIS exemplar fingerprints that are 500 x 500. The detail missing from the 500 x 500 image might be the very detail that establishes that there is no match between the two images. In short, the incomplete detail introduces a possibility of error.

The concern is especially acute when the image is of a narrow finger. The NIST test entitled Pact2002.pdf, using 500 ppi, shows that wider fingers tend to yield more accurate readings than narrower ones.⁷ Wider fingers touch more of the available sensors and leave more data or dots in a 500 ppi image.

To appreciate the significance of the number of dots, consider employing dots to represent numbers. Suppose that we want to represent two numbers, one and seven. If we use only three dots to represent the numbers, the representative images will be ambiguous; it will be difficult to distinguish between the two numbers. Similarly, when we use only 500 dots rather than 6,000 to represent a fingerprint pattern, there can be ambiguity since 6,000 dots are needed to depict a continuous line. By reducing detail, digital systems increase the likelihood that the database will include “matching” images for two or more different individuals.

The Mayfield incident

After the March 2004 terrorist attack on Madrid commuter trains, partial latent prints were discovered and lifted from plastic bags that had contained detonator caps. Spanish law enforcement authorities sent digital images of the latents to the FBI for analysis. According to the FBI statement issued on May 24, 2004, the submitted images were searched through

3. www.mitretrek.org/publications/biometrics/NIST-IQS.pdf.

4. <http://www.fbi.gov/hq/cjisd/iafis/cert.htm>
5. 35 mm forensic film uses approximately 9600 dots per inch to represent a straight line.

6. www.cambridgeincolour.com/tutorials/image-interpolation.htm

7. NISTAPP_Nov02.pdf pages 11,12.

IAFIS. FBI examiners initially concluded that the latents belonged to Brandon Mayfield. However, Mayfield was finally released after Spanish officials conceded that the fingerprints on a bag left near the Madrid bombing site were not his. The FBI later acknowledged its mistake and at first explained that, in part, the misidentification was caused by reliance on “an image of substandard quality,” that is, the digital image.⁸

The later Stacey report stated that

the same color are closer together rather than farther apart.¹¹

“Chain of custody”

The use of digital technology in fingerprint analysis is the microcosm. However, there are broader concerns about reliance on such technology. When we use our personal digital cameras, the technology seems simple in the extreme. However, as in many forensic contexts, computerized analysis of digital fingerprint images

the image is stored, in many cases it must be linked (indexed) to a specific person. Some banking and manufacturing systems automate this step by the use of magnetic ink (MICR) or bar codes, but others do not. Many public sector systems still rely on fallible human beings to perform the indexing. In an Oregon case, authorities had assigned the same electronic fingerprint number to a killer and Miguel Espinoza, a law-abiding, successful restaurateur in Medford. As a result of the error, Mr. Espinoza’s liquor license was revoked; and his business was virtually destroyed.

Storing the scanned image. The indexed, scanned image must be stored for subsequent retrieval. The image might be stored on a standard hard drive. However, computer hard drives are vulnerable to hacking, substituting incorrect information for the correct data. Given the potentially dire consequences of hacking, each data center should be prepared to detect the creation of erroneous information and restore the correct information. However, even some of the largest private companies do not yet have that technical capability. Similarly, many criminal justice data centers currently lack that capability.

Retrieving the stored image. Once stored, images can be retrieved or printed. However, do not assume that the printout is identical to the original image. Most printers operate on a “best fit” principle. They sometimes distort the printout of the image in order to avoid black margins on the printout.

Digital “enhancement”

As the preceding discussion indicates, when a film image undergoes the process of conversion into a digital one, the process may result in alteration of the image. Some of those changes are inadvertent. However, there is also the possibility of deliberate manipulation of the image. Digital enhancement amounts to deliberate manipulation. Image enhancement technology was developed during the late 1960s and early 1970s for NASA.

When a film image undergoes the process of conversion into a digital one, the process may result in alteration of the image.

the quality of the digital image did not contribute to the misattribution.⁹ The panel concluded that the primary causes of the misidentification were the extreme pressure of such a high-profile case and the subtle bias created by the realization that other examiners had already found a match.

Ken Moses, a respected fingerprint expert, and several highly regarded FBI examiners acknowledged their error in misidentifying Brandon Mayfield as the Madrid Bomber. A computer imaging expert might consider a different type of explanation: important details can be lost or distorted when the wrong settings, components, or combinations of both are used to display images. Proper alignment is a complex topic. One example is the number of times in a second that the computer screen is illuminated. The higher the setting the better the image.¹⁰ Inferior displays are a second example. Better quality displays are sharper and more accurate as the phosphor dots or LCD cells of

to identify a culprit is a multi-step process, and there is a possibility of error at every step. For instance, there are potential weaknesses at the following, major steps.

Initially scanning the image into the system. The original latent or exemplar fingerprint image must first be scanned into the computer. This raises an input problem. Even the best modern scanners are not accurate enough to perfectly represent the images they are tasked to scan. (If they were, we all could have Rembrandts in our living rooms.) In roughly 90 percent of the country, LiveScan scanners have replaced inked-paper based fingerprint images. Often there are two available settings on LiveScan: 500 dots per inch (dpi) and 1,000 dpi. If the operator chooses the first setting, the scanned images can omit a critical detail.

Image clean-up (enhancement). Even in this early stage of the conversion process, it is not uncommon to have a computer operator “clean up” the scanned image. The operator may exercise subjective judgment in deciding to delete certain pixels. If there is a later enhancement, the image has been altered not once, but twice.

Indexing the stored image. Before

8. Paul C. Giannelli & Edward J. Imwinkelried, *Scientific Evidence* § 16-4, at 238 (Supp. 2005) (quoting the May 24, 2004 FBI statement).

9. Robert B. Stacey, *Report on the Erroneous Fingerprint Individualization in the Madrid Train Bombing Case*, 54 J. FORENSIC IDENTIFICATION 706 (2004).

10. http://en.wikipedia.org/wiki/Refresh_rate.

11. http://en.wikipedia.org/wiki/Dot_pitch.

Due to the weight and power limitations of spacecraft, it was impractical for NASA to use state-of-the-art cameras on spacecraft. The cameras used produced somewhat degraded photographs.

One type of image enhancement reverses the degradation. Initially, researchers studied the degradation properties of the use of a particular type of photographic equipment to capture a certain type of image: When this type of camera is used to photograph distant objects, what type of degradation can be anticipated? Next, the researchers designed computer software to compensate for the specific type of foreseeable degradation. The software improves the sharpness and image contrast of the photograph by eliminating background patterns and colors.

Before the image on a normal 35 mm photograph can be enhanced, the photographic image must be digitized. Digital images are composed of millions of tiny dots, referred to as "pixels." Based on degradation models developed in research, computer software manipulates the pixels to filter out graininess and improve brightness and contrast. Although image enhancement technology was developed for the space program, the technology now has a wide variety of applications. The technology has been applied in numerous areas, including medicine, physics, meteorology, resource exploration, factory automation, and robotics control. For instance, forensic scientists utilize the technology to enhance photographs of finger and palm prints.

In order to "enhance" the image, the computer uses mathematical transforms, that is, formulae which dictate the alteration of the image. The accuracy of the enhancement depends on the validity of these formulae. If the formula is "junk science," the "enhanced" image will be distorted. A purportedly enhanced image should not be accepted at face value. Rather, the decision maker should demand a showing of the validity of the mathematical transforms programmed into the enhancement software. Unfortu-

nately, if the transforms introduce distortions into the image, the distortions can be terribly difficult to detect. A 500 x 500 fingerprint image consists of 25,000 discrete points. Imagine how difficult it would be to detect that the enhancement program has altered 7 of the 25,000 points.

Conclusion

The focus of this article has been the extensive reliance on computerization and digital technology in fingerprint analysis. Two caveats are necessary. First, we are not proposing that we return to the days of yore. Again, there are significant advantages to computerization.

Secondly, this article is not intended to suggest that all questions about the reliability of a fingerprint analysis evaporate when a live fingerprint examiner conducts an analysis of traditional film images of fingerprint impressions. Some critics have sharply criticized fingerprint analysis on the ground that there are no objective criteria for determining whether two fingerprint impressions "match."¹² In his initial decision in *United States v. Llera Plaza*,¹³ Judge Milton Pollak took that criticism so seriously that he ruled that fingerprint examiners may not opine on the ultimate question of whether both impressions can be attributed to the same person; the experts would be confined to noting points of similarity between the two images. Admittedly, in his later decision, Judge Pollak did an about face; but even in his second opinion he indicated that fingerprint analysis does not qualify as full-fledged science.¹⁴

The point of this article is that a further set of troublesome problems is triggered when a live examiner relies on a less detailed digital image that may also be interpolated instead of a traditional analog photograph. Until recently, society, including the public sector, has readily accepted computerized fingerprint analysis, including reliance on digitized images of fingerprint patterns. This article has demonstrated that greater skepticism is warranted. The bottom-

line is that digital images are simple, incomplete approximations of the images they attempt to capture.

There are hopeful signs that government agencies and courts are beginning to take a more critical attitude toward this technology. To its credit, US-Visit is leading the way. US-Visit is now using two exemplar fingerprints as well as a photograph to verify the identity of arrivees in the United States; and in close cases, it is having human examiners check the identification. In the near future, the agency may further upgrade its system to require a match of all 10 fingerprint patterns. For their part, some courts are demanding more persuasive showings of the reliability of digital evidence. Perhaps coincidentally, in May 2004—the very same month as the Mayfield incident—the Connecticut Supreme Court announced that in the future Connecticut courts would insist on a more extensive evidentiary foundation as a condition for accepting digital images.¹⁵ ❧

MICHAEL CHERRY,

president of Cherry Biometrics, designs identification systems. He is Vice Chair, Digital Technology Committee, National Association of Criminal Defense Lawyers (NACDL). (mcherry@cherrybiometrics.com)

EDWARD IMWINKELRIED

is the Edward L. Barrett, Jr. Professor at the University of California, Davis, School of Law. (ejimwinkelried@law.ucdavis.edu)

Editor's note: The authors would like to thank Jack King for reviewing the article. Pictures can be viewed at www.cherrybiometrics.com/Images.html

12. Robert Epstein, *Fingerprints Meet Daubert: The Myth of Fingerprint "Science" Is Revealed*, 75 S. CAL. L. REV. 605 (2002).

13. 179 F.Supp.2d 492 (E.D.Pa. 2002).

14. 188 F.Supp. 549 (E.D.Pa. 2002).

15. *State v. Swinton*, 268 Conn. 781, 847 A.2d 921 (2004); Reni Gertner, *Computer-Enhanced Evidence Requires Detailed Foundation*, *Lawyers Weekly USA*, June 7, 2004, at 1, 16.