Digitized prints can point finger at innocent

Mon Jan 3, 2005 9:40 AM ET

By Flynn McRoberts and Steve Mills Tribune staff reporters

Deep inside a sprawling complex tucked in the hills of this Appalachian town, a room full of supercomputers attempts to sift America's guilty from its innocent.

This is where the FBI (news - web sites) keeps its vast database of fingerprints, allowing examiners to conduct criminal checks from computer screens in less than 30 minutes--something that previously took them weeks as they rummaged through 2,100 file cabinets stuffed with inked print cards.

But the same digital technology that has allowed the FBI to speed such checks so dramatically over the last few years has created the risk of accusing people who are innocent, the Tribune has found.

Across the country, police departments and crime labs are submitting fingerprints for comparisons and for entry into databases, using digital images that may be missing crucial details or may have been manipulated without the FBI knowing it.

Not unlike a picture from a typical digital camera, a digital fingerprint provides less complete detail than a traditional photographic image. That matters little with pictures from the family vacation. But when the digital image is of a fingerprint, the lack of precision raises the specter of false identifications in criminal cases.

"There's a risk that not only would they exclude someone incorrectly--we have the potential to identify someone incorrectly," said David Grieve, a prominent fingerprint expert who is the latent prints training coordinator for the Illinois State Police crime lab system.

An FBI-sponsored group of fingerprint examiners was concerned enough about the quality of digital images that in 2001 it recommended doubling their resolution. Three years later, though, the vast majority of police agencies still use equipment with the lower resolution.

Equally troublesome, the most commonly used image-enhancement software, Adobe Photoshop, leaves no record of some of the changes police technicians can perform as they clean up fingerprint images to make them easier to compare.

This seemingly esoteric issue is crucial because it raises questions about a bulwark of the criminal justice system: chain of custody. If authorities cannot prove that a fingerprint is an accurate representation of the original and show exactly how it was handled, its validity can be questioned.

FBI officials recognize the resolution problem but say it leads to overlooking guilty people, not falsely accusing the innocent.

"The risk that we're hearing is that we miss people--because the resolution isn't enough--not that we're identifying people incorrectly," said Jerry Pender, deputy assistant director at the FBI's Clarksburg facility.

Potential for error rising

Such confidence is unwarranted, according to digital-imaging specialists and some leading fingerprint experts. And they say the potential for mistakes is growing inexorably as police departments around the nation switch from old inked cards to digitized computer images.

To do so, technicians scan an inked card into a computer, which converts it into a pattern of 0s and 1s that digitally represent the image, similar to how a fax machine works. And, like a fax machine, the process of digitizing the fingerprint loses considerable amounts of detail.

"It gives examiners the misleading impression that they're getting a better-quality image to examine," said Michael Cherry, an imaging expert who is on the evidentiary committee of the Association for Information and Image Management, a business technology trade group. "These images actually can eliminate fingerprint characteristics that might exclude a suspect."

Measuring the number of cases in which a digital image may have wrongly linked a suspect to a crime scene is difficult. The technology is so new that many defense attorneys do not know to ask if the fingerprint image entered into evidence has been digitized.

"I think it's a very real problem, but it's under the [radar] still," said Mary Defusco, director of training at the Defender Association of Philadelphia, a non-profit group that represents indigent defendants. "We have to get up to speed on it."

One of the nation's first successful challenges to the use of digital fingerprinting in the courtroom came in 2003 in Broward County, Fla.

The only physical evidence linking Victor Reyes to the murder of Henry Guzman was a partial palm print--an intriguing trace of evidence found on duct tape used to wrap the body in a peach-colored comforter.

A forensic analyst with the Broward County Sheriff's Office used a software program known as MoreHits along with Adobe Photoshop to darken certain areas and lighten others--a process called "dodge and burn," which has long been used in traditional photography.

Reyes' attorney, Barbara Heyer, argued that such digital enhancements were inappropriate manipulations of the evidence. "It just hasn't gotten to the point of reliability," Heyer said.

Jurors acquitted Reyes, largely because of sloppy handling of the evidence by police. But they also were troubled by the digital fingerprinting technology used in the case. The jury foreman, Richard Morris, who writes computer-imaging software for a living, said in a recent interview that he and his fellow jurors had significant concerns about it.

No record of image changes

"The makers of the [Adobe] software dropped the ball in not providing a digital record of every action applied to the image," Morris said. He said he would like to see lab analysts or police personnel use software that automatically would log any changes so other examiners could determine later whether the digital print had been altered inappropriately.

Ten years ago, only a handful of major police departments used digital fingerprinting. Today, more than 80 percent of the prints submitted to the FBI's Clarksburg facility are digital.

Along with the digital technology has come inexpensive software that allows personnel at many police stations to enhance the prints at their desks. One of the most widely used digital-print software programs, MoreHits, claims about 150 clients among local, state, federal and foreign law-enforcement agencies.

The creators of these explosively popular tools also recognize the potential problems.

"It's like a hammer. It's not evil unless someone who is evil picks it up and uses it," said Erik Berg, a forensic expert with the Police Department in Tacoma, Wash., who developed MoreHits.

Human element crucial

Defenders of the technology contend that concerns about it are overstated because computers only spit out a list of potential matches; typically, human fingerprint examiners at the FBI's lab and at state crime labs make the final matches introduced in court.

"The benefits to law enforcement with digital fingerprints are incalculable in terms of speed of identification and exoneration of the innocent," said Joseph Bonino, former chairman of the FBI's advisory policy board for the Criminal Justice Information Services division in Clarksburg. "They provide a high degree of accuracy, assuming your human examiners are properly trained."

Trust in that safeguard took a major hit last spring when the FBI falsely linked an Oregon lawyer, Brandon Mayfield, to terrorist bombings at Madrid train stations.

When Spanish authorities connected the Madrid print to an Algerian man, the FBI had to admit it erred.

The bureau initially blamed the quality of a digital fingerprint image forwarded from the Spanish National Police. An international panel of experts later concluded that the digital image was fine; instead, the panel found, several veteran FBI examiners had missed "easily observed" details that excluded Mayfield.

Asked last month about the questions involving digital prints, the FBI issued a statement saying it would not comment further until eight teams of forensic scientists--appointed after the Mayfield case unraveled--finish "methodically inspecting every aspect of the latent fingerprint process, which includes the examination of digital images."

The sleek computer equipment inside the bureau's facility in Clarksburg cannot negate this disturbing fact: The FBI does not know if a police agency has altered any of the thousands of new fingerprint images added every day to its database, which now has 48 million sets of prints.

As long as the submissions meet FBI standards on resolution, size and information about the subject, "we wouldn't have any concerns about the quality of images coming into IAFIS," said Steve Fischer, spokesman for the Clarksburg facility, referring to the FBI's Integrated Automated Fingerprint Identification System.

Improprieties possible

But Fischer acknowledged that those standards are not a safeguard against improper manipulation of the images.

"If they were doing something out there," he said, "we wouldn't know about it."

The broader concern, though, remains the quality of the digital images themselves. An FBI-sponsored scientific working group of fingerprint experts cited concerns about the quality of digital images in 2001, when it recommended doubling their resolution, from 500 pixels per inch to 1,000.

But that is only a guideline, and most police departments haven't invested in newer equipment that would upgrade the digital images.

"The quality of the detail . . . in the [lower-resolution] digital image is not sufficient to support a lot of what fingerprint comparisons rely on," said Alan McRoberts, chairman of the working group and editor of the Journal of Forensic Identification.

The roots of using digital images for crime-solving date to the early 1970s, when San Diego police brought a palm print image to the Jet Propulsion Laboratory in Pasadena, Calif., in the hope that scientists could enhance it.

Police had found a bloody palm print on a bedsheet at a murder scene, but the weave of the sheet obscured the print's detail. The lab's scientists managed to separate the print from the bedsheet's weave using a process similar to one employed to enhance photographs taken of the moon and planets.

Since then, the drop in prices for such technology has made it widely available to law enforcement, but critics question whether all police staffers using it fully understand its limitations.

One solution to the problem is simple, according to imaging experts: Have defense attorneys ask the right questions.

Berg, the developer of the MoreHits software, outlined them: "If this is a digital image, has it been enhanced or is this the original capture with no changes to it? If it's been enhanced, I want you to show me what you did and tell me what your training is. And did you go out of your area of expertise to do this?"

If those questions aren't asked, Berg noted, a false identification might not be caught.