

How we can improve the reliability of fingerprint identification

Fingerprints are an excellent source of unique identification. Unfortunately, enormous population growth, worldwide terrorism, and the incorporation of new fingerprint features have occurred without the benefit of badly needed reengineering and recalibration. Our fingerprint matches are no longer foolproof.

by MICHAEL CHERRY and EDWARD IMWINKELRIED

A perfect storm is developing. The reliability of fingerprint identification has declined while the population of fingerprints has exploded. Who is going to tell prospective employees that their fingerprints indicate they have a criminal background? Every night an automated process takes place where the fingerprints of approximately 50,000 job applicants are computer analyzed as a part of civil and government pre-employment investigations. Unfortunately, the FBI systems performing the fingerprint screenings have significant calibration issues that can affect decisions of great importance, both civil and criminal, domestic and international.

Our fingerprint concerns used to be local. Local police departments and agencies maintained their own collections of fingerprints and there was little coordination among those with fingerprint databases. Now, with the threat of international terrorism, the United States faces a global population of dangerous individuals. National security requires a national system that will enable us to correctly identify fingerprints. If analyzed properly, fingerprints can be as accurate as DNA.

The intent of this article is to make several fingerprint identification recommendations to correct our fingerprint problems and reestablish reliability. It describes some old and new concepts regarding fingerprints, briefly traces the evolution of fingerprint examination systems, identifies

the major problems in the current system, and offers recommendations for addressing those problems.

Concepts

Nature appears to be random until you examine it closely. There are approximately six billion individuals in the world. However, most of them have dark hair, dark eyes, are right handed, and share one of two major blood types. If we are to reliably identify criminals and terrorists, we need to rely on their other physical characteristics. Of course, one such characteristic is DNA type. In truth, though, fingerprints offer amazing uniqueness. A full fingerprint is unique and even if the probability of two independent people accidentally having the same fingerprints is only 1,000,000 to 1, then under the same assumptions the probability of the same two people having not one but three matched fingerprints would be 100,000,000,000,000 to 1.

In the late 19th century Sir Francis Galton developed the first system for classifying and identifying fingerprints. He is quoted as having said that “the odds of two individual fingerprints being the same are 1 in 64 billion.” The world population exceeds six billion, and each person has 10 fingerprints. Thus, the world population of fingerprints is now close to 64 billion. If we accept Galton’s assertion, there may well be instances of different persons possessing the same single fingerprint. To ensure reliability, we then need to take into account an individual’s neighboring fingerprints.

Fingerprint identification is predominately based on viewing all the ridges within a fingerprint and then categorizing it into one of three somewhat similar appearing patterns—loops, arches, and whorls. Each of these three patterns can be sub-divided into one of several sub-pat-



Three fingerprint patterns. From left, loop, whorl, and arch.

We would like to thank David Ashbaugh, Forensic Identification Specialist, retired, Royal Canadian Mounted Police, who developed Ridgeology and the quantitative-qualitative friction ridge identification approach, for reviewing our article. Copyright © 2006, Mike Cherry and Ed Imwinkelried all rights reserved

terns. The final step is to find and map the location of small predetermined shapes and contours.

When fingerprints are said to “match,” it means the pattern, sub-pattern, and at least some of the small predetermined shapes and contours present roughly correspond with each other. Since it is very difficult for humans to visualize all of the small predetermined shapes and contours that are present in a fingerprint, a rigorous, systematic procedure is required.

In 1918 Dr. Edmond Locard established the first rules as to the minimum number of minutiae necessary for fingerprint identification. He wrote that “if 12 points (Galton Characteristics) were the same between two fingerprints, that match sufficed as a basis for a positive identification.” By definition, the likelihood of two or more people sharing a partial fingerprint has to be very high in a population of 60 billion fingerprints. As our population grows, the criteria (e.g. number of points) needed to establish a match must evolve.

Evolution of fingerprint systems

The American fingerprint system has evolved through several stages, including nationalization, computerization, and digitization. Initially and for many years, inked fingerprint cards were used. The cards were not stored in alphabetical order. Instead, they were sorted into one of several predefined categories specified by the Henry Fingerprint Classification System, e.g., whorl or tented arch. The Henry System used all 10 fingers and their interrelationships in classifying an individual. Each finger was classified by its pattern and sub-pattern. Searches for a match were limited to the appropriate Henry group. Since the number of prints in a given group tended to be small, it was feasible to manually search for a match.

The Henry System not only allowed for manual searches. It also had important corroboration built into it; a crime scene partial fingerprint often

was ruled out when the neighboring partials did not correspond to their expected patterns and sub-patterns.

Over the years, government agencies collected more and more fingerprints. The databases became so large that manual searches became increasingly time-consuming and impractical. In addition, it was clear that many sophisticated offenders did not obligingly limit their criminal activity to a single metropolitan area or state. Coupled with the growing size of the databases, this consideration generated pressure to nationalize and computerize the fingerprint system. By 1946, the F.B.I. had processed 100 million fingerprint cards in manually maintained files; by 1971, that figure had ballooned to 200 million cards.

With the introduction of computer based Automated Fingerprint Information System (AFIS) technology, the files were split into computerized criminal files and manually maintained civil files. Many of the manual files were duplicates; the records actually represented somewhere in the neighborhood of 25 to 30 million criminals, and an unknown number of individuals in the civil files.

Within the last 10 years, however, new shapes and contours have been incorporated into the identification process. They include sweat pores, ridge width, shape, path deviation, and their governance. In addition, we now rely on the FBI’s computer-based paperless Integrated Automated Fingerprint Information System (IAFIS) and the related regional Automated Fingerprint Identification systems instead of manual searches of conventional fingerprint cards. IAFIS is used by law enforcement, border patrol, and many other agencies including latent fingerprint agencies.

It is critical to realize that the now dominant IAFIS computer system does not incorporate the Henry System. We no longer have the reliability inherent in all 10 fingers. However, these computer systems could be modified to support the Henry System, alphabetic indexing,

and individual fingerprint indexing.

The shift away from the Henry System has been a step backward. Regardless of what was said to Judge Milton Pollack regarding fingerprint governance during the two *Daubert* hearings in the famous *Llera Plaza* case, none of the witnesses addressed the question of why the fingerprint system was modified, and the lack of mathematical studies supporting: (1) the decision not to program the Henry Classifications into the new computer systems; and (2) the choice to incorporate pore and ridge measurements into the identification process.¹

Many defense attorneys are so distrustful of fingerprints that they don’t bother to defend against them. They simply state their reasons for disbelieving in fingerprints and hope the trial judge will be open to their distrust. Unfortunately many of their clients might be better served if an attempt was made to dispute their fingerprint identification that was based on the discovery of partial fingerprints. As the Henry Classification System factored in neighboring fingerprints and IAFIS does not, they could seek permission to determine if the correct patterns and sub-patterns are present in the neighboring partial fingerprints that point to their client.

Need for further research

There are approximately 500 million criminal fingerprints in the FBI’s IAFIS Fingerprint Repository. The current world population of fingerprints exceeds 60 billion. The population of fingerprints has increased so dramatically that we can no longer naively assume the reliability of our current fingerprint standards. We

1. In *Llera Plaza*, 188 F.Supp.2d 549 (E.D.Pa. 2002) after initially deciding to bar expert testimony on the ultimate question of whether the fingerprints belonged to the defendant, Judge Pollack ruled that the testimony would be admissible as non-scientific evidence. However, the opinion contains no discussion of the questions raised in this article.

2. See, Edward J. Imwinkelried and Michael Cherry, *The Myth of Fingerprints*, *Champion Magazine*, September-October 2003, at 36; Michael Cherry and Edward Imwinkelried, *A cautionary note about fingerprint analysis and reliance on digital technology*, 89 JUDICATURE 334 (2006).

need to conduct further testing.

That testing could—and should—take the form of data mining. Computer-based analysis that looks for patterns, trends, and associations within the repository can help us identify the best ways to use ridge information, pores, Galton Characteristics, additional sub-patterns, and other structural elements as identifying characteristics. This type of analysis is commonly referred to as data mining. Wikipedia, the free encyclopedia, says the following about data mining “...Although data mining is a relatively new term, the technology is not. Companies for a long time have used powerful computers to sift through volumes of data, such as supermarket scanner data, and produce market research reports...”

Every biometric system must be reevaluated and often recalibrated or retuned when a large number of new participants are added. For example, a person’s hair color might be unique when observing a small number of people. However, the uniqueness of hair color as an identifying characteristic vanishes when we compare millions of people.

Data mining can assist us in determining the best way to work with fingerprint ridges. For instance, we may want to develop an independent fingerprint identification system based solely on fingerprint ridges. We may also want to incorporate several new fingerprint sub-patterns. We might want to substantially increase or decrease the number of Galton Characteristics needed to serve as the basis for an identification. Data mining helps us find the path to these solutions.

Restoring the Henry System

In general, the reform of the fingerprint system should follow where the research, including data mining, leads. However, it seems relatively clear that research will point to the need to reinstitute some version of the Henry System. On a daily basis our automated computer fingerprint systems—without any human intervention—check approximately 130,000 arrest booking, watch-list, criminal

background pre-employment checks, and other go or no-go decisions. Although they are presented as 10 finger “matches,” the corroboration of neighboring fingers found in the Henry Classification System is lacking. For example, the early, prescreening IAFIS step 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.

Given the failure to analyze images of other fingers, the system can fail to identify the person who is the source of the fingerprint patterns that produced the latent image. Jeremy Jones is a recent example of this failure. Jones was an alleged serial killer who killed a woman each time he was released from custody. Even though the IAFIS library 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. Other IAFIS weaknesses can incorrectly match a prospective employee with someone who had a criminal past.²

There appears to be some proprietary Henry-like filters. If they work the government must mandate they be turned on or choose more reliable alternatives, e.g. a two finger match.

One additional, specific problem needs to be addressed. It has been estimated that at least 5 percent of the fingerprints that are in the IAFIS repository are attributable to aliases for individuals who have assumed multiple identities. These aliases are almost never found. As a result, recidivists who are convicted again may receive an undeservedly light sentence because the sentencing judge does not realize the full extent of the defendant’s criminal history.

Recommendations

The Henry 10 Finger Classification System increases reliability by incorporating information from the neighboring fingerprint. It should be reinstated and used whenever possible. In particular, when feasible, it should be employed with partial (latent) fingerprints and with the

daily 130,000 arrest booking, watch-list, employment background, and criminal checks.

In addition, the current fingerprint paradigm needs to be data-mined and then refined. There has been a huge population explosion since the advent of fingerprint analysis; and, to complicate matters, there has been a recent incorporation of new pore and ridge measurements. New empirical research should lead to improved match criteria and give us further confidence in the reliability of match or no-match decisions.

Aliases should be detected and corrected, and use of the Henry System ought to simplify the detection of aliases.

Until the above systemic recommendations are implemented, judges will have to decide on a case by case basis whether a fingerprint opinion is sufficiently reliable to pass muster under *Daubert*. Of course, defense attorneys will have to do their part to help judges make those decisions. For a variety of reasons, many defense attorneys put up little fight against fingerprint evidence. In many cases where the identification rests on partial fingerprints, it is worth putting up that fight. For example, since, unlike the Henry Classification System, IAFIS does not factor in neighboring fingerprints, defense counsel should consider seeking to discover any neighboring prints found at the crime scene. In a given case, the limitations of the existing system can raise grave doubts about the reliability of the match opinion. Given the stakes—not only justice in a particular case but national security itself—we must do better. ☞

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.
(ejimwinkleried@law.ucdavis.edu)