Automated Fingerprint Identification System (AFIS) technology has been proven in law enforcement over the last 25 years, and the use of AFIS technology is rapidly expanding in a number of new applications areas including welfare. However, the rush to capitalize on the benefits of the technology, in advance of appropriate standards and technology validation methods, is likely to result in a widespread failure to achieve the very valuable programmatic expectations over the long term.

For serious large-scale positive-identification applications, no other currently-available biometric technology comes close to fingerprints. Fingerprint identification technologies are:

- **well established**: fingerprint identification has been used in law enforcement applications over the past 100 years, and has become the *de facto* international standard for positive identification of individuals.

- **proven**: AFIS (Automated Fingerprint Identification System) technology has been developed, refined and proven in demanding law enforcement applications over the last two decades.

- **legally accepted**: The legal precedents which have been established in the U.S. court system make fingerprints the only biometric proof of identification which is readily accepted in legal proceedings.

- **mature**: Fingerprint identification technologies are well beyond the R&D stage, as evidenced by the fact that a number of viable manufacturers produce competing products for a wide-spread and well established marketplace. In most other biometrics, the technology is only available from a single vendor, making any large-scale long-term application very risky.

Recent advances in computing and digital imaging technology have led to the introduction of new AFIS methodologies using electronic “live-scan” plain impression fingerprint images as the basis for identification. The proliferation of plain-impression AFIS systems is rapid and accelerating at the state and federal level, in large-scale applications, including welfare, driver’s licensing, border control, immigration and military personnel identification.

These new identification applications are being treated as straightforward applications of AFIS technology. Plain-impression AFIS applications are relatively new, with a few well-publicized success stories and no documented reports of significant problems. All AFIS vendors and several integrators currently offer applications that use plain-impression fingerprinting, which is an effective endorsement of the plain-impression technologies. Furthermore, plain-impression AFIS applications are not nearly as complex as those in law enforcement, and the associated fingerprint scanners are simple and relatively inexpensive. Many, if not most, lab-collected prints “look” better than inked prints.

In fact, however, the new applications of AFIS technology, especially in welfare, are pressing the limits of AFIS capabilities. The new applications of plain-impression fingerprint technology depart from law enforcement applications in the use of radically reduced fingerprint information to minimize capture times and storage requirements, coupled with requirements for unprecedented levels of identification performance.

Consider the following significant differences between the proven AFIS applications in law enforcement and the new plain-impression applications in welfare:

---

1 Plain fingerprint impressions are also sometimes referred to as “plane” or “flat” impressions.
• Law enforcement AFIS applications use “nail-to-nail” rolled fingerprint impressions as the basis for all identification processing. A plain-impression print can be less than 50% of the area of the equivalent rolled print, providing significantly less data for identification processing.

• The proven law enforcement AFIS applications use either 8 or 10 finger images to achieve identification accuracy. Plain-impression AFIS applications only use 1 or 2 finger images. The other 8 fingerprints are not captured, and are not available for backup comparisons.

• AFIS systems were designed to cope with the typical problems of inked fingerprints, such as smearing and over-inking or under-inking. Electronic live-scan images are subject to image distortion, image breakup and other quality problems that are significantly different from the problems experienced with inked fingerprints.

• In law enforcement applications, the AFIS produces a “candidate list” of possible fingerprint matches (usually 10 - 100 records) which are reviewed manually by an expert fingerprint examiner to determine if any of the candidate records is truly a match for the search record. Most new plain-impression applications are fully automatic, and require that a unique match candidate be identified by the system, without manual intervention. In addition, for most welfare applications, very high identification accuracy is required, in terms of both False Positive and False Negative errors.

AFIS accuracy, cost-effectiveness and interoperability is totally dependent on the quality of the fingerprint images. In the vein of the old “garbage in, garbage out” adage, if the quality of the fingerprint images is poor, the AFIS system’s identification performance is certain to be reduced. As such, the plain-impression live-scan fingerprint scanners could well be the single most important element of the new applications. The following considerations suggest the seriousness of the vulnerabilities which can result from fingerprint scanners:

• Electronic fingerprint scanners are known to be subject to one or more types of geometric distortion as well as image breakup and other types of image quality problems, that do not have an analog in inked fingerprinting. These problems may not be correctable using standard AFIS image processing methods and may contribute significantly to reduced identification accuracy, especially in large systems.

• Although an AFIS can be “tuned” to be insensitive to the systemic distortion problems of a particular brand of scanner, the injection of fingerprint images from another scanner with different image accuracy characteristics will degrade the identification performance of the AFIS in an indeterminate manner. At least one major AFIS vendor refuses to implement an operational AFIS system that incorporates fingerprint scanners from multiple manufacturers, as a matter of policy.

• The FBI has reported informally that poor-quality fingerprint images are significantly more susceptible to image degradation and loss of information, when compressed using the FBI’s WSQ compression technique for telecommunications and/or archival storage. WSQ compression is being widely implemented or specified in law enforcement and the new applications.

To ensure system performance, cost effectiveness and interoperability, the electronic plain-impression fingerprint scanners must produce consistently high quality fingerprint images, and must be subjected to rigorous standards of quality control, both in manufacture and in operation.

Recognizing the impact of image quality on all aspects of fingerprint identification, the FBI, in concert with the National Institute of Standards and Technology (NIST), has led the development of fingerprint image quality standards for law enforcement applications. The FBI has published a definitive set of Minimum Image Quality Requirements which is mandatory for the submission of rolled-impression fingerprints to the FBI for law enforcement applications.

There are no formal standards for single-finger image quality measurement or quality control.

---

2 FBI / CJIS Electronic Fingerprint Transmission Specification (CJIS-RS-0010 (V7)), Appendix F.
The rush to capitalize on the benefits of AFIS technology in the new plain-impression fingerprint applications areas, in advance of appropriate standards and technology validation, is already leading to problems. In at least one case, the lack of technical standards has led to the creation of a very large fingerprint database of such poor quality that a large percentage of the fingerprint images reportedly cannot be processed by an AFIS. Furthermore, well-known systemic problems of the data collection apparatus may result in data that is incompatible with corresponding data collected by different systems in neighboring jurisdictions. As a result, systems in neighboring jurisdictions may only be capable of supporting interoperability at significantly reduced levels of identification accuracy.

Although there are no formal standards for single-finger image quality, the FBI image quality standards are believed to be directly applicable to plain-impression live-scan fingerprint images. The FBI Minimum Image Quality Requirements should be cited in every welfare AFIS acquisition specification. But the FBI standards do not go far enough in specifying how a plain-impression live-scan device or system can be tested to show that: (a) it meets image quality requirements during initial acceptance testing of the system; or (b) it continues to meet image quality requirements during months and years of subsequent operational use.

The coordination of federal and state R&D efforts to develop standards and test methodologies, and to solve the problem of interstate and inter-program incompatibilities, has the potential for very considerable cost savings. As such, the federal government has a vested interest, as well as an obligation, to provide technical standards, technology validation methodologies and implementation guidance in the use of plain-impression fingerprint identification systems. Currently, seven federal Departments have some involvement in, and/or responsibility for fingerprint identification applications, and could all contribute to or benefit from the development and promulgation of the needed standards.

However, until a lead agency is designated and federal standards can be developed and turned into useful technical guidance and methods, it is left as a challenge to each individual welfare agency to devise the appropriate acceptance and operational tests to ensure the continued peak performance of their systems.

About the Author

Gordon Dechman is President FingerPrint USA, a small business that provides expert technical consulting in fingerprint identification technologies and applications, and in the specification and acquisition of complex automated information technology systems. For additional information, contact Mr. Dechman directly (telephone: 703-754-0308; e-mail: gdechman@fpusa.com) or visit the FingerPrint USA home page at http://www.fpusa.com.