Special Report

Standards for the Electronic Submission of Fingerprint Cards to the FBI

Peter T. Higgins

Deputy Assistant Director - Engineering
Criminal Justice Information Services Division
FBI

Introduction

As the Federal Bureau of Investigation starts accepting electronically submitted fingerprints for processing and retention there is a need for a related set of standards. Over the past four years the FBI has developed the necessary standards for the exchange of electronic fingerprint data. Local, state and federal users of FBI identification services will need to understand and employ these standards just as they follow the current standards for cards, ink, etc.

Background

Since the 1920s when the FBI started processing fingerprint cards and established a national repository, it has promulgated a series of standards. These standards ensure the completeness, quality, and permanency of these vital records. They range from the format of the criminal (FD-249) and applicant (FD-258) cards to the specific ink, non-ink (chemical), and glue on re-tabs that can be used on the fingerprint cards. With the introduction of live-scan fingerprint devices in the 1980s the FBI developed yet another standard, the "Minimum Image Quality Requirements (MIQR) for Live-Scan, Electronically Produced, Fingerprint Cards".

J. Forensic Ident.
45 (4), 1 995\ 409

Currently, the FBI receives over 1,000 live-scan generated fingerprint cards each work day. The level of live-scan technology that meets the MIQR resulted in an FBI policy that set forth a cautionary notice regarding fingerprint image quality and training [1]. Live-scanned fingerprints lose some of the quality (i.e., information content) necessary for some latent applications in the process of printing by a laser printer. Subsequent to the issuance of the cautionary notice FBI experts further determined that this warning notice is applicable whether the data is printed or displayed on a CRT. This loss of information is reduced when the live-scanned fingerprints are submitted directly via electronic means into Automated Fingerprint Identification Systems and digital repositories.

By 1997, the number of live-scan fingerprint cards submitted to the FBI is projected to grow to over 20,000 per work day. For this reason and to reduce the time for processing fingerprint cards the FBI is moving toward accepting electronic submittal of *virtual fingerprint cards.* A *virtual fingerprint card* is defined as a series of computer-generated data records containing the digital representation of the information found on an inked fingerprint card. A virtual fingerprint card contains both text and fingerprint image data.

It is important to understand that live-scan devices are digital, that is they represent the information in fingerprints as discrete values rather than as continuous shades of grey produced by ink and paper. One should think of a digital clock. It is accurate and precise but typically does not show seconds, just hours and minutes. While the average analogue clock, with hands and a round dial, shows hours, minutes, and seconds as well as the movement of the second hand. One way scientists deal with this lack of information detail in digital clocks is to specify digital clocks that measure and display more precise information. Some of these clocks display time to the thousandth of a second. Similarly, the FBI has developed expanded standards to specify the precision of the digital fingerprints it will accept.

The FBI's plan to allow virtual fingerprint cards to be submitted electronically includes comprehensive guidelines on the required message formats and image quality standards. As a result of the process of developing these new standards, which took four years to complete, the FBI has significantly raised the level of digital imaging quality from that specified in the MIQR. This important improvement goes a long way toward allowing live- and card-scanned prints to meet the needs of

the entire forensic community. The standards have now been established and are available today for use by law enforcement agencies and departments in fingerprint related procurements and in-house software development. This article will describe the new standards and tell you how to use them.

IAFIS

A new fingerprint processing environment will be established at the FBI to deal with virtual fingerprint card processing and retention. This is being done through the development of the Integrated Automated Fingerprint Identification System (IAFIS). IAFIS will provide the FBI's ten print service providers and latent print examiners with new tools and techniques. It will come on-line in 1997 and will be fully operational in 1998. IAFIS will be a paperless work environment that will allow the FBI to provide one day service on fingerprint submittals. For critical submissions, responses will be returned within two hours on the average. This time does not include local and state processing time.

To better serve the criminal justice community prior to IAFIS'S Initial Operating Capability (IOC), the FBI is implementing a pilot project to demonstrate direct, electronic submittal of virtual fingerprint cards from local, state, and Federal test sites. This pilot, which will be operational as early as the summer of 1995, is called the Electronic Fingerprint Image Printing System (EFIPS). Initially, a few test sites will electronically submit virtual fingerprint cards to the FBI. In turn, the FBI will use this information for the laser printing of fingerprint cards at the FBI. Eventually this service will be available to all submitters as a step on the road to IAFIS. This initial phase will eliminate the time currently required for mail delivery and processing. It will also enhance the quality of the printed cards through the use of tight quality controls on the laser printers at the FBI.

In phase II of the EFIPS pilot the text portion of the virtual fingerprint cards will be sent directly into the FBI's computer thus eliminating the rekeying of this data by FBI personnel. Fingerprint cards will still be printed at the FBI for use by CJIS service providers and latent print examiners prior to IAFIS IOC. In fact, the FBI will retain both its current fingerprint card holdings and all cards submitted until well after IAFIS becomes operational. This will allow the FBI to consider the quality of the virtual cards in IAFIS prior to deciding on a plan for the eventual disposition of the paper cards.

Standards

With the exception of the MIQR being phased out, no existing fingerprint card standards will be impacted by the FBI's transition to IAFIS. This will allow those who do not have access to automated systems to continue submitting inked fingerprint cards. However, independent of IAFIS, the FBI is changing the format of the criminal fingerprint card in 1995 to meet evolving law enforcement needs. Starting with the IOC of IAFIS the FBI will accept both virtual fingerprint cards and mailed-in paper fingerprint cards. Any cards arriving via the mail will be scanned by the FBI upon receipt and then processed electronically. Optionally, a local or state identification bureau can scan these cards on an approved card-scan device and then submit them to the FBI electronically in accordance with the message standards outlined below.

ANSI Standard - Record Formats

The new standards for virtual fingerprint cards relate directly to many of the existing standards. The current criminal and applicant card standards have corollaries in the electronic world. "The American National Standard for Information Systems - Data Format for the Interchange of Fingerprint Information" (ANSI Standard ANSVNIST-CSL 1- 1993) describes the record types associated with digital fingerprint transmission between any two fingerprint systems. This standard can be used to standardize the transmission of fingerprints by localities to a state Identification Bureau or from one Identification Bureau to another as well as exchanges with the FBI.

The FBI's "Electronic Fingerprint Transmission Specification" (EFTS) uses these ANSI record types to define the specific messages that correspond to criminal and civil fingerprint submittals to the FBI. The EFTS specifies the content and format of specific fields (e.g., ORI) in each message and their related responses from the FBI. By way of example, a criminal ten print submission consists of 16 records – one type 1 header record, one type 2 descriptor record and fourteen type 4 fingerprint image records.

Within the ANSI Standard there are nine record types specified (see following table). Five of those record types (types 3,4, 5, 6, and 7) are for the transmission of fingerprint images. It is very important to note that of these five types only type 4 records, high-resolution grayscale images (for ten print transactions), and type 7 records, user defined

image data (for latent transactions, palm prints, etc.), will be accepted by the FBI. The other three fingerprint image record types (types 3, 5, and 6) are specified for other fingerprint image transmissions (e.g., interstate exchange of binary fingerprint images) and are not to be used to transmit fingerprints to the FBI.

By the time a virtual fingerprint card is transmitted to the FBI, the message must fully meet both the ANSI and the EFTS standards. Local departments may choose to use other message formats for internal purposes or when communicating to the state identification bureau, as long as the final message sent to the FBI is in the ANSI/EFTS format. If a virtual card arrives in some other format the FBI's computers will not recognize the format and will reject the transaction.

Record Type	Logical Record Contents	Accepted by the FBI?
1	Transaction Information	Yes
2	Descriptive Date	Yes
3	Low-resolution Grayscale Fingerprint Image Data (FID)	No
4	High Resolution Grayscale FID	Yes
5	Low-resolution Binary FID	No
6	High-resolution Binary FID	No
7	User-defined Image Data (e.g., Latent Fingerprint & Palm Prints	Yes*
8	Signature Image Data	No
9	Minutiae Data	Yes**

* The latent fingerprint data formats will be defined by the FBI in 1995

** The minutiae data, if' any, for IAFIS will be defined by the FBI in early 1996

ANSI Standard - Image Quality

The MIQR is being replaced with specifications that cover both card- and live-scan devices. The minimum scan rate in picture elements (pixels) per inch, the pixel depth in bits (i.e., number of bits which determines the number of gray levels possible per pixel), and the acceptable transmission rates are specified in Section 5 of the ANSI Standard. The minimum scan rate for ten-print records for submission to IAFIS and EFIPS is expressed in pixels per inch (PPI or P/in). Scan rates are often expressed in dots per inch or DPI, just another term for

pixels per inch. One term, DPI, comes from the printing industry and the other, PPI, from the computer industry.

The ANSI standard specifies a minimum scanning resolution of 500 pixels per inch (p/in) +/- 5 p/in for ten print submittals. However, the transmission rate is specified as a range from 500 p/in +/- 5 p/in to 520 p/in +/-5 p/in. This allows scanners operating at 600 p/in to be used as long as the transmitted data meets the ANSI Standard. These scan and transmission rates were arrived at by balancing forensic needs, the state of technology, and the cost of implementation. In 1995 the FBI will begin work on upward revisions to these scan and transmission rates for an anticipated 1998 update of the ANSI Standard. IAFIS is being designed to be able to contain images scanned at different data rates. Plans call for the scan and transmission rates for type 7 records (latent prints) to be as high as 1,000 DPI.

EFTS - Image Quality

The other image quality standards are found in the "EFTS's Appendix F', the "IAFIS Image Quality Specification" (IQS). The IQS specifies the data acquisition standards, for the fingerprint portion of the virtual fingerprint card, such as modulation transfer function (MTF) and signal-to-noise ratio. The MTF measures how much of the fingerprint data can be acquired, it reflects the quality of the optics, the scanner detectors, and the analog to digital converters.

The IQS also specifies quality thresholds for display devices (printers and CRTs) for the fingerprint data. Just as it would be foolish to purchase the best color video camera and then play the tapes on an old black & white TV, it would be foolish to scan fingerprint cards with a high quality, grayscale scanner and then print out a working copy on a binary (i.e., black and white only, no shades of gray) laser printer or display it on a low quality CRT.

IQS standards for printers and other display devices are mandatory for the purposes of FBI procurements. They are provided to the rest of the criminal justice community as advice. Obviously, departments are free to print and display fingerprint data as they see fit. However, if they are going to submit virtual fingerprint cards to the FBI for processing and retention then they must comply with all of the relevant image quality standards (e.g., MTF) in the IQS.

Quality Control

Currently the FBI rejects about 2% of the inked criminal cards and about 10% of the inked civil cards submitted as having fingerprints that are illegible. This reflects on poor training and on insufficient quality control at the point where the fingerprints were acquired. Digital technology will not eliminate either problem. Training and quality control are possibly even more important in the digital image world.

While the person taking the fingerprints can see an image on a computer screen they often do not see the printed card since frequently it is printed at another location. The quality of these printed cards reflects both the quality of the digital data acquired and the quality of the laser printer itself. Unless a laser printer is maintained properly any fingerprint cards generated on it from card- or live-scan data could be illegible or in some cases contain artifacts. Submitting the fingerprints electronically to the FBI can eliminate laser printer problems at the federal repository. It can not eliminate the potential image quality problems caused by poor capture techniques.

Using engineering measurements (e.g., geometric accuracy), the IQS ensures that compliant equipment will permit sufficient, accurate digital fingerprint image data to be acquired and preserved as it goes from the acquisition site (e.g., live-scan booking station) to the relevant local, state, and federal fingerprint repositories. However, the IQS only ensures that the equipment is of sufficient quality when purchased, just as the FBI standard for fingerprint card stock ensures it is of sufficient quality when purchased. The IQS assumes that the person operating the equipment is trained and following instructions properly, just as the card specification assumes the person using it knows how to use it properly. Fingerprint image quality is still very dependant on the operators ability to record a good image, whether with a live-scan device or ink. No standard will preclude the wrong finger being scanned or inked. There are certain levels of quality that only the person taking the fingerprints and quality control can ensure.

It must be noted that the accuracy of the fingerprint characteristics and of their inter-relationships being properly captured and reproduced, either on a card or a CRT, is influenced by the stability and maintenance of the devices used. If the hardware, software, and any mechanical components are not maintained within the IQS and other device specific specifications, then significant degradation of the fingerprints may occur, possibly even the introduction of fingerprint artifacts.

It is highly recommended that any agency using live- or card-scan technology implement a thorough quality assurance plan. The FBI has received live-scan fingerprint cards that contain printer generated fingerprint artifacts that constitute actual changes to the fingerprint. In some cases these changes are easily detected while others are nearly impossible. The FBI strongly recommends that the integrity of fingerprints be maintained through robust quality control processes and quality assurance plans at the local, state and Federal levels.

Compression

A new area to be standardized, compression rate, is specified in the FBI's "Wavelet Scalar Quantization (WSQ) Gray-Scale Fingerprint Image Compression Specification". Data is compressed to save time and money in the transmission of digital fingerprint images and in their computer based storage at the FBI's repository. The WSQ compression algorithm was selected for its compatibility with fingerprint data. The compression rate of 15:1 was selected based on a 1994 IAI comparison test of various WSQ compression rates [2].

Each compressed image carries a tag with the compression rate for that image. This will allow the FBI to use a different compression rate in the future if the WSQ algorithm's data base of wavelets is upgraded. IAFIS is designed to contain images compressed by WSQ at different compression rates. In fact, a typical little finger fingerprint block (more white space that can easily be compressed) is likely to be compressed at more than 15:1 while a thumb fingerprint block will be compressed slightly less than 15:1 to maintain uniform image quality.

There are commercial versions of WSQ software available currently and at least one is in use with a live-scan system. The FBI is developing a test methodology for certifying WSQ software solutions as being compliant with the FBI's WSQ Specification. Both vendor and in-house developed WSQ software products can be submitted for certification. By April of 1995 the certification process will be in place.

Electronic fingerprints submitted to the FBI either through EFIPS or IAFIS may not be compressed with any technique other than WSQ. Images can only be compressed once since small amounts of scanner data necessary for compression are lost in the process of compression. Compressed images can be decompressed many times and used over and over as long as the original compressed copy is preserved.

Procurement

When procuring card- or live-scan equipment or software to transmit fingerprint cards to the FBI, departments must be aware of the standards adopted by the FBI. The FBI is prepared to work with any department in the preparation of Requests for Proposals (RFPs). All RFPs should include the ANSI standard for scan and transmission rates, the IQS, and the WSQ Specification as being mandatory. Recall that the message portions of the EFTS can be generated by software systems other than the original scanner so they do not need to be mandated in all procurements.

The FBI has agreed to "grandfather" all installed or on-order live-scan equipment that meets the MIQR. Live- and card-scan equipment ordered after August 31, 1995 must meet the Interim Image Quality Specifications, a sub-set of the EFTS Appendix F, while all equipment ordered after the IAFIS Final Operating Capability, currently planned for the summer of 1998, must meet the full IAFIS IQS. Even grandfathered equipment must produce virtual fingerprint cards that meet the record formats in the ANSI Standard and the EFTS. This message formatting can occur in a process that is separate from the live-scan device. Only WSQ compression may be used. For fingerprint images that only meet the MIQR the compression rate should be 5:1 rather than the 15:1 for normal ten print submittals.

Acknowledgements

The author would like to thank Dennis G. Kurre, Danny W. Greathouse, Stephen B. Meagher, Roy G. Weise, Walter F. Johanningsmeier, Thomas J. Roberts, and Thomas E. Hopper, all of the FBI, for their review of the numerous drafts of this article. Additionally, the author thanks his wife, Kathy, for the fine editing work she always provides.

For further information and copies of the standards contact:

Roy Weise, Unit Chief
Systems Transition Unit
Criminal Justice Information Services Division
Federal Bureau of Investigation
CJIS Satellite 11
500 West Pike Street
Clarksburg, WV 26306

(304)-367-8100 for voice or fax

References

1. Section 1.1 of the MIQR, Cautionary Note - Image Quality: "To date, the specific live-scan equipment configurations accepted for FBI use produce fingerprint cards which are satisfactory for most ID processing needs. However, it should be noted that live-scan images printed on fingerprint cards do not consistently provide all of the ridge information, such as texture, continuity, edges, and pores, needed to conduct some latent fingerprint comparisons. Improvements to the image quality are required for live-scan fingerprint images to provide the ridge information necessary to support all latent fingerprint comparisons.

   "In addition, extensive testing has revealed that operators of all currently accepted live-scan equipment models will certainly require substantially more training to take live-scan fingerprints than to take inked-fingerprints because of the distinctive methods used to record live-scan fingerprints. Otherwise, images produced by live-scan equipment will not provide the exacting fingerprint qualities needed."

2. Polski, J., "President's Message", *Journal of Forensic Identification, 44(3), 1994, pp 297-298.*