Homeland Security
Science and Technology

TechNote

U.S. Department of Homeland Security
SAVER
System Assessment and Validation for Emergency Responders

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions.

Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercial equipment and systems and provides those results along with other relevant equipment information to the emergency response community in an operationally useful form. SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL).

The SAVER Program is supported by a network of technical agents who perform assessment and validation activities. Further, SAVER focuses primarily on two main questions for the emergency responder community: "What equipment is available?" and "How does it perform?"

For more information on this and other technologies, contact the SAVER Program Support Office.

RKB/SAVER Telephone: 877-336-2752
E-mail: saver@dhs.gov
Website: https://www.rkb.us/saver

This SAVER TechNote was prepared by the National Urban Security Technology Laboratory for the SAVER Program.

NUSTL

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not constitute or imply its endorsement, recommendation, or favoring by the U.S. Government. Neither the U.S. Government nor any of its employees make any warranty, expressed or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose for any specific commercial product, process, or service referenced herein.

Fingerprint Processing and Identification Equipment

Fingerprints—the small ridges of skin on the fingertips which may enhance texture perception and grip friction—are unique to each person and have been used in identification for more than 100 years. Identification, the process of comparing a set of prints or a single print to others in a database, is used in many aspects of law enforcement and counterterrorism operations and investigations. Fingerprints may be compared to local and national databases for criminal history or to watch lists for border security. Latent prints from crime scenes are used in forensic investigations. Fingerprints can also be used to identify victims and for access control. Each application involves different processes for fingerprint capture and database searching and matching.

An Automated Fingerprint Identification System (AFIS) uses imaging technology, computers, and software to acquire, store, and search fingerprint data. Regional and state organizations may maintain their own AFIS, while smaller organizations send prints to local or national databases for comparisons. The Federal Bureau of Investigation's (FBI's) Integrated Automatic Fingerprint Identification System (IAFIS) contains over 70 million subjects in a criminal database, and 31 million non-criminal records such as those of U.S. military or federal employees. The IAFIS responds to requests 24 hours a day, usually within 30 minutes.

Components of Fingerprint Identification Systems

Fingerprint Capture

Optical scanner for electronic capture of exemplar prints
Photo courtesy of Homeland Security Investigations

The first step in fingerprint identification is obtaining an image of the prints of interest. Fingerprints deliberately collected from an individual are called exemplar prints, and may include simultaneous four finger images or rolled prints, which capture an image of each fingertip from one side of the fingernail to the other. Exemplar prints have historically been obtained using paper and ink, which must then be optically scanned for database input. Live scanners electronically capture and store a digital image, eliminating paper and ink. Digitized prints are transmitted electronically for AFIS searches. Most current live scanners are based on optical sensors. Emerging technologies include thermal, capacitive, and ultrasound sensors, and some have begun to use a striped pattern projected onto the fingertip to obtain a three-dimensional image.

In contrast to exemplar prints, latent prints are left behind on surfaces from residual sweat, oils, or other substances and may be smudged or incomplete. Latents usually require treatment to make the residue visible before it can be captured with adhesive tape or digital photography.

Minutiae Encoding

The second step in fingerprint identification is to extract the identifiable characteristics to be used in a database search. Fingerprints can be sorted into general classifications by pattern type, such as arch, loop, or whorl, but minute details such as the ridge endings or bifurcations are unique to each individual. Software identifies these minutiae and converts them into a system of numerical values. These minutiae templates are stored and used in searches instead of the whole image to reduce data and time requirements.

Minutiae encoding and searching software typically use proprietary algorithms. For exemplar prints, the coding process can be mostly automated. In contrast, latent print minutiae points identified by software are reviewed and edited by a trained examiner.

Recognition Software

An AFIS search involves the interaction of various databases where the minutiae are stored. Depending on the application, proprietary algorithms search segments of the database. For example, software may search the minutiae of two fingerprints of each subject, such as two index fingers, two thumbs, or a combination of finger and thumb. In other cases it may be necessary to search a database of all ten fingers.

The simplest type of search is an identity verification used for access control or credentialing applications. Another identifier, such as a username, is submitted with a single fingerprint to specify who is attempting the authentication. The submitted fingerprint minutiae are matched against the enrolled template for that individual; this is called a one-to-one (1:1) search.

In another type of search, called a one-to-many (1:N) search, the minutiae of a fingerprint of interest are compared to many in the database; e.g., minutiae from two index fingers may be compared to the database of enrolled index finger prints. Arrest processing is a common application of 1:N searches. If the subject is in the database from a previous arrest, the result is a positive identification and a criminal history report. Subjects not found in the database are enrolled.

Another type of search is that for latent prints. Minutiae from unknown latent prints are compared to the database of minutiae of all ten fingers. The algorithm returns candidates and a numerical score for the likelihood of a match. A trained latent print examiner makes the final identification. Unsolved latents are stored in a database for future searches.

Certifications and Evaluations

A wide variety of fingerprint capture equipment and proprietary matching algorithms are commercially available. Interoperability is critical to the identification process and is achieved through standards and certification. The FBI has established image quality specifications for fingerprint images as well as data compression requirements for storage and transmission. The FBI certifies equipment compatible with the IAFIS, including live scanners, card scanners, and printers. Certified products are listed at https://www.fbibiospecs.org/IAFIS/Default.aspx.

The National Institute of Standards and Technology (NIST) leads developments in automating fingerprint identification and conducts evaluations of hardware and software. Some examples are: *Fast Capture*, an initiative to improve technology to capture 10 rolled-equivalent prints in less than 15 seconds in a portable, rugged system; the *Minutiae Interoperability Exchange (MINEX)*, which tests the use of a standardized minutiae template, rather than entire fingerprint images, for exchange of data between 1:1 matching systems; and the *Fingerprint Vendor Technology Evaluation 2012*, which assesses the performance of 1:N matching algorithms based on proprietary fingerprint templates using a database of millions of fingerprint sets, including live scan and scanned inked cards.

The FBI, NIST, several state and local agencies, and AFIS vendors are working together in an ongoing effort to develop standardized Universal Latent Workstation (ULW) software. Minutiae encoded from latent prints will be interoperable at all levels because they will not be coupled to a single AFIS. Updated ULW software was released in July 2012 and can be requested at https://www.fbibiospecs.org/Latent/LatentPrintServices.aspx.

Standards

Two standards are currently used in FBI certification. The image quality specifications for interoperability with IAFIS for fingerprint scanners and printers are contained in *Appendix F* of *IAFIS-DOC-01078-9.3 Criminal Justice Information Services Electronic Biometric Transmission Specification.* Fingerprint verification using 1:1 matching is the focus of the standard *PIV-071006.*

Development of national and international standards for fingerprint technology is ongoing, and many other standards are available. For example, *ANSI/INCITS 381-2004* specifies data compression for image storage and transmission, and *ANSI/INCITS 378-2009* defines a fingerprint standard minutiae template.