MITRE TECHNICAL REPORT

State of the Art Biometrics Excellence Roadmap

Technology Assessment: Volume 1 (of 3)
Fingerprint, Palm print, Vascular, Standards

October 2008; v1.2

Destini Davis (Standards)
Peter Higgins (Fingerprint)
Peter Kormarinski (Fingerprint)
Joseph Marques (Vascular, Standards, Palm print)
Nicholas Orlans (Editor, Fingerprint)
James Wayman (Editor)

Sponsor:	Scott Swann, Program Manager	**Contract No.:**	J-FBI-07-164
Dept. No.:	G122	**Project No.:**	14008FC09-LA

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

This document was originally published June 2008, and reflects the state-or-the-art as of that date.

This software (or technical data) was produced for the U. S. Government under contract J-FBI-07-164, and is subject to the Rights in Data-General Clause 52.227-14 (JUNE 1987)

© 2008 The MITRE Corporation. All Rights Reserved

MITRE

Executive Summary

This report presents the technology assessment portion of the State of the Art Biometrics Excellence Roadmap (SABER) study which was conducted over a 10 month period in 2007-2008. The study included an extensive survey of biometric technologies, current products, systems, independent performance evaluations, and an overview of select research activities. The MITRE team was provided access to FBI laboratories where discussions with analysts and scientists contributed enormously to understanding the breadth of forensic biometric applications and how they are used. The MITRE team also had support from senior external consultants. The team visited representative federal, state, and local booking environments, a state detention facility, and saw large surveillance systems used for security and gaming. The site visits provided a valuable perspective on the constraints and challenges that must be considered for the FBI to fully realize the Next Generation Identification (NGI) system. The proposed roadmap recognizes FBI's leadership in fingerprint technology as a solid foundation for expansion, and seeks a pragmatic course using cost-effective supporting technologies.

The Daubert Challenge

All commercial and government application developers seek biometric technologies that are accurate and cost effective. However, biometrics and other identification methods used by the FBI for law enforcement purposes are unique; they may be subjected to additional standards and scrutiny based on Daubert criteria. In the US Supreme Court case "*Daubert vs. Merrell Dow Pharmaceuticals* (92-102), 509 U.S. 579 (1993)," the Court suggested criteria for determining if scientific evidence was reliable and hence admissible:

1. Is the evidence based on a testable theory or technique?
2. Has the theory or technique been published and peer reviewed?
3. For a particular technique, does it have a known error rate and standards governing its operational use?
4. Is the underlying science generally accepted within a relevant community [Daubert vs. Merrell, 1993]?

These Daubert criteria apply in all U.S. federal courts and but only in some state courts. However, the FBI should strive to meet the Daubert standards for biometric evidence used in all prosecutions. For this reason, additional scientific development is needed in biometric technologies and for supporting testimony from scientific experts.

The investigative applications of biometrics are not subject to Daubert criteria; therefore, biometrics can be used in investigations, regardless of their scientific development. Between investigation and prosecution lies the area of warrants. The required scientific defensibility of technical methods is not always clear with warrant actions. It is prudent for the FBI to pursue Daubert compliance, and seek to elevate the usability of technical evidence from investigations to warrants and prosecutorial needs.

Fingerprint technology is the most mature biometric modality. With the FBI's leadership role in fingerprint technology, systems, and standards, fingerprints are widely and successfully used for criminal justice. The success of fingerprint technology is clearly the starting point for the State of the Art Biometrics Roadmap. With that in mind, we summarize the current trends and issues below.

Trends and Issues

Other biometric technologies such as face, iris, voice, and handwriting recognition are maturing. If effectively integrated (fused), additional biometric technologies offer promise for improved performance and an expanded application base for searching and identity resolution.

The strong association of fingerprints with criminal justice perhaps initially hampered adaptation in civil sector applications. Nonetheless, fingerprint searches for civil applications have steadily increased.

With the increase in these civil searches has come a preference for faster, less intrusive fingerprint types. As of 2007, "Identification Flats," consisting of right and left impressions of the four fingers and one impression of simultaneous thumbs, are being collected and submitted to the FBI by the State Department and the Department of Homeland Security.

Mobile identification applications have proposed variations to identification flats that use a smaller platen and, hence, only the first two or three fingers. Other implementations of mobile identification have introduced single finger capacitance sensors.

Personal Identity Verification (PIV) applications, per Homeland Security Presidential Directive (HSPD)-12, also use lower information content prints, single-print flat impressions, or template creation only.

Extended features (e.g., pores or incipient ridges) that are understood and frequently used by latent examiners are not reliably extracted and considered by automated fingerprint identification systems (AFIS) when encoding latent prints for searching. Consequently, there is room for improvement in AFIS search accuracy. The National Institute of Standards and Technology (NIST) and the FBI are actively working to define and encourage broader use of extended features.

The January 2008 Memorandum Decision not to accept fingerprint evidence by the Maryland Circuit Court in the MD vs. Rose case was evidence of continuing fall-out from the so-called Mayfield problem. The 2004 Brandon Mayfield case involved the false arrest of Mayfield, an Oregon lawyer, as a result of an incorrect identification of Mayfield's prints to a partial print lifted from evidence in the Madrid bombings. The court's decision should be a warning of potential future problems to recur until a stronger scientific case can be made for results from large-scale searches with partial features (i.e., searches with low probability results or likely to return multiple "close" matches). Paving the way for prosecutorial admissibility of "forensic-grade biometric evidence" must be a high priority.

The greater variation in print quality and formats is also disruptive to current state and federal identification systems. The variations impose a new requirement to process and manage a more heterogeneous spectrum of quality and information content.

With the expanded formats and uses, the computational demand for matching is also increasing. Standard commodity hardware such as blade server farms, multi-core processors, and graphics processing units, in conjunction with parallel processing for image processing and pattern matching, offer promise for a more cost-effective foundation for scalability.

Based on current trends and issues, we suggest the following notional technology timeline for SABER. Additional recommendations occur within respective topic areas of this report.

Recommendations

0-2 years

- (Continue) augmentation of fingerprint systems to include palm prints and the beginning of automated searching of major case prints.
- (Continue) development, analysis, and publication of extended features–features used by human examiners but not equally supported in automated fingerprint identification systems.
- (Continue) collection of latent data sets for development and evaluation of applications with improved automated latent matching accuracy and interoperability.
- (Continue) development of standards to support Mobile Identification (e.g., "light" transactions and template-only transactions).
- Augment the planning, and science and technology support to current modality specific applications within the labs, special applications, and National Backstopping Unit. (Please refer to the Voice, Face, Iris, Handwriting, and DNA sections of this report for additional information. Recommendations for Defensive Biometrics are contained in a separate document.)
- Provide quality assessment tools and other quality feedback mechanisms to state and local submitters and integrators (e.g., an online Web utility and Criminal Justice Information System (CJIS) generated reports to FBI, federal, state, and local AFIS operators and managers). Quality feedback should contain examples and clear remediation steps.
- Conduct off-line analysis for the reconciliation of records (linking or merging duplicate identities); develop working solutions and feedback mechanisms for resolving data integrity issues and inconsistent use of standards.
- Conduct technology evaluations and consider trial use for the automated comparison of scars, marks, and tattoos.

- Provide quantitative methods and application performance requirements for comparisons between biometric data of differing qualities (this is a prerequisite for multi-biometric searching and fusion across different sources).
- Initiate pilot experiments for common collection and searching of additional biometric features along with or in addition to fingerprints.
- Augment performance evaluations to include computation performance, and encourage vendors and research programs to use parallel image processing techniques to better leverage commodity hardware (e.g., blade servers, multi-core processors, graphics processing units, and field programmable field arrays).

2-5 years

- (Continue) collection pilots and searching of additional biometric modalities along with or in addition to fingerprint, for example:
  - Forensic quality face images
  - High-quality open microphone speaker recordings
- Develop integrated tools for human analysts to support visualization, annotation, and comparative measurement–Universal Biometrics Workstation.

5-10 years or beyond

- Combined (cost effective) facial and iris collection, storage, and automatic comparison.
- Supporting sciences for defending Daubert challenges.

Risks

- More searches with low information content images (e.g., single print or certain latent searches) against a larger database of inconsistent image quality and a mix of criminal and non-criminal prints will generate a larger number of similar candidates. This will increase the load on human reviewers and could lead to increased occurrences of "mis-idents."
- Greater variations in print quality and formats impose new requirements to process and manage a more heterogeneous spectrum of quality and information content.
- The success in scaling IAFIS was largely due to FBI's success with developing and maintaining standards for the collection systems based on the FBI Certified Product List and, in turn, the underlying Image Quality specifications. The submission of additional fingerprint types and formats, as well as face and iris

(non-contact) biometric images, add significant complications in assuring system accuracy and interoperability for identification through consistent image quality.

- An open reference architecture for fusion and multi-biometric searching of variable quality data, with interpretable results and known accuracy, does not exist for large transactional systems. A prerequisite for an effective multi-biometric application framework requires both vendor-specific and universal biometric quality metrics for system tuning and calibration. However, vendors often consider their specific biometric quality metrics to be proprietary.

Overarching Research Challenges

- Sustain efforts to address Daubert and Frye criteria for biometric technologies for automated techniques and to support expert witnesses.
- Provide an increased understanding of close matches when latent fingerprint are searched against large databases so that human-examiner techniques, such as Analysis, Comparison, Evaluation, and Verification (ACE-V) can take the expected level of similarity into account.
- Develop vendor-neutral reference tools and techniques to assess the quality of all biometric data so that the FBI can:
    - Ensure performance (accuracy) and interoperability over inconsistent data
    - Generate useful feedback on quality to collectors and submitting agencies
    - Support automated capture of biometrics and “binning” of investigative sources.

Acknowledgments

This report was actively supported by many dedicated individuals and experts within the FBI and the National Institute of Standards and Technology (NIST). The authors wish to acknowledge special thanks to Tom Hopper, Dr. Hiro Nakosone, Richard Vorder Bruegge, and Dr. Nicole Spaun. We also thank Dr. John Butler of NIST for his review and comments. Any errors or omissions are the fault of the authors.

Table of Contents

1 Technology Overview 1-1

1.1 Distinctiveness and Stability 1-3

1.2 Positive Claim and Negative Claim Applications 1-3

1.3 Spoofing 1-4

1.4 Application Scenarios for the FBI 1-4

1.5 Forensics 1-6

2 Fingerprint 2-1

2.1 Introduction 2-1

2.2 Background Observations 2-2

2.3 AFIS Overview 2-4

2.4 Biometric Matching 2-4

2.4.1 Modes of Biometric Matching 2-4

2.4.2 Applications 2-5

2.4.3 System Size 2-6

2.5 AFIS Technology 2-6

2.6 Evolution of Electronic AFIS Input Collection 2-8

2.6.1 Rolled Fingerprints and Sequence Slaps 2-9

2.6.2 Identification Slaps 2-9

2.6.3 Palm prints 2-10

2.6.4 Latent prints 2-11

2.6.5 Less Than Ten Prints 2-12

2.6.5.1 Historical Approach for Tenprint and Latents 2-12

2.6.5.2 Extended Fingerprint Feature Set Approach 2-13

2.6.6 Evolution of Investigative and Prosecutorial Use 2-15

2.7 Simulation and Modeling 2-16

2.7.1 Models of Processing Scalability 2-16

2.7.2 Matcher Performance Scalability 2-16

2.8 AFIS Products and Sources 2-16
2.8.1 Typical Vendor Offerings 2-16
2.9 Technology Sources 2-17
2.9.1 Large AFIS Vendors 2-17
2.9.2 Smaller AFIS Vendors 2-20
2.9.3 Associated Vendors 2-20
2.9.4 Government Products 2-22
2.10 Risks Associated with Foreign Sourcing 2-24
2.11 Standards and Specifications 2-24
2.11.1 Standards 2-25
2.11.2 Specifications 2-26
2.12 Performance Measurements 2-28
2.12.1 Background 2-28
2.12.2 Performance Metrics Vocabulary 2-28
2.12.3 NIST Testing and Performance 2-30
2.12.4 Test Databases 2-35
2.12.5 Test Data Shortfalls 2-36
2.13 Forensic Capabilities 2-36
2.13.1 Interoperability 2-39
2.13.2 Use and Limitations of Latent Prints 2-41
2.13.3 Use and Limitations of Hand/ Palm prints 2-42
2.13.4 Use of Flats or Plain Impressions in Latent Print Searches 2-43
2.13.5 Use of Fingerprints and Other Biometrics in Disasters and Mass Evacuations 2-45
2.14 Vulnerabilities 2-45
2.14.1 Errors Introduced by Equipment or Operator 2-46
2.14.2 Frontal Attack on the System 2-46
2.15 Forces of Change 2-46
2.15.1 Replacement Cycle 2-48
2.15.2 Centralized IT Procurement and Management 2-49

2.15.3 Multimodal Systems 2-50
2.15.4 Fusion 2-52
2.15.5 Summary of AFIS Evolution 2-53
2.16 Technology Opportunities 2-54
2.17 CJIS Technology Gaps and Challenges 2-55
3 Palm print Recognition 3-1
3.1 Background 3-1
3.2 State of the Industry 3-2
3.3 Performance and Standards 3-3
3.4 Simulation and Modeling 3-4
3.5 Forensic Capabilities 3-4
3.6 Privacy 3-4
3.7 Vulnerabilities 3-4
3.7.1 References 3-4
4 Vascular Recognition 4-1
4.1 Technology Background 4-1
4.2 Vascular Imaging 4-1
4.3 Distinctiveness and Stability 4-3
4.4 State of the Industry 4-4
4.4.1 Fujitsu 4-4
4.4.2 Hitachi 4-5
4.4.3 Techsphere 4-6
4.4.4 Others 4-6
4.5 Growth and Markets 4-9
4.6 Performance and Accuracy 4-9
4.7 Match Error Rates 4-10
4.8 Enrollment and Acquisition Error Rates 4-12
4.9 Conclusions 4-12
4.10 Standardization and Interoperability 4-13

4.11 Image Capture Requirements 4-13
4.12 File Format Requirements 4-14
4.13 Vulnerabilities 4-14
4.13.1 Spoofing 4-14
4.14 Future Capabilities 4-16
4.15 CJIS Technology Gaps and Challenges 4-16
4.15.1 References 4-17
5 Standards 5-1
5.1 History and Organizations 5-1
5.2 Applicable Biometrics Standards and Evaluations 5-2
5.2.1 Synopsis of FBI Electronic Biometric Transmission Specification 5-5
5.3 Vulnerabilities 5-8
5.3.1 Recent Exploits 5-9
5.4 Gaps and Recommendations 5-9
6 Other Technologies of Interest 6-1
6.1 Gigapixel Imaging 6-1
6.2 Next Generation Commodity Hardware 6-1
6.3 Super-Resolution Image Reconstruction 6-2
Appendix A Acronyms A-1
Appendix B Glossary B-1
Appendix C References C-1

List of Figures

Figure 1-1. General Biometric System 1-2
Figure 2-1. Minutiae Extraction from Finger Image 2-7
Figure 2-2. Rolled and Plain Impressions on Tenprint Card 2-9
Figure 2-3. Identification Slaps (or Flats) 2-10
Figure 2-4. Identification Slaps with Segmentation Boxes and NFIQ Scores 2-10
Figure 2-5. Palm print 2-11
Figure 2-6. Latent Print with Scale for Calibration 2-11
Figure 2-7. Extended Fingerprint Features 2-14
Figure 2-8. Fingerprint Image Metadata 2-14
Figure 2-10. Example of Latent Print Minutiae Matching 2-42
Figure 2-11. Example of CJIS Major Case Cards 2-43
Figure 2-12. CJIS Forces of Change 2-47
Figure 2-13. Current AFIS 2-48
Figure 2-14. Notional ABIS Structure 2-51
Figure 2-15. Influences on Fingerprint Technology 2-54
Figure 3-1. Palm Structure 3-1
Figure 4-1. Spectral Response of Hemoglobin vs. Water [Sassaroli] 4-2
Figure 4-2. Reflective Palm (Fujitsu) and Transmissive Finger (Hitachi) 4-3
Figure 4-3. Bone Formation in the Hand for Males Ages 2, 6, and 19 4-4
Figure 4-4. Fujitsu PalmSecure Sensors (Fujitsu) 4-5
Figure 4-5. Hitachi Finger Sensors (From Hitachi) 4-5
Figure 4-6. Identica Vascular VP-II Scanner 4-6
Figure 4-7. Japanese Biometric Growth 4-9
Figure 4-8. DET Curve for CESG Study (Vein in Red) 4-12
Figure 4-9. Hand Vein Spoof Acquisition 4-15
Figure 4-10. Spoof for Techsphere (Back of Hand) Vein Scanner 4-15

List of Tables

Table 2-1. Application of Image Types 2-8
Table 2-2. Vendors for Large AFIS Systems 2-18
Table 2-3. Associated Providers 2-21
Table 2-4. Government Products 2-23
Table 2-5. ANSI/NIST Record Types 2-25
Table 2-6. NIST Special Databases 2-35
Table 2-7. Latent Idents (Hopper and LAPD, June 2005) 2-45
Table 3-1. Industry Vendors for Palm print Scanners 3-2
Table 4-1. Other Vascular Vendors and Relationships 4-7
Table 4-2. True and False Accept Rates for Different-Day Samples (IBG and Vendors) 4-10
Table 4-3. ISO/IEC 19794 Image Capture Synopsis 4-13
Table 5-1. Standards Bodies, Role and Scope 5-1
Table 5-2. Summary and Status of Recent Standards 5-3
Table 5-3. Summary of Standards by Modality and Purpose 5-8
Table 5-4. Recommended Standards Roadmap 5-10

1 Technology Overview

This section describes elements common to all biometric technologies and presents the general format for discussing each modality. “Biometrics” is a term that refers to two things: (1) measurable human characteristics, and (2) the associated methods and techniques for automated recognition based on those characteristics. As defined by the National Science and Technology Council (NSTC) glossary, “biometrics are measurable biological (anatomical and physiological) and behavior characteristic that can be used for automated recognition.” Full automation requires that characteristics be digitally recorded and compared to previously stored records with no human intervention, sometimes known as *unsupervised* processing. The results from automated comparisons are a similarity or difference score, a decision response, or a small list of candidate matches. Examples of automated biometric technologies include fingerprint, palm, face, iris, handwriting, and hand vascular matching. Depending on the technology, how it is used, and the criticality of the results, most biometrics technologies used for identification require human examiners to verify results and confirm matches. Full automation over all types of submissions is currently not possible, at least not for systems that require high-accuracy identification with a low incidence of false matches.

The forensic sciences and associated techniques are a companion discipline to biometrics. Forensics that exist as “residual biometrics” are a critical component for investigative and law enforcement uses. Well-established examples of forensic identifiers include deoxyribonucleic acid (DNA) and latent fingerprints. Audio and video recordings and images are important data sources that also may contain biometric signatures. Forensic identification is not an automated process either; in particular, the stages for evidence detection and collection are largely human processes.

The term “biometric mode” has no precise definition within the science of biometric identification. In this section, we will arbitrarily define the points of articulation between modes, usually following historical usage. For example, we will consider fingerprinting and palm printing as different modes, even though palm prints might contain fingerprints and the same sensors might be used for each. We will consider face and iris recognition as distinct modes, even though facial images might contain iris patterns. We will consider visible wavelength facial recognition and facial thermography as different modes, even though the image body part is the same. However, we will consider iris recognition as a single mode, regardless of what wavelengths are involved.

Figure 1.1, used by permission of the American National Standards Institute (ANSI), shows a schematic of a generic biometric system from “Standing Document 11” of the international standards committee on biometrics, ISO/IEC JTC1 SC37.

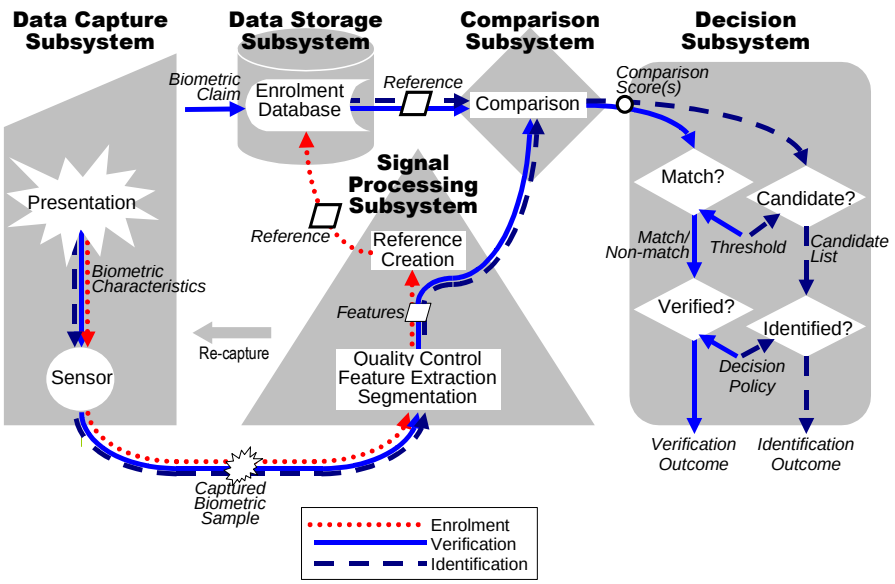


Figure 1-1. General Biometric System[1]

The figure shows five subsystems: data capture, data storage, signal processing, comparison, and decision. Not shown, but implied, are transmission links connecting these subsystems, which are generally modality-specific; in discussing "state of the art" technology, we can decompose each modality into its specific components. Sensor and signal processing technologies will differ by modes. Storage requirements and architectures may also differ, as will pattern comparison algorithms, transmission compression techniques, and decision methods.

In suggesting a path forward for technology development, we can comment on gaps and performance improvement requirements at the subsystems level, but we must put these subsystem requirements in the context of an application to fully appreciate the infrastructure and social/political/legal context into which each technology application fits. Consequently, we must also discuss biometric applications from the integrated system point of view. In this report, we will discuss technical issues arising from large-scale automated searches of fingerprint databases

---

[1] (c) ISO/IEC 2006. This material is reproduced from ISO/IEC 19794-1:2006 with permission of the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO). No part of this material may be copied or reproduced in any form, electronic retrieval system or otherwise or made available on the Internet, a public network, by satellite or otherwise without the prior written consent of the ANSI. Copies of ISO/IEC 19794-1:2006 may be purchased from the ANSI, 25 West 43rd Street, New York, NY 10036, storemanager@ansi.org, (212) 642-4900, <http://webstore.ansi.org <http://webstore.ansi.org/>.

that mix criminal and non-criminal records that have led to problems with forensic admissibility of expert testimony.

1.1 Distinctiveness and Stability

Central to the concept of recognizing people from biological and behavioral characteristics in all applications is the requirement that the measurement of characteristics be repeatable over time for each individual and distinguishable at any time across a population. Figure 1.1 shows a "captured biometric sample" resulting from the presentation of a characteristic to a sensor. The captured biometric sample will be repeatable if the characteristic, presentation, and sensor are stable. In reality, no environmental factors are completely stable over the applications, time scales, and populations of interest to the FBI. Allowances must be made within the signal processing, comparison, and decision subsystems for changes over time and capture conditions in the biometric samples from a single individual. The goal is to minimize "within-class" variations, through the establishment of standards for the presentation and acquisition sensors. Although it is not possible to standardize the characteristics themselves, it will be possible to create mechanisms for dealing with biometric characteristics that are outside population norms.

We require that expected variations between individuals–the intraclass or "between class" variation–be maximized. Biometric systems capable of extracting characteristics with the most variation across individuals will be the most interesting. The decision subsystem will always be at risk for mistaking between-class variation for within-class variation, thus leading to false matches (OIG, Mayfield report) or within-class for between-class variations, thus leading to false non-matches or "misses" (John Paul Chapman). There is no biometric modality for which we have good estimators for how much between-class variation can be expected between possible matches across large databases and how much within-class variation can be expected across long periods of time and various collection conditions. This knowledge gap will impact the forensic admissibility of all biometric measures, even fingerprints [MD vs. Rose, 2008]

1.2 Positive Claim and Negative Claim Applications

Biometric data and systems are fundamentally about recognition, not identity. Biometric data are combined with identity information and contextual information for the purpose of linking them with records and events. The FBI's concern is "Do we recognize this person, or have we seen this person before?" Without validation of all identity documents at the time of collection, biometric systems do not assert "absolute identity".

Some systems are architected with the expectation that the data subject will make the positive claim, "The system will recognize me." Some are architected for a negative claim, "The system will not recognize me." The FBI is interested in both claims and therefore architects systems to address them both. For example, in access control systems, each data subject (enrolled user and impostor) make the positive claim, "The system will recognize me." ISO/IEC documents refer to systems of this type as "positive claim" systems. In watchlist and background check applications, all data subjects (unknown and known) make the claim, "The system will not recognize me." ISO/IEC documents refer to systems of this type as "negative claim" systems. Both systems

confer benefits (such as allowing access) if the claim is true, but these are opposite claims; a positive claim system confers benefits if the data subject is recognized, while a negative claim system confers benefits (or does not deny benefits) if the data subject is not recognized. In the event of a "Type I" mistake (rejecting a true claim), the subject is inconvenienced. We can expect such errors (which are not uncommon to biometric systems) to be quickly reported by the inconvenienced subject. On the other hand, a "Type II" mistake (accepting a false claim), results in a security breach and will generally not be reported.

ISO/IEC JTC1 SC37 Standing Document 2, "Harmonized Vocabulary," defines a false match as "comparison decision of 'match' for a recognition biometric sample and a biometric reference that are from different biometric capture subjects." A false non-match is defined as "comparison decision of 'non-match' for a recognition biometric sample and a biometric reference that are from the same biometric capture subject and of the same biometric characteristic."

In positive claim systems, a Type I error results from a false non-match, while Type II errors result from a false match. In negative claim systems, a Type I error results from a false match, while a Type II error results from a false non-match.

1.3 Spoofing

The matching logic directly impacts all discussion of "spoofing" or fooling biometric systems. Spoofing is the intentional attempt to produce a Type II error resulting in a security breach. For positive claim systems, a Type II error results from a false match. For negative claim systems, a Type II error results from a false non-match. A false match requires impersonation of an enrolled data subject. A false non-match requires alteration or concealment of a biometric characteristic. The biometrics community universally agrees that someone seeking to create a false match through impersonation is called an "impostor." There is no agreed naming convention for someone attempting to produce a false non-match through alteration, obfuscation, or concealment, although the terms "concealer" or "uncooperative" have been suggested. In general, it is much easier to produce a false non-match through alteration, obfuscation, or concealment than it is to produce a false match through impersonation. The techniques required to achieve either false match depend upon the biometric modality; it will be discussed in only general terms in following sections by modality. The intentional spoofing or manipulation of biometrics invalidates the "zero effort imposter" assumption commonly used in performance evaluations. When a dedicated effort is applied toward fooling biometrics systems, the resulting performance can be dramatically different.

1.4 Application Scenarios for the FBI

Understanding how biometric systems are used is a critical part of assessing their maturity, suitability, and utility. There are five high-level application areas where biometric data is collected and used:

1. **Criminal and Forensic Applications:** Criminal applications collect biometric traits for searching at the time of arrest to record the arrest event and determine if a person has a

known criminal history. Biometric checks may also record release events or be used to manage registered offenders. Forensic and latent fingerprint applications seek to link biometric signatures to known persons. Criminal and forensic uses are largely identification applications.

2. **Applicants:** Applicant searching or background checks are done when a person applies for a position of trust. The search determines if the applicant has any criminal history that might disqualify them; applicant searching may also be used to discover fraud and abuse in the form of duplicate requests for entitlements and benefits. These are identification applications.
3. **National Security:** National security applications can vary and are beyond the scope of this document. An example is when non-U.S. citizens apply for a visa to come to the United States; biometric data is collected and searched to determine if they are known or suspected of being unacceptable to enter the US for any security-related reason. This is an identification and investigative application.
4. **Civil Identification:** Civil identification refers to all forms of government issued identification, of which driver's licenses are the most common. In Civil Identification, identity information is *optionally* searched to ensure subjects have not registered under a different identity or had similar identification revoked. This is an identification application.
5. **Physical and Logical Access Control:** These applications involve the authentication of a claimed identity in the context of an access control event. Physical access is typically for entrance to a government building or facility. Logical access is typically authentication to a personal computer, device, or network. Physical access generally is a verification application, or also known as authentication. Some physical security environments may involve one-to-few matching against a look-out or exclusion list.

The above application areas span different uses, environments, and search populations. The boundaries and intersection between civil, criminal, and national security applications are critical policy issues. The same boundaries and intersections affect which biometric sensors can be used and how well they will perform. Criminal and forensic applications span the following collection environments:

Booking Environment: This is a controlled or semi-controlled indoor environment where biometric data and contextual information is collected, typically at distances of 0-2 meters, under the supervision of the arresting officer. Traditional 'booking' calls for 10 rolled fingerprints, face pictures, and recording of scars, marks and tattoos.

Mobile Identification: This is a semi-controlled or uncontrolled, indoor or outdoor environment, typically at distances of 0-2 meters, attended use, and with interactive response times. Mobile fingerprint identification systems use 1, 2, 4 or 8 flat prints. Subsystems for face and iris identification are also commercially available.

Surveillance and Investigations: This includes both indoor and outdoor environments wherever the investigation leads, attended and unattended use, and a range of distances per situational needs. Forensic audio and video and images may be provided from security cameras, identification documents, 911 calls, family photos, and any other source.

1.5 Forensics

Forensics is a companion topic to biometrics; it may not always be embraced by the mainstream biometrics community, perhaps due to continued vertical organization within industry. The lack of full automation and a live subject historically made forensic sciences different from biometrics. Nonetheless, the role of forensics and its critical importance to law enforcement, military, and counter-terrorism is well established in operational practice. We use forensics to mean "residual biometric signatures" or evidence that can be used to link or exclude a subject to an event, events to other events, or identify a previously unknown subject. Audio and visual recordings and images are important forensic sources that contain biometric signatures.

In the U.S. Supreme Court case "*Daubert vs. Merrell Dow Pharmaceuticals* (92-102), 509 U.S. 579 (1993)," the Court suggested criteria for determining if scientific evidence was reliable and hence admissible:

1. Is the evidence based on a testable theory or technique?
2. Has the theory or technique been published and peer reviewed?
3. For a particular technique, does it have a known error rate and standards governing its operational use?
4. Is the underlying science generally accepted within a relevant community [Daubert vs. Merrell, 1993]?

The requirements for establishing Daubert standards for "forensic quality biometrics," are unique to the Departments of Homeland Security and Justice, and fall heavily on Criminal Justice Information Services (CJIS). Frequently, there is a need to defend against Daubert-based and Frye-based criticism from defense attorneys who may use the criteria as a checklist for questioning the veracity of evidence.

2 Fingerprint

2.1 Introduction

Fingerprints have been used in the criminal justice domain for over 100 years. For the last 30 years, automated technology has been brought to bear on fingerprint searching and matching. The FBI funded and employed some of the earliest automation that has come to be called Automated Fingerprint Identification Systems (AFIS).

In the 1990s, the FBI led the way with the introduction of standards and technology to support high volumes of transactions and faster turnaround. The system integrated computerized criminal history records management with AFIS technology. The system is called the Integrated Automated Fingerprint Identification System (IAFIS).

Changes in service demands, due to post 9-11 federal laws and numerous state laws associated with increased mandatory background checks, have started to overwhelm the IAFIS capacity. Also, the FBI is faced with a demand for terrorist fingerprint checks against Known and Suspected Terrorists (KST) lists, requiring responses in seconds rather than minutes. These increased demands for more and more rapid searches have led the FBI to develop a program to refresh and upgrade IAFIS. The upgrades are intended to provide more service, more accurately, with continued high availability, using the same skilled service providers, even in the face of a higher workload. This new program, Next Generation Identification (NGI) is very well-timed, and should enable the FBI to take advantage of new technologies. Some technology trends that will enable new NGI capabilities are:

New image processing algorithms developed specifically for fingerprints have produced major improvements in feature extraction with low-quality images. The improved features combined with advancements in matching algorithms have produced AFIS ten print accuracy above 99.9 percent (excluding any filtering and sequence errors).

Virtualization of servers can simplify redundancy and improves availability in large systems.

Standard hardware, such as blade servers, along with advancements in parallel algorithms will provide a cost-effective foundation for scalability. Commodity image processing hardware such as Graphics Processing Units (GPUs) and multi-core processors can augment general purpose processors with low-cost vector processing capabilities.

The industry transition to Service Oriented Architecture (SOA) promises improvements in flexibility as business requirements evolve over time.

Multi-modal Biometrics affords more flexibility in data submittal, and the capability of searching across modalities enables new applications.

-

Current conditions offer a unique opportunity for the FBI to expand its leadership in the area of identification, particularly opportunities that use fingerprints as the primary or initial search biometric and identity anchor.

2.2 Background Observations

Looking back at the mid-1990s and the impact of the 1994 IAFIS A-109 funding of three of the four major AFIS Vendors (through their associated System Integrators), we see some unintended outcomes. The three funded vendors were able to advance their technology through R&D funded, in part, by the A-109 contracts. Several years later, in NIST's Fingerprint Vendor Technology Evaluation 2003 (FpVTE), these three companies were identified as the three Tier 1 vendors, based on matching performance in non-forensic scenarios. The fourth major vendor, whose system integrator partner was not awarded a contract, sold substantially more systems during the period when the three funded companies focused on IAFIS. Today, all four are much closer in (non-forensic) matching performance than in the FpVTE timeframe. In addition, another company has entered the market. As the FBI's NGI trade studies and performance tests start in 2008, the question remains if there will be another set of unanticipated consequences across the market.

Over the past 20 years, the Information Technology (IT) market has moved from mainframes through mini-computers to networked servers and workstations. The AFIS industry has followed this trend. But, as the size of the repositories grows, industry might follow the latest IT movement back to virtual machines running on new technology mainframes and blade farms for ultra-large data applications with high transaction rates. While there is healthy movement toward Mobile ID devices and distributed processing, the ultra-large repository/high transaction rate central sites that run virtual systems for better performance, availability, and flexibility should not be ignored or assumed to continue to fit the server/workstation model.

In 1999, the shortcomings of having two disparate AFIS systems in the U.S. government (i.e., IAFIS developed for and used by the FBI and law enforcement community, and IDENT, developed for and used by the Department of Homeland Security) became a critical liability and tragically brought to public attention in the case of Rafael Resendez-Ramirez, AKA the "railway killer." In 1999, Rafael Resendez-Ramirez was apprehended by the Border Patrol and released into Mexico, despite the fact he was wanted for murder (information discoverable with an IAFIS search). Because IAFIS and IDENT were not integrated, Border Patrol did not learn of the outstanding warrant for his arrest. Following his return to Mexico, he reentered the U.S. and murdered four individuals.[2] Since then, the two systems have shared more data and, with the advent of NGI, they will share data and searches, interoperating in the public interest.

In 2003, the Department of Defense (DoD) Automated Biometric Identification System (DoD ABIS) sought to extend their AFIS with collection systems that store and match fingerprint, face

[2] FBI FY 2008 Authorization and Budget request to Congress, page 4-157.

and iris modalities. The DoD ABIS environment uses the FBI's Universal Latent Workstation (ULW) software on their workstations for all their latent fingerprint searches against their own system and IAFIS. The 2003 DoD ABIS system, modeled after FBI IAFIS, was a single modality system (fingerprint only) with the goal of expanding to additional modalities. If successful, the DoD Next Generation ABIS, slated for initial operating capabilities the summer of 2008, would be the first large-scale, transactional production environment migrating from a fingerprint-only system to one with fingerprint, palm, face, and iris modalities. Many companies and federal agencies have adopted the ABIS concept; however, integration challenges remain a concern.

As a result of 9/11 and even earlier border control requirements, AFIS systems are migrating toward "real time" response. When IAFIS was initially funded in the early 1990s, the response time for tenprint searches at the FBI was measured in months. With the advent of IAFIS operations in the late 1990s, the response for criminal searches has been measured in hours or minutes. With NGI, the goal is to provide responses in seconds for high-risk, National Security encounters to be searched against the KST and a few other high priority files. When a visa applicant is fingerprinted at a consulate overseas, the search needs to be completed in a few minutes. Mobile-ID devices will require real-time responses for searches against limited repositories (e.g., wanted persons) often using less than ten fingers. The Royal Canadian Mounted Police (RCMP) has appropriately named their new AFIS–*Real Time ID*.

In 2005, the U.S. Army installed an AFIS in Iraq for use by the Iraqi National Police. One feature requested by the Iraqis and provided in the system was the ability to match latent footprints. Given the high volumes of latent footprints on hard surfaced floors being observed in Afghanistan and Iraq, in 2008 the FBI asked the Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST) to recommend a standardized collection methodology for plantar prints. SWGFAST has provided recommendations to CJIS, including draft sample card formats. It is anticipated that CJIS will ask the International Association for Identification (IAI) to approve the drafted card formats and pursue standardization in the ANSI/NIST standards process. Currently, NGI has no requirements to capture plantar prints; however when technology refreshment lends itself to support this within the NGI Program, the FBI intends to pursue this capability. SWGFAST recommends capture of footprints at 1,000 pixels per inch (ppi) with eight searchable areas per foot. The areas are the five individual toes, the ball/interdigital area, the arch, and the heel.

In 2005, the failure-to-match rates for tenprints of even a few percent became painfully obvious with the Jeremy Jones case. Jeremy Jones, suspected in the deaths of at least five women in four states, spent much of 2003 and 2004 in the Carroll County and Douglas County jails in West Georgia. He was wanted on a fugitive warrant in Ohio for jumping bond on a rape charge when he was jailed for minor offenses in Georgia. IAFIS failed to make a match on his fingerprints. Jones was released and suspected of committing at least two more murders, including that of Patrice Endres, missing since April 2004 and whose body has not been recovered. Jones has confessed to kidnapping and killing the woman, and dumping her body in a Douglas County creek. The FBI has a target of a 99 percent reduction in their already low error rates–to help

prevent errors and simultaneously to provide for increased productivity–more transactions without additional labor.

2.3 AFIS Overview

AFIS systems were initially used to identify candidates for skilled examiners to use in their searching and matching decisions. Over time, AFIS systems increased in reliability; if the AFIS had no tenprint-to-tenprint candidates with a score above some threshold, then no candidates were returned and the transaction was treated as a non-ident. More aggressive system owners, such as the New York State Division of Criminal Justice Services, took the absence of a clear candidate as the seed to launch additional name-based searches and 100-percent searches with no filtering such as pattern, sex, or age.

After years of monitoring IAFIS, the FBI established a second threshold. If a candidate were returned above that threshold, then the system would consider that high-scoring candidate a match.

AFIS systems are used in several places in the U.S. government including the FBI, Department of Homeland Security (DHS), and the DoD. The states and others have systems for criminal justice uses and civil applications such as benefits resource management. The following subsections address classes of use and size and then identify significant trends and events of the past few years. Other subsections explain how the systems work and the evolutionary movement from paper input to digital transactions.

2.4 Biometric Matching

2.4.1 Modes of Biometric Matching

The use of all biometric technologies can be classified into three basic modes.

Verification involves a 1:1 record comparison and is used to see if an individual's claimed identity is consistent with a registered account or previously enrolled record. Typical applications include access to secure areas, Personal Identity Verification (PIV) use, or voice verification to financial services. Verification applications often involve integration with card technologies and public key infrastructure (PKI).

Identification involves a 1:N (many) search against a database, the type of search used by state and federal agencies in generating and providing background information on subjects to submitting agencies. One or more biometric samples are searched against a database of previously enrolled subjects. If a match (or in some cases multiple possible matches) is found, the enrolled record is updated with the new event and the response is returned to the inquiring agency. If there is no match, a response of *no known record* is returned to the contributor and the record is enrolled into the database, if appropriate.

Watchlist involves a 1:few biometric comparison, and is used at a checkpoint as a screening mechanism to search for ineligible persons or persons determined to pose a threat. These applications may pose privacy concerns and tend to be the most technically

challenging in terms of throughput, accuracy, and reducing and managing the number of false alarms.[3]

2.4.2 Applications

Fingerprint-matching technologies have a variety of uses in the public and private sector. There are five high-level application areas where biometric data is collected and used:

1. **Criminal and Forensic Applications:** Applications of biometrics for criminal investigations and forensic work entail collecting biometric traits for searching at the time of arrest. The primary purpose is to record the arrest event and determine if a person has a known criminal history. Biometric checks may also record release events or be used to manage registered offenders. Forensic and latent fingerprint applications seek to link biometric signatures to known persons. Criminal and forensic uses are largely identification applications.
2. **Applicants:** Applicant searching or background checks are done when a person applies for a position of trust. The search determines if the applicant has any criminal history that might disqualify them; applicant searching may also be used to discover fraud and abuse in the form of duplicate requests for entitlements and benefits. These are identification applications.
3. **National Security:** These applications can vary and are beyond the scope of this document. An example is when non-U.S. citizens apply for a visa to come to the US. Biometric data is collected and searched to determine whether they are known or suspected of being unacceptable to enter America for any security-related reason. This is an identification and intelligence application.
4. **Civil Identification:** Civil identification refers to all forms of government-issued identification, most commonly driver's licenses; identity information is *optionally* searched to ensure subjects have not registered under a different identity or had similar identification revoked. This is an identification application.
5. **Physical and Logical Access Control:** These applications involve the authentication of a claimed identity in the context of an access control event. Physical access is typically for entrance to a government building of facility. Logical access is typically authentication to a personal computer, device, or network. Physical access generally is an authentication application, but may involve one-to-few matching in some environments.

The DoD also uses mobile identification technology to develop census data for areas where insurgents are trying to hide among the local population. These applications are instances of civil

[3] The alarm rate of watchlist applications can be estimated as a function of the watchlist size, data quality, and prior probability of the subject population.

identification coupled with national security checks as the people encountered at check points can be simultaneously verified as being enrolled in the census, checked against a watchlist, and returned to the DoD ABIS to check for hits against the Unsolved Latents collected in theater. Thus, the five application types can be run in various mixtures and should not be thought of as standalone or stovepipe applications.

2.4.3 System Size

Automated fingerprint matching applications are typically classified as one of the following sizes. There are no hard-and-fast rules for the breakpoint between the two size classes.

Large-scale where there is a large number of enrollees and/or a high transaction rate of searches/new enrollments. These systems often have over a million enrollments in the repository and/or tens of thousands of transactions a day, and are usually distributed with direct (or reasonably timely) access to a central repository (or multiple repositories).

Smaller-scale where there is a smaller number of enrollees and/or a lower transaction rate of searches/new enrollments. These systems can have repositories from a handful of people to a hundred thousand or more, and are often stand-alone, self-contained, and communicate with the central repository only occasionally, if at all.

The remainder of Section 2 will look at the automated fingerprint-matching technology market as it pertains to large-scale identification applications for criminal, applicant, national security, and civil identification. Such systems have traditionally been called AFIS. The desired trend is to move toward multimodal biometric identification systems that work with a combination of biometric data such as fingerprints, palm prints, facial images, and iris images.

2.5 AFIS Technology

AFIS technology started as a semi-automated way to generate candidate lists for tenprint–to-tenprint searches to deal with the steady growth in transaction volumes. The original systems required substantial human involvement. Personnel were required to scan fingerprint cards and enter basic biographic data, such as date of birth and sex. The largest labor element was the manual generation of extended Henry Class codes at the fingerprint card level for manual filing. Over the past 30 years, the need for binning by Henry Class, sex, or age to reduce the search depth has been eliminated by automated techniques. Today, tenprint-to-tenprint searches are extremely accurate and involve human intervention only to verify candidates when the score is too low to preclude a candidate but not high enough as to assure a match. The processing of latent prints involves human annotation and verification and, in general, is not as easy to process as tenprint searching. Latents are more challenging due to a reduced print area and inconsistent quality.

All large-scale AFIS systems follow a similar process. Images are entered, fingerprints are segmented from the background, ridges are located and thinned, and features such as bifurcations of ridges or locations of deltas are located and encoded in a Cartesian coordinate system. The coordinate systems typically have the zero, zero (0,0) point in the upper left corner of the image with the Y values increasing as they go down the image–the traditional coordinate protocol for

image processing. These points are encoded with elements that include (x, y) locations, the angle of ridge flow (θ), and vendor-specific attributes (e.g., ridge count to nearest neighbor). The extracted features are loaded into computer hardware, sometimes referred to as "registered to the system."

Figure 2-1. Minutiae Extraction from Finger Image

New fingerprint images are also subjected to feature extraction. The new feature sets are then compared to the registered sets by using vendor-developed algorithms to determine whether any two fingerprint sets are matches. Most feature sets are similar, but each vendor has slightly different representations or different feature attributes based on their algorithms. These differences do not pose an interoperability issue in tenprint transactions since they typically employ image-based transactions. Several standard templates representations are supported by leading AFIS vendors. However, the representation comes at a cost to accuracy.

In the latent print world, finding the features requires human review before or after the encoder processes an image. Rather than submitting image-based searches to remote AFIS systems, it would be more efficient if the original latent examiner could extract features once and send them to other AFIS systems, independent of the algorithm and encoding technique used. A phrase often used to describe this process is "enter once, search many." This leads to the overarching interoperability issue that the National Institute of Justice is studying and for which it has established an AFIS Interoperability-Experts Panel.

Systems have become more sophisticated. They often use two or more matching stages to perform a coarse initial filter and then compare results further in subsequent search stages with finer grain algorithms. In addition to minutiae comparison, matching algorithms can include other image features, such as pattern and ridge counts and ridge flows, to minimize the search space. Multi-stage matching typically occurs in parallel on different processors dedicated to work on partitions of the overall database. Efficient parallel computation that is neither constricted by data access nor communications is an important consideration for NGI.

Civil and criminal fingerprinting processes have moved to electronic livescan tenprint and palm capture devices using Certified Products (see the section on FBI CPL) with the results being submitted electronically using appropriate standards.

2.6 Evolution of Electronic AFIS Input Collection

In the past 20 years, the trend has been to move from inked/paper fingerprint capture to livescan stations where "virtual fingerprint cards" are generated and sent electronically to AFIS sites. This process reduces the keying of biographic and demographic text at the AFIS site, and eliminates card scanning and re-entering biographic data at the central site. These livescan transactions rarely are printed to card stock, but can be printed for courtroom use, investigative activities, and archival purposes.

The input to a search/enrollment for a large-scale AFIS can be from any of the following image types:

Rolled fingerprints and sequence slaps (virtual fingerprint cards)

Identification Flats (ID-Slaps)

Palm impressions

Latent impressions

Less than 10 fingers (Mobile-ID and DoD collection systems).

Not all of these record types are currently accepted by IAFIS. The following table shows how the image types are used in various applications.

Table 2-1. Application of Image Types

Type	Typical Use	Used by IAFIS?
10 rolled and sequence-slaps	Identification applications	Yes
Identification slaps	Identification applications for applicants	Yes
Palm impressions	Crime scene-related identification	No
Latents	Crime scene-related identification	Yes
Less than 10 prints	National Security and mobile applications	Starting in 2008

2.6.1 Rolled Fingerprints and Sequence Slaps

The 10 rolled images and four sequence-slap images have been the "gold standard" for AFIS systems and earlier manual systems. The sequence-slap impression is captured when the fingers of each hand are captured together and the thumbs are captured individually. In addition to providing a second set of finger images, these impressions also reduce the opportunity for sequence errors in the rolled set–such as rolling two or more fingers in the wrong order. This could cause a serious matcher error resulting in a missed ident.

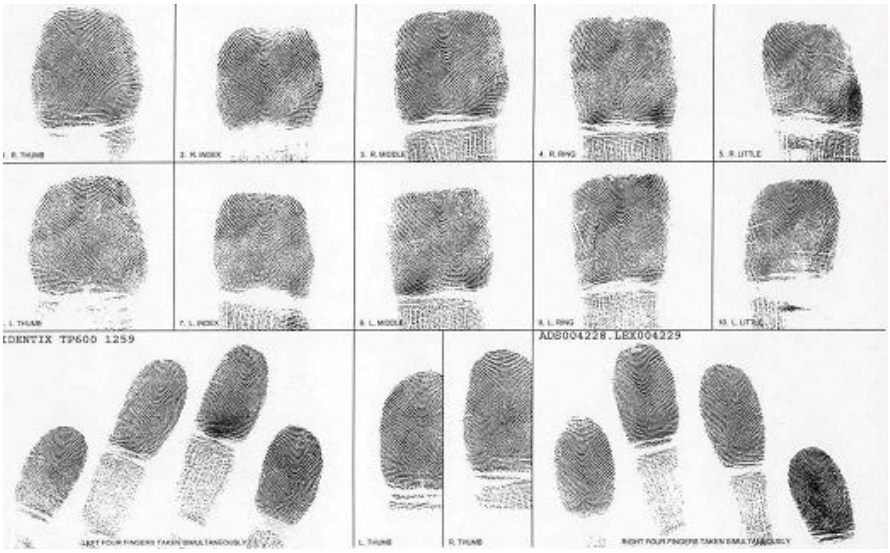


Figure 2-2. Rolled and Plain Impressions on Tenprint Card[4]

2.6.2 Identification Slaps

In 2007, the FBI started to support Identification Slaps (ID-slaps, or also sometimes called ID flats) to permit states and other subscribers to collect and submit plain impressions rather than a full set of rolled and sequence-slap prints for applicant searches. While Identification flats are more computationally expensive to search on IAFIS than rolled tenprints, they are faster and easier for the subjects being fingerprinted (seconds rather than minutes) and less intrusive than traditional 10 rolled and four flat (plain) image capture. Four-finger ID-slaps images in an FBI-EBTS transaction each have a segmentation box defined by the capture device and provide an NIST Fingerprint Image Quality (NFIQ) score for each finger. The use of ID-slaps, instead of sequence-slaps in tenprint collection on livescans, is the latest evolution in data collection.

---

[4] http://www.highered.nysed.gov/tcert/images/samplecard.gif.

Figure 2-3. Identification Slaps (or Flats)

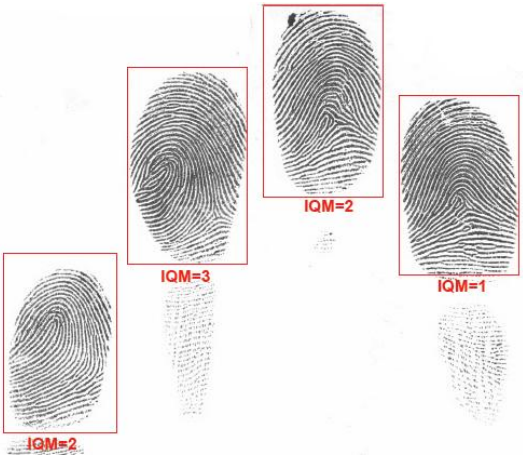


Figure 2-4. Identification Slaps with Segmentation Boxes and NFIQ Scores

2.6.3 Palm prints

Palm prints have been captured for years. In early 1994, an automated palm print matching system, called "Recoderm," was installed by the Hungarian company "Recoware" in the Szolnog police headquarters, a suburb of Budapest, Hungary. Now, all of the large-scale AFIS companies offer this capability. The IAI worked closely with the FBI to develop a standard palm print card. At that time, many livescans had platens that could not capture an entire palm image from the tip of the fingers to the carpal crease. The technique used to permit these smaller platens to capture a whole palm was to capture two images with sufficient overlap to permit an examiner to verify that the upper and lower palm images are from the same hand. The overlap area is the interdigital area. In addition, the "writer's palm" is also collected (i.e., the edge of the hand that comes in contact with a writing surface). Palm prints collected from a subject are called "known palm prints" to differentiate them from latent palm prints. In criminal cases, palm prints are typically collected with a full rolled tenprint capture. Palm searches are made from known palm prints to latent palm prints and vice versa. Known palm prints are typically not searched against other known palm

prints. The following image has an arrow and an outline box indicating the location of the inter-digital area.

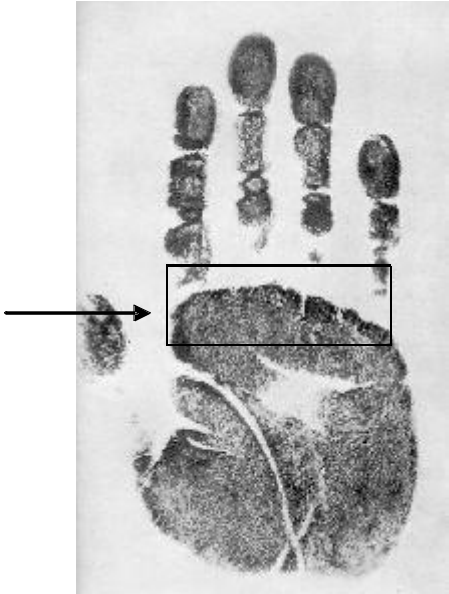


Figure 2-5. Palm print

2.6.4 Latent prints

Latent Prints (from fingers or palm) are scanned and read into an AFIS latent workstation and searched on AFIS systems against some or all of the records in the fingerprint and palm print databases. A latent print examiner will work with the latent workstation software to prepare the image (e.g. orient, crop, annotate features). After the candidate list is returned, the examiner will compare the latent print image with the candidate images to determine if a match exists. As an aid to investigators, latents can be searched against latents to link crimes.

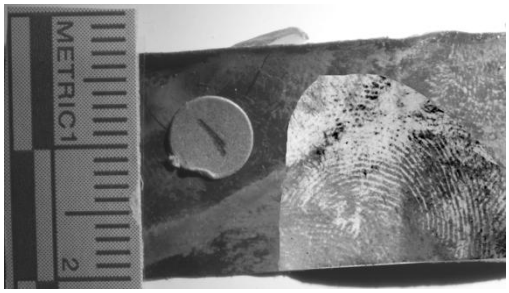


Figure 2-6. Latent Print with Scale for Calibration

2.6.5 Less Than Ten Prints

Less than 10 prints is a collection mode used in operational environments such as the DoD, where the time available or the configuration of the collection device does not support the full 20-finger collection associated with 10 rolled and four sequence-slap images or even the Identification flats. This mode is becoming more prevalent as Mobile-ID devices are proliferated across law enforcement agencies. While this approach is more time-efficient for collectors, it means that NGI will have to deal with degraded source material and less information per enrollment. An ad-hoc working group is addressing the extension of the standards to deal with Mobile-ID transactions. The Advisory Policy Board (APB), FBI, and NIST recognized the need for this extension and established the ad-hoc group. The working group's first meeting was held in July 2007.

2.6.5.1 Historical Approach for Tenprint and Latents

Historically, tenprint and latent images were processed to extract four kinds of data:

- minutiae locations and angles;
- primary features, such as pattern type, core, and delta locations;
- neighborhood relationships such as inter-minutiae ridge counts; and
- quality and confidence levels for various data points.

In the processing of tenprint, palm, and other known images, the AFIS does all the necessary steps autonomously, including image quality assessment and sequence checking. The images with problems are sent to a Quality Review workstation for human intervention. Image processing includes segmentation of slaps into individual finger images, orientation correction for finger images captured off axis, contrast adjustments, and thinning and binarization of ridges to support feature extraction. Image sets with irresolvable sequence errors and extremely low image quality are rejected. The reject rate at the FBI is higher for applicant prints than for criminal prints, as applicants are normally available for being reprinted. With the rapid turnaround at IAFIS and fast responses from NGI, the likelihood of an arrestee still being available is becoming higher. The resultant Type-9 feature sets (e.g. pattern type, minutiae) are typically vendor-specific and kept secret by the vendors.

Latent print images are not enhanced during the AFIS acquisition process. No information or detail is added to the lift/image containing the latent print. Photographic filters and computer-based image processing techniques, such as contrast adjustment and removal of high frequency noise, can be used to make the image more apparent and distinct (to humans). This may include vendor-provided software and techniques such as measuring the amount of grayscale light in a captured image, black/white balancing, and image reversal with ridges appearing as valleys. Some vendors claim to "project" where an obscured ridge section is; this information may sometimes

result in the generation of new candidate matches. That additional estimated information is never added to the original image nor used in making a match or no-match decision. It is an interim detail used by the algorithms for finding possible matches that might otherwise be missed.

Digital image manipulation programs provide tools that may appear to visually enhance images of low quality or overlapping latents, and reduce background image interference. However, operating procedures require that all processing steps be noted to ensure that spurious information is not unintentionally lost or added.

2.6.5.2 Extended Fingerprint Feature Set Approach

In 2005, the ANSI/NIST Committee to Define an Extended Fingerprint Feature Set (CDEFFS)[5] was established to identify, define, and provide guidance on additional fingerprint features beyond the traditional ending ridges and bifurcations defined in the ANSI/NIST ITL-1 standard for Type-9 representation of minutiae. This feature set would include more complete finger image information for the human examiner and improved automated feature extraction.[6] It is important to note that the default Type-9 minutiae set defined in ANSI/NIST ITL-1 has never been tested on a large-scale database and is not used in any productions systems. The ANSI/NIST ITL-1 lists the following alternative Type-9 structures in Table 2-5:

- IAFIS Features
- Cogent Systems Features
- Motorola Features
- Sagem Morpho Features
- NEC Features
- M1-378 Features
- Identix Features.

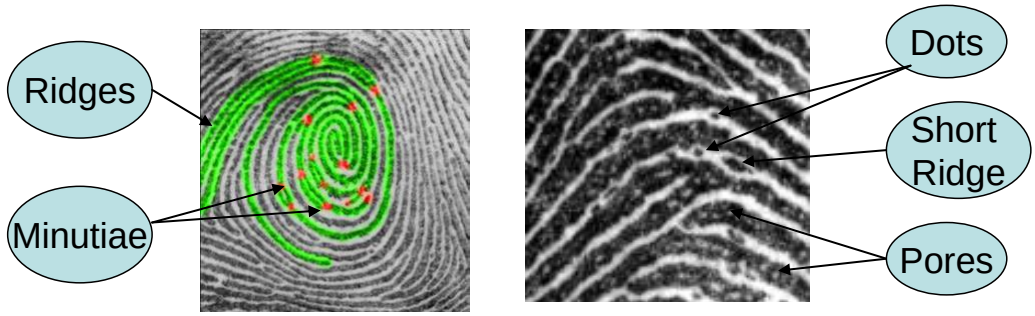
CDEFFS is looking at methods to capture and represent, in an ANSI/NIST ITL-1 Type-9 style record, additional fingerprint features such as dots, short ridges, ridge protrusions, spurs, pores, and incipient ridges. Each feature is in addition to the minutiae currently used by AFIS coders and as specified in the ANSI/NIST ITL-1 Type-9 definitions. They propose changing the Type-9 Record title from a Type-9 Minutiae Data Record to a Type-9 Friction Ridge Feature Data Record. In the figure below, the two images depict some of the additional information as currently

---

[5] http://fingerprint.nist.gov/standard/cdeffs/index.html.

[6] "Standardizing a More Complete Set of Fingerprint Features," Briefing at the International Association for Identification conference, 24 July 2007.

envisioned by the CDEFFS. The addition of ridge path flow, pores, dots, and short ridges are examples of Proposed Level 3 details under consideration.



Augmented Level 2 Ridge Path Dots, pores and short ridges

Figure 2-7. Extended Fingerprint Features

In contrast to earlier applications of rolled and flat finger image feature encoders, new AFIS systems can already extract more traditional features from the same images. This will increase latent print matching accuracy without adding all of the CDEFFS-defined extensions. The graphic below lists some additional information items. Vendors already may be using some of the CDEFFS recommended additions in their registered Type-9 feature sets. With the expansion of the standard to include these additional attributes, interoperability at the feature level might be enhanced.

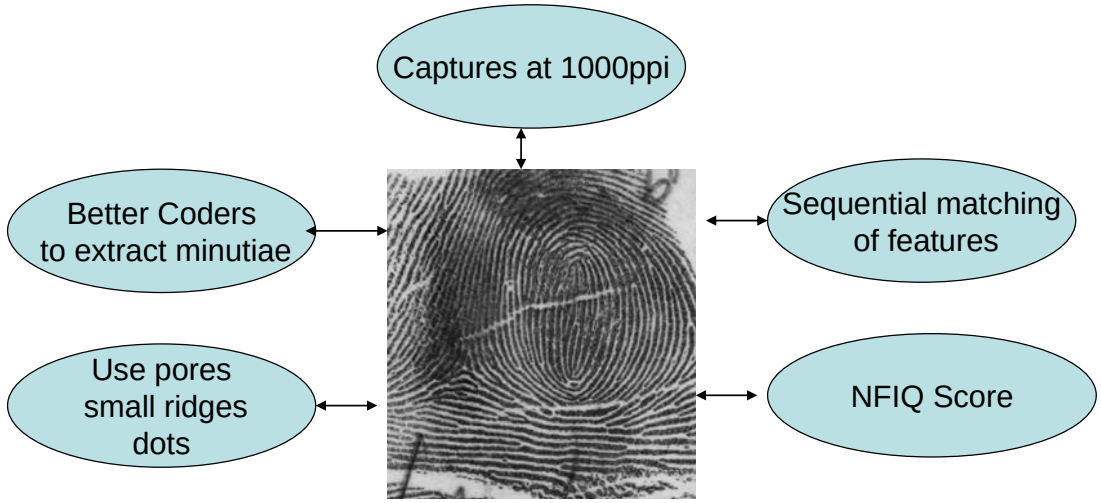


Figure 2-8. Fingerprint Image Metadata

2.6.6 Evolution of Investigative and Prosecutorial Use

Of all the biometric modalities, fingerprints are the most prolific in their use in daily law enforcement and criminal justice administration. Thousands of arrestees are fingerprinted daily. The search results are used in investigations, case development, prosecutorial decisions, court hearings, and sentencing decisions. At the same time, thousands of latent finger and palm prints are searched daily as part of criminal investigations.

There is little documentation to indicate the number of latent print identifications that have led to convictions or how many are searched across all the AFIS systems in the U.S. Because criminal processing is segmented among crime scene technicians, forensic lab latent print examiners, detectives, and prosecutors, latent examiners frequently have no knowledge of the effect of their identifications. Fingerprint evidence is always considered in the context of other evidence to ensure the evidence is directly attributed to the perpetrator and links the perpetrator to a crime. However, there are examples of heinous crimes where the only evidence was a latent print that was subsequently identified, resulting in an arrest and conviction.

An extreme example of investigating and solving a crime via the latent match is the murder investigation into the killing of FBI Special Agent (SA) Stanley Ronquest, Jr. On the night of March 11, 1992, SA Ronquest was shot and killed when an assailant attempted to rob him outside of a hotel in Kansas City, Missouri. The only evidence was a fingerprint on a wrapper found at the scene. The FBI spent over 40,000 Special Agent hours on the investigation in the pre-IAFIS era. A perpetrator was eventually identified by the pre-IAFIS, semi-automated, latent search capability of the FBI, and upon questioning and further investigation two perpetrators were convicted. It is thought that IAFIS could have identified the perpetrator as a candidate within hours of the initial latent fingerprint submittal at a substantial savings in investigative hours.

Starting with the United States of America vs. Byron C. Mitchell case on October 27, 1998, there have been a series of defendant motions in criminal cases challenging the scientific validity of the claim of individuality in the matching of fingerprints. In the Federal courts, there were Daubert hearings,[7] while in some state courts there are Frye hearings that determine the acceptance of expert testimony (and methods). Several motions were successful, but only temporarily. In the case of the State of Maryland vs. Bryan Rose, the defendant asked for and received a Frye hearing allowing them to question the veracity of the fingerprint evidence. Judge Susan Souder found for the defendant and excluded the latent fingerprint testimony. While the case may be reopened in the federal courts, the Daubert/Frye challenge is large and growing. A later section will address the challenge of establishing "an error rate and of objective criteria which when applied, are documented and can be verified."[8]

---

[7] Daubert vs. Merrell Dow Pharmaceuticals, 509 U.S. 579, 113 S. Ct. 2786, 125 L. Ed. 2d 469 (1993).

[8] Conclusion of Judge Souder's Memorandum Decision in State of Maryland vs. Bryan Rose.

Defense attorneys are becoming more familiar with the latent print identification process and increasingly challenge such evidence as is seen in the number of Daubert and Frye hearings requested.

2.7 Simulation and Modeling

Simulations can be used to develop models of processing scalability and matcher performance scalability.

2.7.1 Models of Processing Scalability

A common technique in architecting an AFIS solution is to develop models of processing scalability from an IT perspective. This includes queue lengths, network loading, disk transfer rates, computing resources, and memory capacity. Individual vendors, some agencies, and some consultants have their own models for this aspect of systems analysis and planning. This class of modeling is imperative in design efforts for new systems to ensure that sufficient disk storage is provided, network architecture is appropriate, and adequate verification and latent workstations for the anticipated workload and the anticipated manual review rates.

2.7.2 Matcher Performance Scalability

Matcher performance scalability is difficult to model on operational systems where ground truth data is not available. It is not possible to directly measure performance at ultra-high transaction rates against ultra-large repositories, particularly *a priori*. NIST and other performance evaluations show that as the repository size increases, there is an increase to the error rates. As the repository grows, matchers are exposed to more and more fingerprint feature sets with similar characteristics. Matching performance is typically measured in terms of performance v. repository size, number of fingers compared, and the quality and type of prints.

2.8 AFIS Products and Sources

2.8.1 Typical Vendor Offerings

Multiple vendors operate in the AFIS market. Typical capabilities and products that these companies can offer are indigenously produced or based on the integration of third-party technology (e.g., card scanners). They include:

AFIS proprietary coding and matching capabilities

- Fingerprints
- Latent fingerprints
- Palm prints
- Latent palm prints

Live capture devices–multimodal collection

- Fingerprint, Palm prints, Mug shot, Signature(s), Voice

Card conversion to digital records

- Tenprint cards
- Palm cards

Latent Case Management Software

Facial Recognition

Iris Recognition

Fusion within a modality and across modalities (fusion approaches vary and may be difficult to extend, but examples are Face and Iris collection and Fingerprint and DNA collection)

2.9 Technology Sources

There are four sources of fingerprint-matching technology:

1. Large companies that build large-scale systems
2. Smaller companies that build mid-sized through large systems
3. Companies that offer products associated with AFIS enterprises
4. Government agencies that supply free tool sets, known as government off-the-shelf (GOTS).

The following subsections address each set of sources, in order.

2.9.1 Large AFIS Vendors

Below is a listing of established biometric companies conducting business in the U.S. Each company offers an AFIS system and offers an array of products and services in the AFIS area.

Table 2-2. Vendors for Large AFIS Systems

AFIS Company	History	Notable AFIS Contracts	HQ
Cogent Systems S. Pasadena, CA	Cogent Systems is a global biometric identification solutions provider, having researched, designed, developed, and marketed fingerprint biometrics technologies. Cogent was established in 1990 and became a publicly traded company in September 2004. Trades on NASDAQ as COGT.	LASD, Ohio, Maryland	U.S.
L-1 Identity Solutions, Inc. Stamford, CT	Formed in 2006 through the merger of Viisage and Identix. L1 includes Integrated Biometric Technology, SecuriMetrics, Iridian, SpecTal, ComnetiX, McClendon, Advanced Concepts, Inc. and Bioscrypt. Trades on NYSE as ID.	DoD next generation ABIS (a multimodal system with fingers, palm prints, faces, and irises)	U.S.
Motorola Biometrics Business Unit Anaheim, CA	The Biometrics Business Unit serves the AFIS, Livescan, and Identity Management markets. The unit is the result of Motorola's acquisition of Printrak in 2000. The company was originally created as a division of Rockwell International and sold in 1984 becoming De La Rue Printrak, Inc. Trades on NYSE as MOT.	U.S. Army, Iraqi National Police, State of Louisiana, State of Nevada; State of Florida, FDLE	U.S.

AFIS Company	History	Notable AFIS Contracts	HQ
NECAM Sacramento, CA	The NEC Corporation was founded in July 1899 as the Nippon Electric Company, Limited. The NEC Corporation of America (NECAM) began on July 1, 2006, combining NEC America, NEC Solutions America, and NEC USA.	Illinois State Police, Texas DPS, Pennsylvania State Police	Japan
Sagem Morpho, Inc. Tacoma, WA	The company was founded in the U.S. in 1985 as a subsidiary of French fingerprint system developer MORPHO Systèmes, S.A. Purchased in 1993 by the SAGEM Group of Paris. Now a wholly-owned subsidiary of the European firm Sagem Sécurité, a company in the SAFRAN Group.	New York State, Arizona DPS, Hawaii, NYPD	France

The U.S. government has laws and regulations associated with procurement of information technology (IT) systems from companies where a foreign entity has a controlling interest. This set of legislation traces its roots to the Buy American Act of 1933 (41 U.S.C. § 10a–10d). When the application domain is inside a classified contract, the standards are more rigorous. The National Industrial Security Program (NISP) sets standards for companies intending to participate in classified U.S. government contracts. One standard is that a company must not be under the ownership, control, or influence of a foreign entity to the extent that if the company had access to classified materials, it would not be in the best interest of U.S. national security. The criteria for establishing the degree of foreign involvement is found in the NISP Operating Manual (NISPOM). It defines what is a concern regarding foreign ownership, control, and influence (FOCI) and provides evaluation standards.[9]

Some AFIS companies establish U.S. companies to meet various U.S. laws and regulations. NEC established NECAM, headquartered in Sacramento, CA, and Sagem established Sagem Morpho, Inc. in Tacoma, WA. This assessment does not attempt to address legal issues of foreign ownership or control and the associated nuances.

[9] http://www.fedcontracts.org/overcoming-foreign-ownership-control-and-influence-issues.

There are other large-scale AFIS developers/vendors in Europe and Asia. They include: Germany (Dermalog); India (CMC–a TATA Enterprise, and Zygox–affiliated with NEC); Korea (Hyundai); and Russia (BioLink, Papillon, and Sonda Technologies) and possibly other countries. Currently, these companies have little or no direct presence in North America, but the FBI stays informed about their offerings, as they could offer the next set of clever algorithms. BioLink formerly had a presence in the U.S. as BioLink USA.

2.9.2 Smaller AFIS Vendors

There are several smaller vendors in the U.S. selling competitive AFIS products. They fall into two product groups: medium- to large-scale systems and small to medium systems.

Medium- to large-scale systems for national ID and criminal justice use are intended to provide a combination of low cost per transaction and high "accuracy" rates. Most of these companies' sales are in the national ID and election enrollment market, but they are moving into the criminal justice market place. Two examples of medium-to-large system companies are:

- East Shore Technologies, Inc. of Troy, New York. They are a provider of services to fingerprint recognition system prime contractors and to integrators of multi-technology systems where fingerprints are a single component within a larger integrated system.
- ID Solutions, Inc. of Orlando, Florida. They offer AFIS algorithms running on scalable PC networks–scalable to millions of records for criminal and civil markets.

Small to medium AFIS systems provide finger, palm, and latent matching, permitting small to medium size cities and counties to have their own forensic capability. That market addresses many of the U.S. State and city law enforcement agencies. Two such companies are:

- AFIX Technologies' AFIX Tracker system that runs on Windows™. An American investment firm, "L1 Investment Partners" (associated with, but different than L1 Biometrics) owns AFIX Technologies, Inc. of Pittsburg, Kansas.
- SPEX Forensics' AFIS system that runs on Linux. SPEX Forensics of Edison, New Jersey is owned by "HORIBA Jobin Yvon Ltd.," based in Stanmore, North London, UK.

2.9.3 Associated Vendors

The following companies do not sell ABIS systems, but offer products and services in the North American market that are components of some ABIS systems and some livescan systems. They are representative of the many companies that are significant contributors to the growth of the fingerprint-based identification industry.

Table 2-3. Associated Providers

Company	Specialty	Headquarters
Aware Inc.	The company offers biometrics and imaging applications including enrollment of fingerprints and facial images, identification personalization and reading, and networking primarily in government systems. It sells its products to original equipment manufacturer suppliers.	Bedford, MA
Biometrics4ALL	This technology company provides software for criminal and civil transactions on all vendors' livescan devices.	Santa Ana, CA
Cross Match Technologies, Inc.	Cross Match Technologies, Inc. provides interoperable biometric identity management systems, applications and services in the area of multimodal biometric capture, Verification and Identification, and document and credential authentication and verification. Solutions are offered as fixed, mobile (jump Kits) and hand-held offerings.	Palm Beach Gardens, FL
ImageWare Systems, Inc.	Image processing for IQS/compression/printing. Multimodal fusion tool set	San Diego, CA
Mentalix, Inc.	Image processing software for IQS/compression/printing.	Plano, TX

Company	Specialty	Headquarters
Neurotechnology (Formerly Neurotechnologija)	Provides algorithms and software development products for biometric fingerprint and face recognition, computer-based vision, and object recognition to security companies, system integrators, and hardware manufacturers. These matcher algorithms are used in the DoD Biometrics Automated Toolkit (BAT). Neurotechnology recently introduced VeriEye ™ iris matching capability to their product offerings.	Vilnius, Lithuania

2.9.4 Government Products

The U.S. federal government has developed several software tools to provide functionality that can deal with vendor-specific proprietary techniques without disclosing the underlying intellectual property. Other tools have been developed to measure image quality across all vendor collection devices.

This software is typically developed with the support of contractors and Federally Funded Research and Development Centers (FFRDC). Key challenges are to maintain and improve this software (e.g., keep up with OS evolution and enhance functionality) and to provide customer support.

The following table provides an overview of some of the applicable GOTS software products associated with automatic fingerprint identification. Many NIST tools are more suited for engineers and researchers than for production fingerprint shops. More details on the NIST tools can be found on the Web.[10]

[10] http://fingerprint.nist.gov/NFIS/.

Table 2-4. Government Products

Product	Purpose	Agency Providing the SW
DoD Fingerprint Image Quality Measurement Tool (FIQM)	The DoD/Biometric Task Force (BTF) FIQM software (2008) can be used as a reasonable predictor of AFIS matching performance. The tool is vendor agnostic and has been evaluated by NIST. A report is available from the BTF. Their website is www.biometrics.dod.mil.	DoD/BTF
NIST Biometric Image Software (NBIS); replaced NIST Fingerprint Image Software (NFIF2)	NBIS is an ongoing tools development project by the NIST for the FBI and DHS. For details on obtaining the latest version of NBIS Non-Export Control source code or requesting the NBIS Export Control source code, visit http://fingerprint.nist.gov/NBIS/index.html.	NIST
NIST Fingerprint Image Quality Software (NFIQ)	The NFIQ software (2004) assesses fingerprint images and assigns a quality score of 1 (highest) to 5 (poorest). The related NIST test demonstrated that image quality metrics can predict matcher performance. This single quality measure can be used for multiple vendors and multiple data sets.	NIST
NIST Fingerprint Matching Algorithm (AKA Bozorth3 Matcher Algorithm)	A minutiae-based fingerprint-matching algorithm. It will do one-to-one and one-to-many matching operations.	NIST/FBI
NIST Slap Segmentation algorithm (NFSEG)	NFSEG can segment the four-finger plain sequence impression found on the bottom of a fingerprint card into individual fingerprint images or it can be used to remove white space from a rolled fingerprint image.	NIST

Product	Purpose	Agency Providing the SW
Universal Latent Workstation (ULW)	Sharing latent identification services within the US is complicated by the hierarchical network of AFIS systems and the variation in latent search feature sets. The ULW simplifies cross-jurisdictional searches by enabling an examiner to search multiple AFIS with a single fingerprint feature encoding. The examiner will edit the features to optimize the search for a particular AFIS but may not need to reenter the entire case.	FBI

2.10 Risks Associated with Foreign Sourcing

Section not for public release.

2.11 Standards and Specifications

The development of IAFIS required a standardization of information content and format that would make the interface between the states and IAFIS electronically uniform. Only with electronic submittals and responses could the FBI support same-day service. This standardization included data formats, transmission protocols, image compression and decompression standards, and image capture quality-related technical thresholds (e.g., modulation transfer function, MTF).

These fingerprint-related publications are described in more detail below. The root document for all of this standardization was the 1993 release of an ANSI/NIST standard that has been updated several times.

There are many standards existing and emerging in the U.S. and international standards bodies (please refer to section 5 for more additional information). In the AFIS area, there are a handful of critical standards and specifications for which compliance is essential. They are:

NIST Fingerprint Interchange Standard.

FBI Electronic Biometric Transmission Specification.

FBI EBTS Appendix F, IAFIS Image Quality Specifications.

Department of Defense Electronic Biometric Transmission Specification.

Interpol Implementation of ANSI/NIST-ITL 1-2000.

WSQ Fingerprint Image Compression Encoder/Decoder Certification.

NIST Fingerprint Image Quality (NFIQ) Compliance Test.

2.11.1 Standards

NIST Special Publication 500-271: Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information–Part 1 (ANSI/NIST-ITL 1-2007) began in 1986 as a mechanism to exchange fingerprint minutiae information between states and the FBI. That version focused on minutiae exchange. It was never used in a production environment. In 1992 and 1993, the FBI worked with NIST to develop a more robust and broader-in-scope document that carried forward some of the 1986 material. The current version, adopted in 2007, includes provisions for fingerprint; palm print; face; iris; and scar, mark and tattoo images, friction ridge minutiae/features, and a place holder (Type-99) records to support exotic modalities (such as ear-prints) as they are introduced. An XML version (to be known as Part 2) of the ANSI/NIST-ITL 1-2007 document is under evaluation as a DRAFT and is anticipated for approval in the summer of 2008.

The ANSI/NIST Fingerprint Interchange standard defines 16 record types (Types-1 through 10, Types-13 through 17, and Type-99). The FBI implementation, FBI-EBTS, use these record types as follows:

Table 2-5. ANSI/NIST Record Types

ANSI/NIST Record Type	Use	Acceptability per FBI-EBTS
Type-1	Transaction Information	Mandatory
Type-2	User Defined Descriptive Text Record	Mandatory
Type-3	Low Resolution Gray Scale Fingerprint Image Record	No
Type-4	High Resolution Gray Scale Fingerprint Image Record	Optional
Type-5	Low Resolution Binary Fingerprint Image Record	No
Type-6	High Resolution Binary Fingerprint Image Record	No
Type-7	User Defined Image Record	No
Type-8	Signature Image Record	No
Type-9	Minutiae Data Record	Optional
Type-10	Facial and SMT Record	Optional
Type-13	Variable Resolution Latent	Optional

ANSI/NIST Record Type	Use	Acceptability per FBI-EBTS
	Image Record	
Type-14	Variable Resolution Tenprint Image Record	Optional
Type-15	Variable Resolution Palm print Image Record	Optional
Type-16	Test Record	Optional
Type-17	Iris Image Record (new in 2007 revision)	Optional
Type-99	CBEFF (new in 2007 revision)	No

2.11.2 Specifications

FBI-EBTS[11]

The FBI Electronic Biometric Transmission Specification (FBI-EBTS) (IAFIS-DOC-01078-8.002): This document is the FBI's implementation of the ANSI-NIST standard. It is the base document for all fingerprint related transactions between the FBI and the states. Originally approved in 1994 as the Electronic Fingerprint Transmission Specification (EFTS), and most recently updated in 2008, it includes provisions for the additional biometrics addressed in the 2007 version of the ANSI/NIST Standard.

FBI EBTS Appendix F, IAFIS Image Quality Specifications: This document is a critical element of the FBI's EBTS. It states the requirements for certification of scanners and printers. This set of requirements is the basis for FBI certification (see the section on CPL).

DoD-EBTS[12]

Department of Defense Electronic Biometric Transmission Specification, November 8, 2006, Version 1.2 DIN: DOD_BTF_TS_EBTS_ Nov06_01.02.00: This document is the DoD's implementation of the ANSI-NIST standard. The specification addresses DoD systems and data exchange within the DoD domain of ANSI/NIST ITL-1 users. Their needs often include

[11] http://www. fbibiospecs.org/fbibiometric/biospecs.html.

[12] http://www.biometrics.dod.mil/CurrentInitiatives/Standards/DoDEBTS/tabid/106/Default.aspx.

transactions that are neither law enforcement- nor applicant-related (e.g., base access control transactions).

Interpol EFTS[13]

Interpol Implementation of ANSI/NIST-ITL 1-2000 Version No. 4.22b, October 28, 2005: This specification addresses data exchange among Interpol domain member states. The Interpol AFIS Expert Working Group prepares and maintains it.

WSQ[14]

WSQ Fingerprint Image Compression Encoder/Decoder Certification Guidelines, January 12, 1999: The Wavelet Scalar Quantization (WSQ) Gray-scale Fingerprint Image Compression Algorithm is the standard for the exchange of compressed 500 ppi fingerprint images within the criminal justice community. The WSQ Specification defines a class of encoders and a single decoder with sufficient generality to decode compressed image data produced by any compliant encoder. Fingerprint images should not be compressed more than 15:1 on average.

WSQ Compression Guidelines - Commerce Business Daily (CBD) (August 17, 1995 PSA#1412): In this CBD issue, the FBI announced their plans for compression rates for digital fingerprint images. "The Electronic Fingerprint Transmission Specifications (EFTS) establishes image quality standards for card- and live-scan equipment. Fingerprint images captured on systems that are certified to comply with EFTS image quality specifications shall be compressed to a maximum average ratio of 15:1 using Wavelet/Scalar Quantization (WSQ) algorithm. ... The average compression ratio is measured as the average across several sets of 1.5 by 1.6 inch rolled impressions. Once the algorithm has been calibrated to the source image characteristics with this procedure, then images of any dimension can be compressed with the same compression parameter settings."

NFIQ[15]

NISTIR 7300: NIST Fingerprint Image Quality (NFIQ) Compliance Test: NIST studied fingerprint image quality as a predictor of AFIS match accuracy and implemented the algorithm in an open software tool. NFIQ analyzes a fingerprint image and assigns a quality value of 1 (highest quality) to 5 (lowest quality) to the image. Higher quality images produce better performance with matching algorithms.

---

[13] www.interpol.int/Public/Forensic/ fingerprints/RefDoc/implementation6.pdf.

[14] WSQ Fingerprint Image Compression Encoder/Decoder Certification Guidelines: http://www.itl.nist.gov/iad/894.03/fing/cert_gui.html.

[15] Elham Tabassi, NIST http://www.itl.nist.gov/iad/894.03/fing/cert_gui.html.

NFIQ can be used for real-time quality assessment; all government agencies are directed to use NFIQ to assess the quality of fingerprints for PIV cards per SP 800-76 Biometric Specification for Personal Identity Verification.

NFIQ will be used by FBI to assess quality of ID-Slap submittals and by submitters of ID-Slaps to the FBI.

Vendors normally use a proprietary metric that has a wider range (e.g., 1-100 in steps of 1) and addresses other fingerprint attributes such as presence of cores and deltas, which are not factored into the NFIQ algorithm. These proprietary scoring techniques are typically tuned to specific matcher algorithms.

2.12 Performance Measurements

2.12.1 Background

Prior to IAFIS, there was an ANSI/NIST standard for testing AFIS systems and one for AFIS Technical vocabulary. Both are about 13 years over the mandatory ANSI window for renewal (each standard must be reviewed, and updated or confirmed as relevant every five years). These older AFIS standards are still referenced in other standards documents such as ANS/NIST ITL-1 2007. These two standards should be updated and re-issued to assist the community. Copies of these 1988 standards documents are available from the International Association for Identification (IAI). They are:

> American National Standard for Forensic Identification–Automated Fingerprint Identification Systems–Benchmark Tests of Relative Performance. (ANSI/IAI 1-1988)
>
> American National Standard for Forensic Identification–Automated Fingerprint Identification Systems–Glossary of Terms and Acronyms. (ANSI/IAI 2-1988).

2.12.2 Performance Metrics Vocabulary

The aforementioned ANSI/IAI standards, Benchmark Tests and Glossary of Terms and Acronyms provided definitions of performance metrics. Since they were approved in 1988, the biometrics landscape has changed dramatically. With the emergence of a broader biometrics community, there has been an increased interest in testing and reporting metrics. Performance metrics provide insight into algorithm performance as a function of scoring thresholds–Receiver Operating Characteristic (ROC) curves. These and other metrics are common in the research and academic world, but not easily recognized or understood by the AFIS operators or the AFIS management community. Moreover, ROC curves do not address the human examiner role in AFIS system use. For complete information on performance testing and reporting methods, please refer to ANSI/INCITS 409.x-2005, Biometric Performance Testing and Reporting, parts 1-4.

The basic terms and their definitions are:

Receiver operating characteristic (ROC) curves: an accepted method for summarizing the performance of imperfect pattern matching systems. A ROC curve plots, parametrically as a function of the decision threshold, the rate of "false positives" (i.e., false matches) on the x-axis against the corresponding rate of "true positives" (i.e., true matches) on the y-axis. ROC curves are threshold independent, allowing performance comparison of different systems under similar conditions, or of a single system operating under differing conditions.

Detection error trade-off (DET) curves: In the case of biometric systems, a modified ROC curve known as a "detection error trade-off" curve is preferred. A DET curve plots error rates on both axes, giving uniform treatment to both types of error. The graph can be plotted using logarithmic axes. This expands the plot and distinguishes different, well-performing systems more clearly.

Cumulative Match Characteristic (CMC) curves: CMCs plot the probability of identification against the returned 1:N candidate list size. It shows the probability that a given user appears in different sized candidate lists. The faster the CMC curve approaches 1, indicating that the user always appears in the candidate list of specified size, the better the matching algorithm. CMCs are oriented toward access control systems and user performance.

Historically, collections of registered/enrolled/saved fingerprints and their features were known as a repository. The general biometric community has some members pushing to adopt the vocabulary in use by the facial recognition community for all biometric modalities. In their construct, repositories become galleries and search records become probes. These terms are alien to 100 years of fingerprint comparisons, predating automation, and are definitely not euphonic in this community.

The movement toward True Accept Rate (TAR) and other metrics also is out of alignment with identification searches where there are high rates of matching for certain classes of subject system pairs (e.g., criminals in a criminal justice AFIS), and low rates for others (e.g., citizens enrolling for voter registration). For years AFIS system managers have used straightforward metrics:

AFIS systems <u>matcher performance</u> metrics:

- Missed Matches (TP)
- Missed Candidates (LT)
- False Matches (TP)

Percentage of TP searches requiring human review

The related <u>human performance</u> metrics:

Missed Matches when in candidate list

False Matches.

Another challenge is to understand the statistics of fingerprint search results. For instance, it is known from CJIS observation that approximately 69 percent of all persons arrested are recidivists. Historically, about 12 percent of applicants will have a criminal history and thus might be matched in IAFIS. However, this mixed-use model can lead to potentially dangerous conclusions if the statistics are not understood and interpreted incorrectly. For instance, the fact that *the likelihood of a person being arrested today already having a criminal record is 69 percent* **does not imply that** *69 percent of previously arrested persons will be arrested again*, in fact it offers no insight into the likelihood of a criminal being re-arrested.

2.12.3 NIST Testing and Performance

In the aftermath of 9/11, the Patriot Act of 2002 had a profound effect on the growth of the biometric industry by requiring improved verification and identification at borders, airports, government facilities, and the inclusion of new groups of persons requiring background checks. This new operational demand has led to the development of new biometric technology applications for new biometrics customers.

The criminal justice community has based its standards and implementation on ANSI/NIST activities for 20 years. After 9/11, the DoD started using biometrics extensively in Afghanistan and Iraq. DoD's needs are a unique set of requirements and applications that are reflected in their direct participation in the various standards bodies and their own implementation specification (DoD-EBTS) of the ANSI/NIST ITL-1.

After 9/11, ANSI/INCITS (International Committee for Information Standards) and ISO (International Standards Organization) started to enter the biometric standards field. Their biometric standards are driven more by vendors and academicians than by government end users. The INCITS Technical Committee, M1, develops standards and represents the U.S. at certain international standards bodies when they are deliberating biometric standards.

It is important to note that a series of ANSI/INCITS data interchange standards were developed concurrently with, and have recently been moved to, their counterpart international standards. While NIST and INCITS/M1 represent the U.S. at ISO standards meetings, the Criminal Justice community is heavily invested in NIST Information Technology Laboratory (ITL) when it comes to currently adopted standards and best practices to ensure accuracy and interoperability. Historically, Criminal Justice standards have emerged at the practitioner level and the advantages of international standards is not clear in all situations. Some of the international standards lack robust conformance aspects such as the EBTS guidelines for implementation of the ANSI/NIST standards. However, as biometric technologies proliferate internationally the FBI should be prepared to influence or augment these standards as conformance aspects become more available and adopted.

NIST has undertaken an active role in biometric product testing evaluation as manifested in a series of vendor tests, Software Development Kit (SDK) tests, and challenge evaluations. These tests include fingerprint, face, iris, speaker, and multi-biometric using large, university collected, data sets.

The introduction of NIST testing provides AFIS managers with information from a neutral third party. NIST can measure vendor claims and provide simulation and modeling results where the same test data baseline was used for all products. The resultant reports document comparable performance metrics from identical scenarios. To date these tests have been oriented almost exclusively toward non-forensic use cases, which somewhat limits their usefulness to the large-scale tenprint AFIS community. These tests provide the vendors with very useful information as to how their products fared under certain test conditions (e.g. single finger verification) against the competition.

The NIST testing to-date has proven to be useful, contentious, and limited – all at the same time. Some tests were limited to single finger testing because they were focused on specific application environments. Others were contentious because at least one iris algorithm designer correctly pointed out that by lowering quality so they could measure some false matches the true error rates was compromised[16]. But it is clear that these tests have been instructive and ground breaking in approach.

While some tests were run five years ago and the algorithms under test have all been upgraded or replaced, they are worth listing and referencing. Note that supplemental results are being reported on the NIST website from time to time.

MINEX (discussed below) is a program of NIST-coordinated development efforts aimed at improving the performance and interoperability of core implementations of the INCITS 378 and ISO/IEC 19794-2 fingerprint minutia standards.

MINEX 04–Minutiae Interoperability Exchange Test 2004 [17]

MINEX Performance and Interoperability of the INCITS 378 Fingerprint Template NISTIR 7296

The tests led to some improvements in the specificity of ANSI/INCITS 378. Tests showed that implementations of 378 by most vendors would be sufficient for verification tasks. 378 was used in establishing an initial compliance for the PIV program.

The Minutiae Interoperability Exchange Test (MINEX 04) was to determine the feasibility of using minutiae data (rather than image data) as the interchange medium for fingerprint information between different fingerprint matching systems for the PIV card verification application. MINEX 04 was designed to evaluate whether various populations and combinations of enrollment and verification templates from different vendors will produce successful matches when using matchers from other vendors.

Ongoing MINEX–Continuing testing of INCITS 378 interoperability

---

[16] John Daugman, October 2007, Flat ROC Curves, Steep Predictive Quality Metrics: Response to NISTIR-7440 and FRVT/ICE2006 Reports.

[17] Minutiae Interoperability Exchange Test (MINEX), http://fingerprint.nist.gov/minex/

Upon completion of the MINEX evaluation, a submitted product is considered MINEX-compliant If it meets the performance criteria defined by NIST, it is listed on the NIST website as suitable for use in the PIV Program.

The Ongoing MINEX test is a continuing evaluation of the INCITS 378 fingerprint template and its use as a common format across vendor technologies. The test program has two mandates:

- To provide measurements of performance and interoperability of core template encoding and matching capabilities to users, vendors, and interested parties.
- To establish compliance for template encoders and matchers for the United States Government's PIV program.

The test follows the approach of NIST's MINEX04 test.

The Ongoing MINEX program evaluates template encoding and matching software submitted to NIST in the form of a Software Development Kit (SDK) library. This SDK must implement the MINEX Application Program Interface (API) specification available on the NIST site. This involves the submission of an SDK that provides functionality to create MINEX-compliant templates based on individual fingerprint images.

MINEX II–An assessment of Match-on-Card technology

MINEX II Performance of Fingerprint Match-on-Card Algorithms Evaluation Plan NIST Interagency Report 7485

The results showed that the best implementations on-card were as accurate as those performed off-card.

MINEX II is the part of the MINEX program dedicated to the evaluation and development of the capabilities of fingerprint minutia matchers running on ISO/IEC 7816 smart cards.

FpVTE–Fingerprint Vendor Technology Evaluation[18]

Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report Summary of Results NISTIR 7123

The FpVTE demonstrated that the variables that had the largest effect on system accuracy were the number of fingers used and fingerprint quality.

The Fingerprint Vendor Technology Evaluation (FpVTE) 2003 was an independently administered technology evaluation of fingerprint matching, identification, and verification systems.

[18] Fingerprint Vendor Technology Evaluation (FpVTE), http://fpvte.nist.gov/

FpVTE was designed to assess the capability of fingerprint systems to meet requirements for large-scale and small-scale, real world applications. FpVTE 2003 consisted of multiple tests performed with combinations of fingers (e.g., single fingers, two index fingers, four to 10 fingers), and different types and qualities of operational fingerprints (e.g., flat livescan images from visa applicants, multi-finger slap livescan images from present-day booking or background check systems, or rolled and flat inked fingerprints from legacy criminal databases).

ELFT–Evaluation of Latent Fingerprint Technologies[19]

Summary of the Results of Phase I ELFT Testing 24 September 2007

NIST is conducting a series of tests for evaluating the state-of-the-art in latent fingerprint matching. This testing will quantify the core algorithmic capability of contemporary matchers with the goal of providing automated assistance to latent examiners. The testing is using fully automated software-only implementations in a "lights out" environment. A subset of searches is being conducted with human markup of the input latent images to help identify algorithmic limitations. Initial testing includes only single-finger latent searches; multi-finger latent searches may be investigated in subsequent tests.

The initial test (Phase I) has been completed; aggregate results are available on the NIST website. Phase I was a proof of concept that demonstrated automated feature extraction from latent images, and the ability to match those features against enrolled tenprint backgrounds and produce candidate lists of manageable size.

Phase II testing commenced December 2007. It expands on Phase I through the use of improved software and larger data sets to give refined estimates of capability. Performance will be explored at both 500 and 1000 ppi, with and without supplementary Regions-of-Interest (ROI) markup. Phase II is limited to those participating in Phase I.

SlapSeg04 - Slap Fingerprint Segmentation Evaluation 2004[20]

Slap Fingerprint Segmentation Evaluation 2004 Analysis Report: NISTIR 7209

Through SlapSeg04, NIST demonstrated that improvement in image quality is needed for accurate segmentation and that the errors due to poor segmentation are large enough to significantly decrease TARs for flat-to-rolled and flat-to-flat matching.

The Slap Fingerprint Segmentation Evaluation 2004 (SlapSeg04) was conducted to assess the accuracy of algorithms used to segment slap fingerprint images into individual fingerprint images. Thirteen slap segmentation applications from ten different vendors were evaluated using data from seven government sources. The source of data, the segmentation software used, and the

---

[19] Evaluation of Latent Fingerprint Technology (ELFT), http://fingerprint.nist.gov/latent/elft07/phase1_aggregate.pdf

[20] http://fingerprint.nist.gov/slapseg04/index.html

scoring criteria used each had a significant impact on accuracy. The most accurate segmenters produced at least three highly matchable fingers and correctly identified finger positions in 93 percent to over 99 percent of the slap images, depending on the data source. The data source had a greater effect on success rate. Most segmenters achieved comparable accuracies on the better quality data, but there were significant differences among segmenters when processing poor quality data. Some segmenters can identify many, but not all, problem slaps: failure rates could be cut substantially by allowing some of the slaps to be recaptured or rejected.

SDK testing[21]

NISTIR 7249 (July 2005) Two Finger Matching with Vendor SDK Matchers

Through the SDK test, NIST determined that half of all vendors have reasonably accurate algorithm matchers; and combining two fingers provided very effective one-to-one verification for the U.S.-VISIT program.

A lower scoring, single-finger matcher can make significant improvements by using two fingers and be competitive with the better single-finger matchers. It appears that the higher performing single-finger matchers will be better than two-finger matchers at extreme performance points (i.e., TAR of 0.998).

NISTIR 7221 (April 2005)–Studies of One-to-One Fingerprint Matching with Vendor SDK Matchers

One major test result demonstrates that NIST in-house testing using vendor-supplied biometric software (SDKs) is a practical, accurate, and cost-effective alternative to public competitions such as FpVTE. Once the SDK specification was written, the interaction between NIST and the vendors worked effectively. Comparison with the medium-scale test shows that similar accuracy results and better speed results can be obtained using SDK testing. The process is also more cost-effective than public competitions.

Each vendor's performance and ranking on the SDK and FpVTE tests were compared. Only one vendor performed with significantly lower accuracy on the SDK test. This vendor was not one of the three highest ranked vendors in FpVTE. All other vendors had similar performance and ranking. This testing provides independent confirmation that the systems used in FpVTE contained substantially the same algorithms as discussed in this report.

Results show there are SDKs that perform consistently well across all data sets. This level of performance results in lower matcher speeds. Experimentation with the Ohio data set demonstrated that if the data quality is good enough, a faster matcher could do as well as the slower matchers. Also, thumbs and index fingers performed equally well on the high quality Ohio data set.

---

[21] http://fingerprint.nist.gov/SDK/

2.12.4 Test Databases

NIST has created several Special Databases (SD) for testing. Vendors and the FBI have larger sets of mated pairs that should be made available to the researcher community by the actual data owners. The FBI's APB would be an appropriate body to foster this open, scientific approach to information sharing. The results would be more and better research likely leading to innovative algorithmic improvements.

Table 2-6. NIST Special Databases

Special Database	Title
SD 4	NIST 8-bit Gray Scale Images of Fingerprint Image Groups
SD 9	NIST 8-Bit Gray Scale Images of Mated Fingerprint Card Pairs.
SD 10	NIST Supplemental Fingerprint Card Data (SFCD) for NIST Special Database 9
SD 14	NIST Mated Fingerprint Card Pairs 2
SD 24	Digital Video of Live-Scan Fingerprint Data
SD 27	Fingerprint Minutiae from Latent and Matching Tenprint Images
SD 27a[22]	SD 27 with 1000 ppi images
SD 29	Plain and Rolled Images from Paired Fingerprint Cards
SD 30	Dual Resolution Images from Paired Fingerprint Cards
NBIS	NIST Biometric Image Software
PCASYS	NIST Pattern-level Classification Automation System for Fingerprints
NFIS2	NIST Fingerprint Image Software Version2

Other sources of test data include the ability to generate synthetic fingerprints. **SFinGe** (**S**ynthetic **Fin**gerprint **Ge**nerator) is a method for the generation of synthetic fingerprint images. Developed in Italy by the University of Bologna, SFinGe can rapidly create large (e.g., 10,000) finger image databases in a few hours. This process follows four steps**:** directional map generation; density map generation; ridge pattern generation; and noising and rendering the image.[23] SFinGe eliminates the

[22] SD 27a is one of several names under discussion for this Special Database at the time of this writing.

[23] Fingerprint Generation, Biometric System Laboratory, DEIS, University of Bologna.

expense and time to enroll large numbers of subjects. However, the creation of SDs by NIST has provided a set of finger images that are more consistent with those in real-world databases.

A new SFinGe feature is the capability to reconstruct fingerprints images from templates. They can generate a family of fingerprint images, each with ridge flows that contain features and minutiae found in a given template. While useful for testing, the implications for use in fraudulent login and access control systems are enormous.

2.12.5 Test Data Shortfalls

With the migration to multimodal systems, there is a parallel need for collecting and sharing multimodal sample data from test subjects. This test data needs to include samples from each biometric modality for tens of thousands of subjects. Samples must be collected for each subject at multiple times, at different hours, and using different capture devices and environmental conditions. The availability of this class of data is becoming critical to the research community and will be required to benchmark multimodal AFIS subsystems.

DHS developed the Multimodal Biometric Application Resource Kit (MBARK) in partnership with NIST. This multimodal data collection platform integrates information from multiple sensors into a single software package. The FBI established a similar platform referred to as BIO-COP. Neither has been extensively tested beyond the laboratory.

2.13 Forensic Capabilities

In the 1993 Daubert vs. Merrell Dow Pharmaceuticals decision (509 U.S. 579), the U.S. Supreme Court outlined a test for scientific evidence to be admissible in court.. But, as the Court stated in Daubert, the test of reliability is ‘flexible,’ and Daubert’s list of specific factors neither necessarily nor exclusively applies to all experts or in every case. The law grants district courts latitude similar to federal courts when determining reliability of technical evidence.[24]

The FBI and latent fingerprint community are seeing legal attacks with the Daubert challenges more frequently. The first one was raised successfully (albeit briefly) in the case of the United States of America vs. Criminal No. 96-00407, Byron C. Mitchell. That challenge was lodged in late October 1998.

Since that time, the government maintains that the Analysis, Comparison, Evaluation, Verification (ACE-V) methodology is sound, however, there are limited scientific studies to determine the error rates of human practitioners. To be purely scientific, there must be error rates for generation of candidate lists that consider image quality, quantity, and other variables. Then these rates will have to be aligned with studies of human application of ACE-V across latent images of variable size, quality, number of minutiae, and other variables that may be difficult to quantify. Additional

[24] See General Electric Co. vs. Joiner, 522 U. S. 136, 143 (1997).

studies are being undertaken in this area to re-enforce, inform, or refine the best implementation of ACE-V.

When compared with forensic fingerprints, DNA has an extremely strong scientific basis. However, forensic DNA results have been questioned in some instances as they may pertain to mixed samples and small class sets. While these are special cases, they serve as reminders that forensic capabilities cannot reach beyond the sciences that establish the individuality of the physiological or biological trait in open populations. To this end, fingerprint minutiae in forensic fingerprints do occur as consistently as alleles do. DNA measures the presence of alleles that, if not present in a sample, preclude using that test; this presence or absence is something that can demonstrated and directly interpreted as inclusion or exclusion. Latent fingerprints, at times, require skilled examiners to locate minutiae and other image features from a low quality image. Unlike alleles, minutiae do not have pre-determined positions in a genetic sequence but are located in accordance with ridge formations. Locating and labeling minutiae positions in forensic prints and images requires clean exposure of ridge flow details (and absence of dirt, smudges, and other obfuscating factors).

There are recorded instances of well-qualified examiners making mistakes (i.e., Shirley McKie and Brandon Mayfield). In the *Wall Street Journal*, October 7, 2005 there was an article about a study performed by academicians in the UK[25]. Part of the story is provided below:

> **FINGERPRINT MATCHES COME UNDER MORE FIRE AS POTENTIALLY FALLIBLE**
>
> By Sharon Begley
>
> Fingerprint examiners would probably be happy if they never heard the name "Brandon Mayfield" again, but for researchers who study the scientific basis for fingerprint identification Mr. Mayfield is the gift that keeps on giving.
>
> Mr. Mayfield is the Portland, Ore., lawyer and Muslim convert whose prints the FBI matched to those taken from a suspicious bag near one of the 2004 Madrid train bombings. When Spanish police insisted the prints didn't match Mr. Mayfield's–and eventually linked them to an Algerian living in Spain–the FBI conceded the error and apologized to the jailed Mr. Mayfield.
>
> Since such an error is supposed to be impossible (an FBI handbook says, "Of all the methods of identification, fingerprinting alone has proved to be both infallible and feasible"), the case has achieved a certain notoriety. So when scientists recently tested fingerprint IDs, they told examiners one set of prints were from Mr. Mayfield and the other set from the Madrid bombings. "We told them we were trying to understand what went wrong in that case," says Itiel Dror of Britain's University of Southampton, who did the study with student David Charlton. "Could they please look at the prints and tell us where the examiners had gone wrong."

[25] January/February 2006, California Identification Digest, Volume 6, Issue 1, pg. 13.

> One examiner said he couldn't tell if the pair matched. Three said the pair did not match and helpfully pointed out why. The fifth examiner insisted the prints–notorious for not matching–did match.
>
> Give that one a gold star.
>
> Unbeknown to the examiners, the prints were not from Madrid and Mr. Mayfield. They were pairs that each examiner had testified in recent criminal cases came from the same person. The three who told the scientists that their pair didn't match, therefore, reached a conclusion opposite to the one they had given in court; another expressed uncertainty, whereas in court he had been certain. Prof. Dror will present the study later this month at the Biometrics 2005 meeting in London.
>
> A study this small would hardly show up on scientists' radar screens. But it comes at a time when traditional forensic sciences–analysis of bite marks, bullets, hair, handwriting, and fingerprints–are facing skepticism over the validity of their core claim: that when two marks are not observably different, they were produced by the same person or thing.

More important was the reaction after the rejection of fingerprint testimony in the 2007 case of the State of Maryland vs. Bryan Rose. At that point, "insiders," such as the editors of the UK Fingerprint Society's *Fingerprint Whorld Journal*,[26] cried for more science and less denial when it reprinted a portion of an editorial from *Crime Lab Report*. The title and the first sentence sum it all up:

> **Many are to blame for Maryland judge's ruling**
>
> November 8, 2007 by Crime Lab Report
>
> It's a simple story about a judge who asked the right questions and didn't get the right answers. Nobody should be shocked by the outcome.
>
> In a recent decision that sent panic throughout the forensic science community, Baltimore County Circuit Court Judge Susan Souder ruled that forensic fingerprint identification was "a subjective, untested, unverifiable identification procedure. As a result, the state was precluded from admitting the testimony of a forensic scientist who identified a suspect's fingerprints on two vehicles associated with the murder of a local store merchant. The defendant, Bryan Rose, could face the death-penalty if convicted.
>
> Prosecutor Jason League said in court that the ruling "virtually overturns 100 years of jurisprudence with respect to the admissibility of latent fingerprint evidence."
>
> But in her 32-page decision, Judge Souder issued a stern reminder that judges in previous Maryland cases, where fingerprint identifications were judged admissible, "were not presented with proof of erroneous identifications which refute the infallibility claimed by the State's expert."
>
> In the case against Bryan Rose, defense attorneys, without objection from the state, introduced a 220 page review of the FBI's highly publicized misidentification of a Muslim lawyer, Brandon Mayfield, in the investigation of the 2004 Madrid train bombing that killed 191 people. Mayfield, who was living in Oregon, was arrested by the FBI even after Spanish investigators disagreed with the fingerprint match.

---

[26] December 2007, Vol. 34 No.130 of Fingerprint Whorld.

> Faced with compelling evidence of a significant error in a major terrorism case, Judge Souder was understandably suspicious of testimony offered by an FBI expert who claimed that the comparison of fingerprints has no potential for error. The methodology, he testified, "is infallible".

The following sections of the Crime Lab editorial were not provided in the Journal. The entire Crime Lab editorial is available on the Web.[27]

> *Crime Lab Report* respectfully disagrees with Judge Souder's decision, but acknowledges the awkward position in which she was placed by the state's fingerprint expert. We further sympathize with Judge Souder for the blame she will receive from critics throughout the country, including forensic scientists who might be wise to tone-down their rhetoric.
>
> Historically, forensic scientists have openly argued that the self-correcting mechanisms of our adversarial system of justice are what should be relied upon to weed out junk science and unreliable experts. In fact, during the early years of forensic science accreditation, stubborn voices from within the profession argued that accreditation was an unnecessary and intrusive process that should be reserved for the courtroom, since judges and trial lawyers are ultimately responsible for evaluating the reliability of evidence.

The Bryan Rose case was a capital one. The Judge considered the nature of the case in deciding the motion (discussed below in the ruling) as a critical factor in her consideration. Her decision[28] starts out:

> Pending before the Court is Defendant's Motion to Exclude Testimony of Forensic Fingerprint Examiner and Request for a Frye Hearing (paper 100000, "Motion to Exclude"). The State opposed the Motion. The Court granted the request to have a Frye hearing and the hearing was held May 29 and 30, 2007. Each side presented testimony of one expert to support its position. For the reasons set forth herein, the Court will grant the Motion because the State did not prove in this case that opinion testimony by experts regarding the ACE-V method of latent print identification rests on a reliable factual foundation as required by MD Rule 5-702.

With movements to standardize third-level detail, improve encoders, establish better training, and provide additional scientific studies and error analysis–the fingerprint community should be well prepared to deal with these legitimate challenges. The legal system is designed to allow accused persons and their attorneys the opportunity to review (and question) incriminating evidence; attorneys have come to use Daubert criteria as a checklist if there are compounding factors. The FBI must take a lead in documenting and re-enforcing the scientific underpinnings of forensic fingerprint matching.

2.13.1 Interoperability

As early as 1996 and 1997, the IAI tested the cross-jurisdictional use of FBI-EBTS image-based records between booking stations and operational AFIS systems. These demonstrations/tests pre-

---

[27] http://www.crimelabreport.com/library/pdf/11-07.pdf.

28 State Of Maryland V Bryan Rose: In The Circuit Court For Baltimore County Case No.: K06-0545.

dated the operational use of IAFIS and the CJIS Wide Area Network (WAN).[29] The goal was to remotely search already encoded latents so the receiving AFIS would not have to employ scarce labor to encode them and so a jurisdiction with another vendor's AFIS could still search them. The earliest start to interoperability was the 1986 ANSI/NBS-ICST 1-1986 American National Standard for Information Systems–Fingerprint Identification–Data Format for Information Exchange. The introduction to the standard sums up the goal:

> "This standard provides methods for agencies that use automatic fingerprint identification systems obtained from different suppliers to exchange fingerprint information. The standard provides for the exchange of any combination of descriptive textual information, extracted feature (minutiae-based) information, or fingerprint image information for direct input to a remote automated fingerprint identification system processor."

Unfortunately, the Type-9 representation was not very robust and the standard was neither tested nor used operationally. It was not until 1992/1993, with the anticipation of IAFIS, that the standard was updated. With IAFIS, the concept of operations was that local agencies would search latents on the own AFIS, then submit them to their state or regional AFIS and, if there was still no match, to IAFIS. To save time required for re-encoding the latents to be compatible with the state and federal systems, the FBI developed the Universal Latent Workstation that permits the local latent print examiner to search locally, re-encode (almost automatically) for the state system, and then again for IAFIS.

The notion of AFIS interoperability, in particular latent print interoperability, has become an area of interest again for several reasons. Adjacent political areas frequently do not have access to the neighboring AFIS database where there might be criminal records that were not submitted to the FBI. (Until recently, the FBI would not retain fingerprint records unless they were for "category" crimes. Now they are willing to store all records, if asked by the submitter.) If the perpetrator has no criminal record in the locale of the crime, but has an extensive record on the adjacent AFIS database, the likelihood of identification locally through the use of latent prints is marginal. While access to the CJIS database is possible, the subject might not be there; many states still do not submit many latents to IAFIS for searching. IAFIS should be fully exploited before the request for cross-jurisdictional searching is addressed. Yet, there are cases where the importance of the crime warrants searching all available repositories.

At the direction of Congress, the National Academies have undertaken a two-year study entitled, "Identifying the Needs of the Forensic Sciences Community." Among the eight areas of interest is an examination of the Interoperability of Automated Fingerprint Information Systems. The project began in September 2006 and is expected to be completed in summer of 2008.[30]

---

29 Automated Fingerprint Identification Systems (AFIS) , Komarinski, Higgins, Higgins, Fox, Elsevier Press 2005, Appendix B.

30 http://www8.nationalacademies.org/cp/projectview.aspx?key=48741.

Many organizations and individuals appeared before the Committee. In addition to providing background information, the International Association for Identification issued a position paper[31] to the National Academies on September 19, 2007 that included the following:

Recognition that AFIS technology is an excellent tool for searching prints

Recommending that the technology should be fully exploited

Noting the final latent print identification decision still requires a competent examiner.

The IAI further recommended funding national legislation to advance the use of latent and recorded print services, as well as other forms of impression evidence, via improved and increased automation, interoperability, and broader connectivity.

The National Institute of Justice (NIJ) has also weighed in on the issue in two areas.

NIJ funded the IAI to undertake a research project to link the New York City Police Department Latent Print Unit with the New Jersey State Police AFIS. Latent prints not solved in New York would be searched against the New Jersey database. A variety of issues, including installation delays, incompatibility of systems versions from the same vendor, legal and administrative challenges, and costs, terminated the project after Phase I.

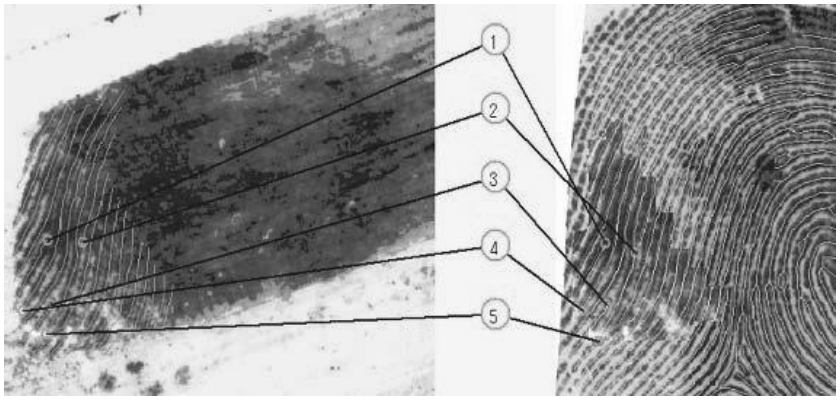
NIJ initiated an AFIS Interoperability–Experts Panel that held its first meeting in May 2008.

2.13.2 Use and Limitations of Latent Prints

Prior to the introduction to AFIS technology, latent print matching was limited to searching file cabinets of tenprint cards of known offenders. The cards might be arranged by criteria such as crime type or geographic location of crime, to help limit the search to "likely" suspects. Comparison of crime scene lists to "elimination prints" from first responders represented a large part of latent print processing. AFIS systems changed the latent print business dramatically.

Latent fingerprint examiners now can search databases containing millions of fingerprint and palm print records. They are aided by advanced image processing techniques and computer systems. Ultimately, the latent print examiner determines the match.

[31] September 19, 2007, IAI Positions And Recommendations To The National Academies Of Sciences Committee To Review The Forensic Sciences.



Left: Latent print Right: Rolled impression

Figure 2-9. Example of Latent Print Minutiae Matching[32]

The corresponding five minutiae from the latent (left) are identified on the rolled impression "mate" (right). These minutiae are connected via arrows to demonstrate the reason for individualizing the two impressions to the same subject.

Latent print examination ultimately requires the decision of a latent print examiner who determines if the latent print image matches a known record (i.e., a previously enrolled encounter). The use of AFIS systems has expanded the opportunities for a match with large databases of enrolled records and electronic search capabilities. Latent Print Examiners reliably make positive latent print identifications with:

- Appropriate training
- Appropriate experience
- Appropriate ability
- Using the scientific procedure of ACE-V (**A**nalysis, **C**omparison, **E**valuation, **V**erification).

2.13.3 Use and Limitations of Hand/ Palm prints

The success of finger image capture devices provided a mechanism for the capture of palm prints. More AFIS system managers are purchasing palm capture devices when they upgrade their livescan devices. The addition of palm records requires more storage and network capacity to collect and submit these images.

---

[32] November 2006, NISTIR 737 Summary of NIST Latent Fingerprint Testing Workshop, pg. 13.

Palm prints are generally captured in a "day one forward" process starting with the addition of the capability to capture them and the capability to search them. Some agencies have repositories of palm impressions–not always centralized or organized with the associated tenprint files. When a palm matching capability is added, managers will have to decide if the palm prints should be gathered to a central site, converted, and features extracted or not; the image may be captured in its entirety or in two overlapping images–the upper and lower palm prints. The images are not "stitched together" but remain separate and sharing a common area (i.e., the interdigital area). In addition, the writer's palm is typically captured and encoded.

NGI will provide a palm service that will serve as a National Palm Print Repository.[33] The repository will receive, search, and store palm prints, including Major Case prints as shown below.

Figure 2-10. Example of CJIS Major Case Cards

2.13.4 Use of Flats or Plain Impressions in Latent Print Searches

In the analysis of the first 1,805 latent print identifications with their new AFIS that searched rolled and plain impressions, 224 (12.4 percent) were made *only* on the flat or plain impression and not on the rolled impression. This offers tremendous opportunities to increase the number of latent print identifications when the plain impressions are included in the search database. Many AFIS systems procured since that time (e.g., DoD ABIS and DoD Iraqi National AFIS) have mandated this capability. By including plain impressions in a latent print search, there is a documented increase of identifications. If latent searches are consolidated, there is minimal impact to the latent print examination process.

---

[33] B. Scott Swann, April 5-6, 2006, NIST Latent Workshop, Needs & Applications of Latents at FBI/CJIS.

Table 2-7. Latent Idents (Hopper and LAPD, June 2005)

Finger Image Mated	Number of Idents	Percentage of Idents
Flats only	224	12.4
Rolls only	504	27.8
Both Flats and Rolls	1,079	59.8
Totals	1,805	100

2.13.5 Use of Fingerprints and Other Biometrics in Disasters and Mass Evacuations

As evidenced in the SEARCH report regarding record checks following Hurricane Katrina[34] natural disasters and other situations of mass evacuations will increasingly rely on biometrics to identify displaced persons. Identification services may be necessary for access to shelters, emergency services, and identification of the deceased. When the disaster causes the movement of persons across state borders, CJIS may be asked to assist in determining identification.

Among the displaced will be criminals, sex offenders, and wanted persons who are of interest to law enforcement agencies; they must not be permitted to anonymously commingle with potential victims.

The report identifies a number of factors that should be addressed when crafting policies governing criminal history record checks during periods of mass relocations. They include:

- Creation and issuance of verifiable identification and emergency credentials
- Privacy protections of displaced persons/survivors
- Costs
- Name-based identification checks such as phone books to see if a person really lived in the affected area
- Non-criminal background check guidance for relief managers
- Recommended minimum record search for classes of persons (e.g. victims, volunteers).

2.14 Vulnerabilities

Section not for public release.

[34] Report of the National Focus Group on Emergency Housing and Criminal Record Checks: Hurricane Katrina Experience: SEARCH, The National Consortium for Justice Information and Statistics, September 2007.

2.14.1 Errors Introduced by Equipment or Operator

Image capture equipment such as livescan devices must be certified to Appendix F of the EBTS if they are to be used in transmitting images to CJIS. Newer livescan devices can capture at higher resolution (1000 ppi) and are claimed by the manufacturer to be self-calibrating. Sensors measure the amount of light and adjust intensity to correct any degradation over time. When the device no longer performs to specifications, it should cease to operate and display an error message.

In spite of technical self-corrections, other actions can degrade the image. Excessive pressure, a dirty or smudged platen, or inattentiveness by the operator are examples of errors that can be introduced.

2.14.2 Frontal Attack on the System

Section not for public release.

2.15 Forces of Change

Forces of change in the automation and use of fingerprints occur at all facets of the identification hierarchy. Some of the internal forces driving change include the need to upgrade equipment, reduce staff/increase productivity, and take advantage of newer programs and features. Some of the external forces for change include increased and divergent demands on the current systems (e.g., new laws mandating new services, evolving standards, and new technology).

As the premier national repository of biometric information, CJIS faces many forces of change from state and other federal agencies. The need to accept more searches with less than ten rolled images from more investigative agencies typifies these forces.

The addition of new users and the greater demand for faster, more accurate, identifications with fewer finger images presents new challenges for NGI. The introduction of better technology (e.g. computers, encoders, and algorithms), enhanced standards, NIST test results, and recognition of current vulnerabilities will shape NGI.

The following graphic illustrates some of these forces.

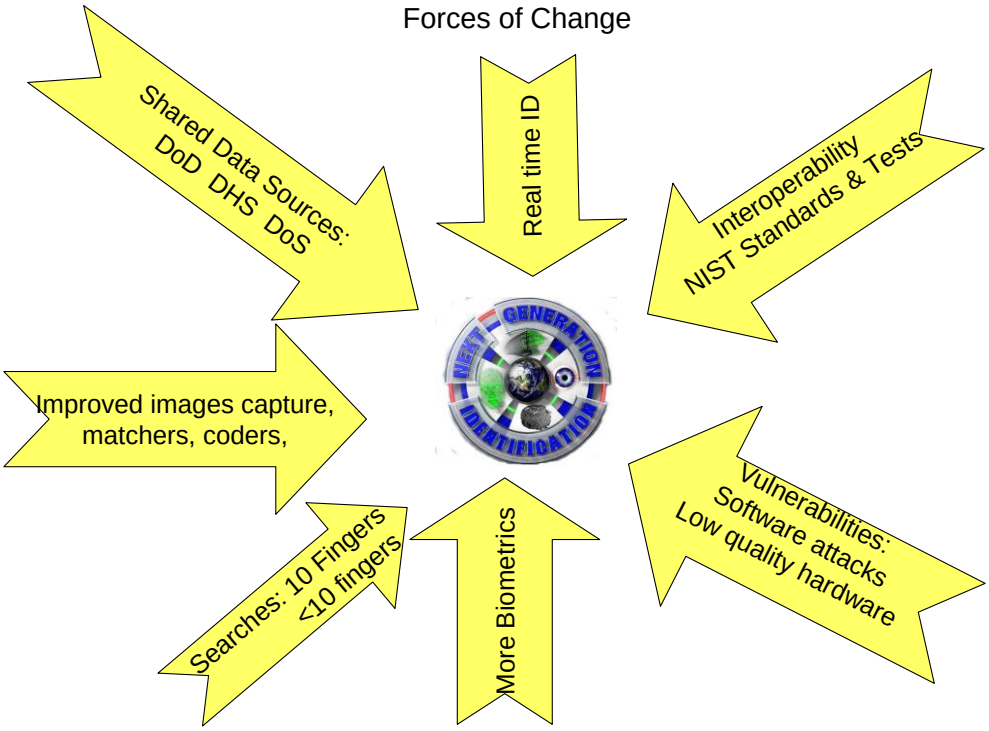


Figure 2-11. CJIS Forces of Change

State and local system administrators are also facing the need to upgrade or replace their systems. Many operational livescans capture at 500 ppi, but are being replaced with 1000 ppi models; tenprint identification may have limited lights-out capability; and the latent print processing is almost entirely manual. The system coders and matchers are not the latest available. There may be some interaction with another agency such as the Department of Corrections and perhaps some access to CJIS through the ULW workstation. These forces for change cannot be addressed with the older systems.

The following graphic shows a conceptual architecture for a typical state or local AFIS system.

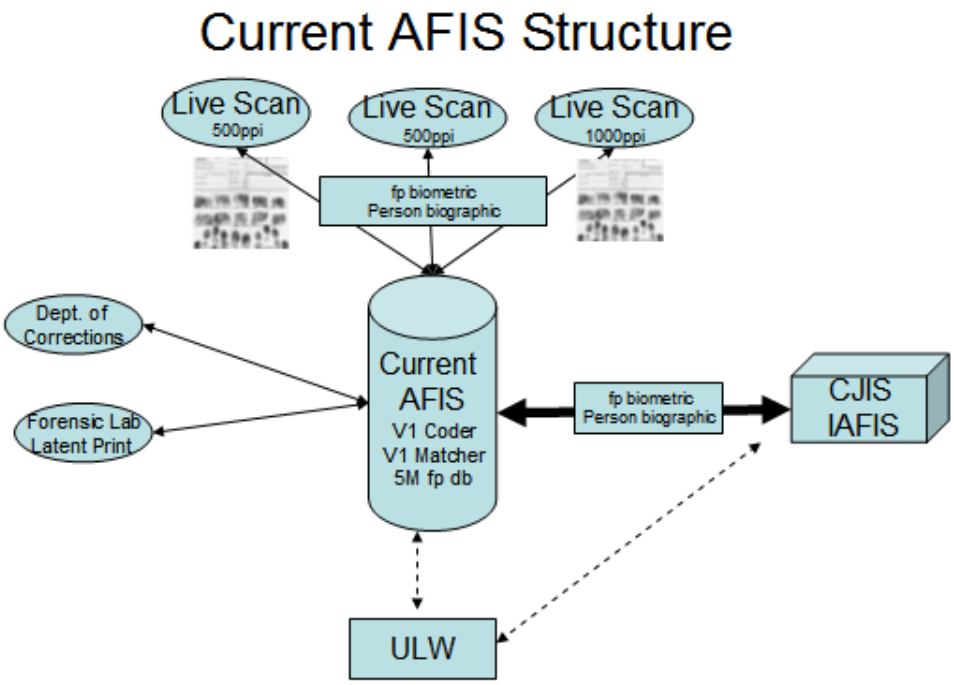


Figure 2-12. Current AFIS

2.15.1 Replacement Cycle

AFIS Systems are upgraded or replaced for various reasons, including:

- Accuracy: Improved accuracy, as new systems typically offer better encoding and matching, thus improving public safety
- Cost-effectiveness: Obsolescence, which occurs when parts are no longer available or maintenance costs exceed the cost of a new system
- Functionality: New functionality not available on current technology (e.g., palm or foot latent searching, Mobile ID interfaces, Real Time searching, and connectivity to other agencies)
- Productivity: Support increased personnel productivity or reduced personnel expenses while contending with growth in transaction rates.

- Performance: Near real-time response for searches against critical files such as Watchlists and wanted person files.

AFIS vendors will typically write maintenance agreements for three to five years after the initial installation and acceptance testing; upgrades to installed systems occur earlier than three years. Upgrades may include more robust matchers and coders, as well as fixes to problems reported from operational use.

The advantage to upgrading systems is that newer biometric technologies and access to CJIS through ULW are coming to agencies that own a modern AFIS. These upgrades could have a significant impact on CJIS as more latent prints are searched through the ULW following state and local AFIS upgrades. After five years, the systems become less cost-efficient, unless they are incrementally enhanced and upgraded with software patches, hardware replacement, and new operating system versions.

2.15.2 Centralized IT Procurement and Management

Like corporations and federal government, many state and local agencies have, over the last decade, moved to more centralized IT procurement and management than they had in the 1980s and early 1990s. As a result, state and local agency IT shops (rather than biometrics experts and system users) are increasingly driving AFIS system design and implementation. This trend has the benefit of integrating AFIS technology within the overall electronic data processing architecture of the identification agency and related IT agencies. Because it positions agency IT people to talk with the vendor's IT people, this approach can enable vendors to better understand the technical issues between the identification agency and the vendor.

However, without strong input from the biometrics experts in the agency's identification shop, a newly acquired AFIS system may not meet current and projected identification needs. If acquisition decisions are not informed by biometrics and customers' operational needs, the new identification system may disappoint users and fail to provide a foundation for new functionality.

A particular problem in acquisition is the tendency to focus on simply replicating functionality from legacy systems. If identification agency staff do not interact with the FBI's NGI activities, they think in terms of their current AFIS, not a multimodal ABIS. A significant outreach and education process must occur to demonstrate the advantages of multimodal capture and processing to the IT managers, budget officers, purchasing departments, and other key decision makers who can affect functional priorities, resource levels, acquisition timing and schedules, and other acquisition choices.

System managers can increase their awareness of these forces by participating in professional associations training conferences (e.g., International Association for Identification), trade shows, user group meetings, and NIST reports on performance.

2.15.3 Multimodal Systems

One of the strongest, and potentially the most disruptive, forces today's system managers encounter is the trend to go multimodal. In the past, identity systems focused on fingerprints. Now, AFIS systems today routinely include mug shot, palm functionality, and options for face and iris matching. AFIS managers have based their agency's identification services on fingerprints and rely on fingerprint individualization to establish and maintain identities. Managers and law enforcement practitioners have lived in a world where an identity is initially started with a foundation of a fingerprint. Now they have to deal with a world where the identity might have to be expanded in scenarios such as:

> A subsequent set of fingerprints is submitted with a facial image, and the fingerprints are individualized to the same identity. The facial image is linked to the identity.
>
> A subsequent facial image is submitted with an iris image set, and the facial image is matched to the same identity. The iris image set is linked to the identity.
>
> A subsequent set of fingerprints, a facial image, and a set of iris images are submitted and the iris images match. Before the fingerprints or facial image is linked to the identity, the other modalities (fingers and face) must be verified as matching.

The proliferation of biometric modalities means that AFIS system managers must adjust their mindsets, business processes, and technological systems to deal with identity data that may or may not be tied to a fingerprint.

When an agency starts up new operations of multimodal biometrics, they typically begin without large existing repositories of faces and known palm prints to convert. This is called a "day-forward" approach, as in "from this day forward, we will link legacy data to new data as it comes in." This approach to data migration and conversion has the advantage linking all biometrics (e.g., finger images, iris, face, and palm) to an individual at the time of processing. It is more operationally satisfactory than attempting to simultaneously convert and verify the linkage across multiple modalities for a substantial number of records. This step is necessary to assure continuity of individual identities that is biometrically, rather than biographically, based.

This day-forward process minimizes labor costs and potential errors by connecting the new biometrics to a biometric (i.e., fingerprint) already widely in use. Estimates suggest that 69 percent of arrestees' and 12 percent of applicants' fingerprints are already in IAFIS. With such a large "hit" rate, a day-forward scheme will add better images (e.g., captured at 1000 ppi) and more biometric modalities to existing identities to a substantial percentage of new transactions, while adding new modalities as part of newly established identities.

If any modality search leads to a recognition, there may be no need to continue with other biometric searches other than to verify they are mates before adding them to the repository. This step is analogous to fingerprint sequence checking. It is considered to be a "best practice" to detect malicious or innocent enrollment contamination across modalities. Contamination can occur in various ways. For example, if two different subjects' faces are submitted with a single subject's

fingerprints, the erroneous connection of face to fingerprint represents an instance of enrollment contamination across modalities.

Just as portions of the "master" or "composite" record may be replaced with better samples, other biometric modalities, such as palm prints and iris, may be added to a record if none exist. Likewise, better samples may be substituted for previously enrolled, lower quality samples.

These new modalities, combined with more automated processing, will increase the demand on CJIS and other identification service providers for fast, accurate turnaround. The transmission of palm images, face, and iris search will present significant challenges, particularly at reconciliation. The access to semi-automated, latent print searches and general access to CJIS through ULW will impact operations.

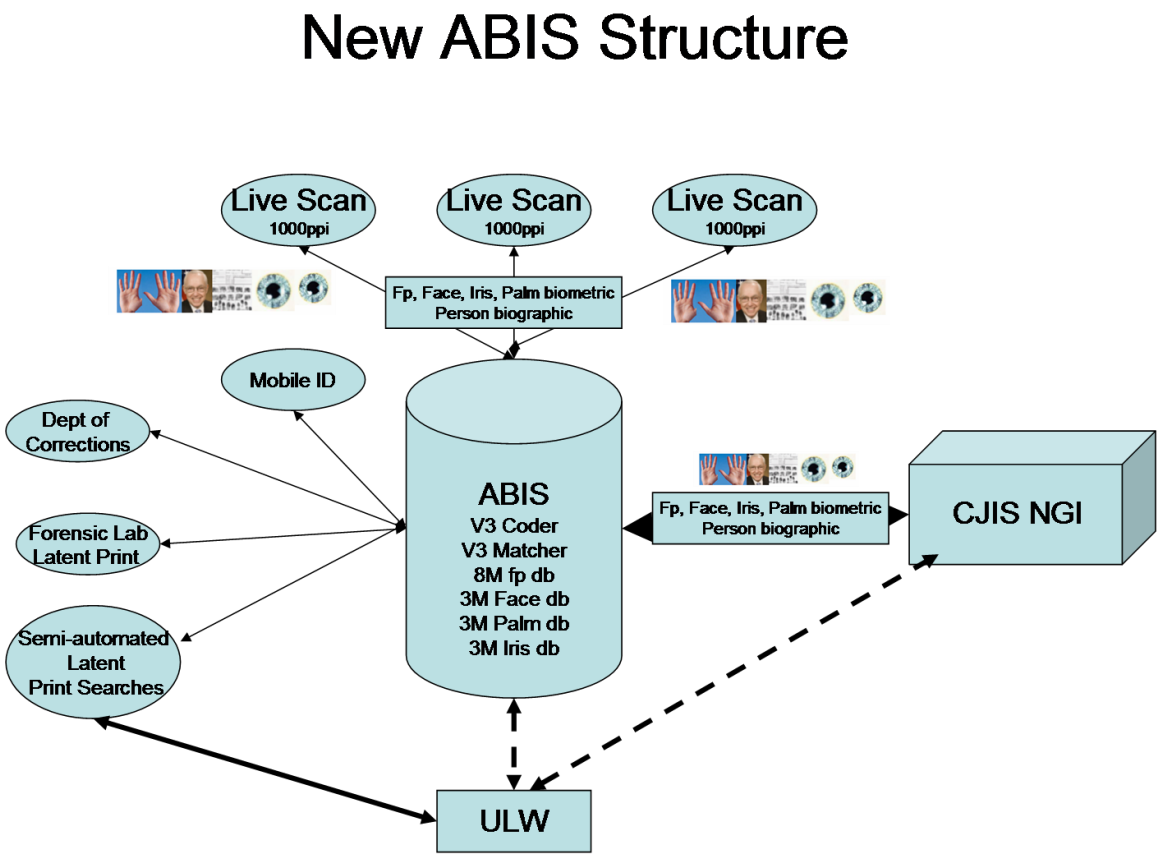


Figure 2-13. Notional ABIS Structure

As the application suite evolves into areas such as Mobile-ID, new data types will be submitted; standards, interface specifications, and training will need to adapt to these changes. As we move into multimodal, we will need facial, fingers, and iris data from the same person at the same time,

usually at enrollment or subsequent capture event (e.g., re-arrest). Therefore the current "gold standard" of rolled and sequence slap fingerprint collection needs to be expanded.

Decisions regarding the sequence of identification processing in the multimodal environment must be made. When systems potentially can retain and search multiple copies of 10 rolled finger images, 10 plain impressions, both palm prints, two iris images, and multiple facial images, a new paradigm of identity baseline will be required. The move from exclusively fingerprint-based identity to multi-biometrics will permit more applications. The fusion of results across modalities will help improve performance. However, the additional modalities complicate the collection process and require search applications to fuse technologies with quite different operating characteristics. A multi-biometric framework must also adjudicate results and generate exceptions when modality-specific results don't agree with each other.

For instance, in the presence of a very low-quality fingerprint set and good iris images, it is likely that the iris matcher will single out the correct mate and permit the fingerprint examiner to verify one candidate set or even for the fingerprint matcher to make a successful 1:1 comparison. The positive impact on productivity and accuracy will likely be remarkable. The training needs for non-fingerprint modalities have unique challenges for operation of equipment and forensic image comparisons.

Newer releases of ABIS technology may continue to reduce the need for specialized training and human intervention. For example, livescan capture devices are more reliable and less dependent on human experience than when originally introduced. In the latent print area, there is a move to semi-automated, latent print preparation and searching. This enables examiners to focus on review of candidates and declaring matches. As the expanded feature set starts to be utilized, examiners will have to perform more manual encoding and more complicated review, at least until familiarity with and confidence in the new approach is developed.

2.15.4 Fusion

Biometrics Fusion encompasses methods and techniques for using information from multiple biometric samples, modalities, or identity attributes to generate a statistical likelihood of matching that is more useful than any of the constituent information. NIST defines Biometric fusion as *"the use of multiple types of biometric data, or methods of processing, to improve the performance of biometric systems*."[35]

For years AFIS systems have performed biometric fusion in the form of tenprint matching, which is typically transparent to the users. For instance, IAFIS considers single-print matches before final results are "fused" and the system generates the final candidate list. Biometric Fusion can be achieved through several techniques that include:

---

[35] NIST Technical Report, *NISTIR 7346 Studies of Biometric Fusion*, September 2006.

- Multiple instances of the same biometric (e.g., multiple captures of the same finger)
- Multiple samples of the same modality (e.g., two or more fingers)
- Multiple modalities (e.g., fingerprints, face, and irises)
- Multiple algorithms processing the same data in sequence or parallel.

There are many ways that the results can be fused. In its 2007 report on fusion (NISTIR 7346), NIST provided a brief look at their analysis of several methods that fused scores. An excerpt from that report follows:

> Eight score-level fusion techniques were implemented and evaluated. These differed in effectiveness, in the types of training data required (if any), and in their requirements for modeling genuine and imposter distributions.
>
> • The most effective fusion techniques were Product of Likelihood Ratios and Logistic Regression, which are implementations of the theoretically optimal Neyman-Pearson Lemma. Product of Likelihood Ratios involved complex, detailed modeling of score distributions. Logistic Regression achieved similar results using a standard statistical technique. Both techniques require statistical tools, training, and a substantial amount of training data.
>
> • Techniques that were nearly as effective were product of FARs and Best Linear. Product of FARs requires modeling the non-mated (imposter) distribution, but does not require mated (genuine) data. Best Linear is a conceptually simple technique that requires joint training data, but does not require modeling of distributions.
>
> • For cases in which the input scores are of similar strengths and distributions, such as fusing two index fingers using a single matcher, the choice of fusion technique had minimal effect on accuracy.

With the move to NGI, CJIS will be in a position to move from multiple-fingerprint algorithm fusing to a broader set of fusion techniques.

2.15.5 Summary of AFIS Evolution

Understanding AFIS' evolution provides a basis for understanding the next wave of change in identification processing and management. AFIS ushered in new technologies, procedures, and challenges. AFIS replaced the old ink and rolled tenprint paper cards with livescan capturing at 500 ppi. The development of AFIS standards assured connectivity between identification bureaus and IAFIS. Appendix F and Appendix G of the EFTS provided certification for image capture devices.

The Identification staff drove the development of AFIS by working in partnership with the technical staff. Latent print processing remained primarily a labor-intensive process in the early AFIS environment. Some tenprint search functions were adapted to lights-out processing.

All of this is changing. Currently deployed livescan devices capture at 1000 ppi (four times as much information as their 500 ppi predecessors) with better image quality. NIST has developed more biometric standards and initiated testing across vendor implementation of the standards, e.g. MINEX.

Improvements in coder and matching software, combined with the improved images, enable more features to be extracted from a finger image. More tenprint searches are conducted without human intervention (i.e. lights out). Semi-automated or batch latent print searches are possible. The IT staff directs more identification system development than in the past. The use of remote search opportunities such as through ULW is increasing.

The finger image, once the only biometric that could be captured and searched, is being joined by other biometric modalities as they become cost effective, which include palm prints, face, scars, marks, and tattoos, and eventually could include collection of handwriting, iris and voice. The following graphic summarizes the changes discussed in this section.

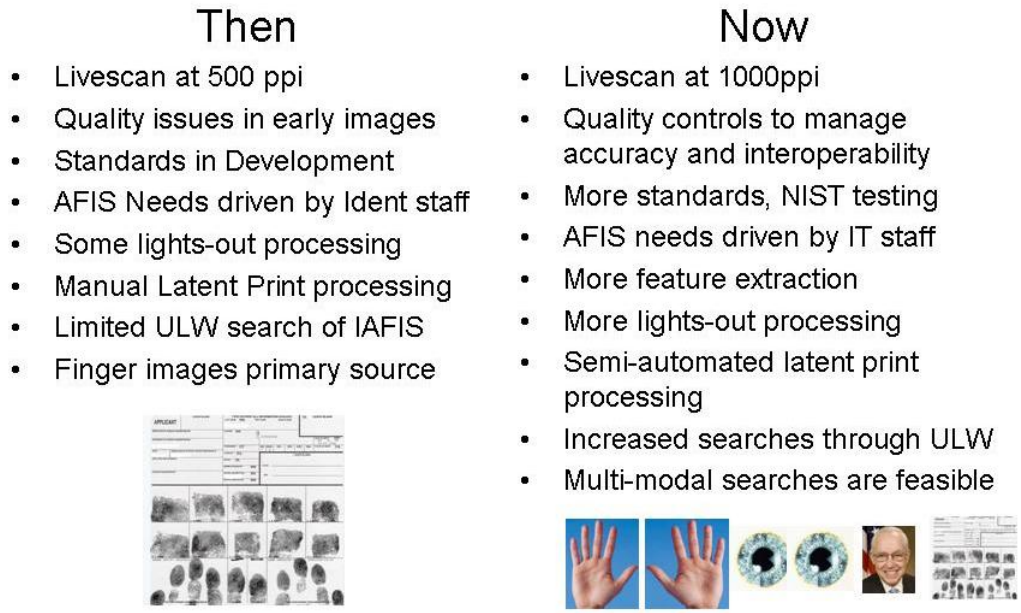


Figure 2-14. Influences on Fingerprint Technology

2.16 Technology Opportunities

No successful industry achieves a performance plateau and stops developing. Consider the financial industry, which in the 1950s was dependent on adding machines, ink, and paper to record credits and debits. With the investments in IT technology in the 1960s, managers not only improved the speed and accuracy of record processing, but offered better service to their

customers. The financial industry constantly upgrades their systems to take advantage of evolutions in account management, service, and customer demands, which are both driven and answered by technology. The nation is moving to a cashless, internet-based economy that has provided faster, better, and more complete service to the industry and the consumer.

Likewise, the identification industry migrated from the mailed submission of ink and rolled cards to the electronic transmission and receipt of finger images and other biometrics. The introduction of IAFIS marked the beginning of an evolutionary process for CJIS. The NGI will usher in another, but not ultimate, identification platform. The investments in the future are never a one-time event, but a continuum that requires planning and funding for the foreseeable future.

Fortunately as NGI starts, technology presents many opportunities for enhanced capabilities. Some of the emerging technologies that industry is embracing include:

- Virtualization of computing infrastructure
- High-performance computing environments built from cost-effective commodity hardware
- Alternate collection technologies (e.g., Ultrasonic solid state devices) particularly for Mobile ID systems
- Third level detail-based algorithms – NIST standard will harmonize the definitions – FBI will need to lead in the use by accepting these types of transactions in NGI and generating them in ULW output
- Alternate matching approaches
- Increase in transaction record size; transmission and storage of additional information content is a small price to pay for records to be retained and used for up to 80 years.
- Transition from segmenting ID-Slaps to native processing.

2.17 CJIS Technology Gaps and Challenges

The June 5, 2008, National Security Presidential Directive-59 / Homeland Security Presidential Directive-24 (NSPD-59/HSPD-24)- emphasizes information sharing and interoperability. The directive states that each of the Secretaries of State, Defense, and Homeland Security, the Attorney General, the DNI, and the heads of other appropriate agencies, shall: “maintain and enhance interoperability among agency biometric and associated biographic systems, by utilizing common information technology and data standards, protocols, and interfaces.”

Surveying the gaps between service demands and currently available technology, policy, and standards, one notes that there are areas that will require additional FBI emphases. As the world leader in fingerprint biometrics, the FBI has established a Center of Excellence (COE) to address these gaps and to permit CJIS to focus on the now as well as the future.

The technology Grand Challenge for the FBI COE is to maintain and enhance the interoperability and accuracy of biometric technologies. To this end, several themes emerge as multimodal identification looms for CJIS. These include:

- Less than ten prints will become more prevalent as Mobile-ID devices are proliferated across law enforcement, national security, and military agencies. NGI will have to process and manage degraded source material and less information per enrollment while striving for accurate matching.
- State and local systems upgrades with new technologies such as palm prints, mug shots, and access to CJIS through ULW are approaching. These state and local AFIS upgrades will have a significant impact on CJIS as they will increase tenprint and latent print searches.
- These new modalities, combined with more automated processing, will increase the demand on CJIS and other identification service providers for fast and accurate responses. The transmission of palm images, face, and iris (future) search will present challenges, particularly at reconciliation.
- The access to semi-automated latent print searches and general access to CJIS through ULW will increase the search space for idents, but will also increase demand on both the system and the need for trained examiners.
- The need will increase for test data to include samples in each biometric modality from the same subject, collected at multiple times. These fused data sets are becoming critical to the technical and research community.
- NGI will be an evolutionary step in the CJIS identification process.

There are many areas that the COE could be tasked to address. These areas can include business trade studies, technology trade studies, research, white papers, and initiatives. Below are examples of possible opportunities for the COE in each area:

Business Trade Studies:

- Cost/Benefit Analysis Studies: Determine the Return on Investment for functions such as Major Case Prints, or use of Unsolved Latent File. Such a report would begin to develop a business model in which functions are prioritized based on overall cost-benefit trade off.
- Labor Analysis Studies: Characterize the supply and demand of latent print examiners. It will serve little purpose if system improvements produce more

and better latent print candidates, but there is no one to compare the candidates with the latent print.

- Security Studies: Security in the wireless and internet-dominated marketplace will require 2-factor authentication at customer end. Plans will have to be made for this eventuality.
- Fusion Studies: Undertake Fusion studies for multimodal thresholding.
- Integration Studies: Examine the integration with hand/vein collection/verification and other verification-only modalities.
-

Technology Trade Studies

- Mobile ID Studies: Initiate a Technology study on the development of Mobile ID systems and a companion Policy Paper on the administrative challenges and recommendations.
- NFIQ Studies: Work with NIST on updating NFIQ to include additional metrics beyond one to five integer values; additional possible metrics include area and core finding.
- Palm print Metrics Studies: Develop and assess palm print image quality metrics.
- Image Metrics Studies: Add other modality image open quality metrics as a part of fusion approaches.
- Records Distribution Studies: Create a management plan to update distributed records when external changes have to be applied (e.g., expungements, new events and corrections, Watchlist synchronization). Distributed systems lead to the challenge of records getting out of control. For example, if a record is expunged at the originating site, that change has to be conveyed to the Mobile ID systems on remote networks such as DoD, or another states, or counties.
- Civil Sensing Studies: Explore alternate sensing technologies used in civil applications
- Equipment Calibration Studies: Undertake an equipment certification/calibration program similar to laboratory level record keeping on calibration. The Certified Product List is dominated by items no longer manufactured; pace of change in scanner industry is a challenge. Is there still need to certify tenprint card scanners when few cards are inked and latent scanners are not certified? Or do we need to start addressing a CPL for mobile

ID, facial, palm, iris, and other capture devices to support responses end-to-end (collection through testimony) to Daubert challenges?

-

Research Studies

- The overarching theme of research is to help advance the identification process. Meeting this challenge requires research that is coupled with recommendations from SWGFAST[36] and others. Possible topics may include:
- Error Studies: Continue modeling error rates in automated systems and in human examination when using real world, large databases. Further the scientific basis for the laws of uniqueness and permanence to include persistence of level three fingerprint features over long periods of time.
- Threshold Studies: Determine the minimum number and type of features that are needed for an examiner to declare a positive match, and devise confidence metrics to describe different matching conditions.
- State of the Practice Studies: Provide updated ground truth latent data to boost research on collection, processing and performance.
- Implementation Studies: Determine how to migrate to the recommendations of CDEFFS, which will likely become mainstream and eventually encompass 10 prints
- Alternative Match Studies: Explore alternative matching techniques, which are likely non-compatible with current practices/training. This could include palm creases, light frequency filtering.
- Automated Search Studies: Examine methods to move toward more lights out (unsupervised) searching. This will become necessary with increased demand, particularly with the introduction of functionality such as Mobile ID devices.
- Interoperability and Data Sharing Studies: The interoperability and interchange with other, interagency databases will continue to pose a significant challenge. Provide policy framework and prototype application for federated identity searching with distributed storage and a small set of commonly supported attributes.

[36] See the complete list posted on the SWFAST website, www.swgfast.org.

- Criminal History Studies: More up-to-date Computerized Criminal History (CCH) with real dispositions, other modality searching, court systems that can process cases involving e-tickets, and single finger prints.
- DMV Interoperability Studies: Interoperability with motor vehicle databases; often the only biometric source data for immigrant populations.
- Commercial Interoperability Studies: Interoperability with commercial databases as biometrics become more widespread and subpoenas may be used to review data from these sources.

White Papers

Examine policy/privacy issues in NGI era such as:

- Investigative searches against civil repositories
- Secondary distribution issues associated with National Security searches
- Public access to information for accuracy and completeness
- Examine the limitations and benefits of alien students and instructors conducting government supported research. While not intended as a legal document, a paper on this topic would raise awareness and possible implications to International Traffic and Arms Regulations (ITAR).

Initiatives

- Terminology: Work with the IAI and SWGFAST to update and reissue ANSI/IAI 1 and 2 to provide an agreement of commonly used terms and benchmarking approaches for multi-biometric identification.
- Vendors: Develop and maintain a comprehensive list of government agencies at the state and local level, and their associated AFIS vendors. Such information will become increasingly important as the demand develops for interconnectivity and interoperability through programs such as Mobile ID.
- Latent Prints: Support latent print identification applications such as the expansion of the Universal Latent Workstation (ULW) program. This would include further technical development such as encoder modernization and the addition of palm prints, a 24/7 Support Center, more research into methods for expanding the program and collecting data on its use.

3 Palm print Recognition

3.1 Background

Palm print technologies share many acquisition and matching characteristics with fingerprint methods. Just as flat finger impressions provide a subset of the information available in a rolled print, the ridge patterns in the fingers are part of the overall ridge information in the entire hand. Along with the fingerprints, palm ridge structure forms during the 10th to 16th weeks of pregnancy and remains stable thereafter [Kucken, 2005]. Existing technologies used to image and match fingerprint areas can be expanded to incorporate palm ridge structure as well.

The palm consists of several regions that may be scanned independently, stored, or transmitted, depending upon device support and operational use case. Figure 3-1 illustrates the structure of the [right] palm and its relation to the full hand structure.

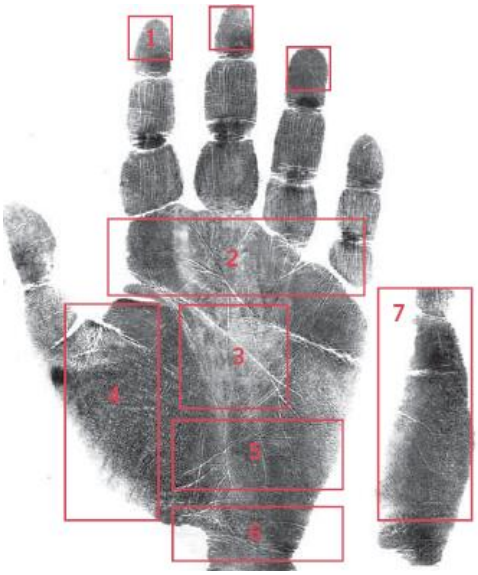


Figure 3-1. Palm Structure

The following regions provide the opportunity for subject differentiation through analysis and matching.

1. Fingerprints–Terminus of the fingers
2. Interdigital–Area between third finger joint and the cup, thenar and hypothenar
3. Cup–The depression between the thenar and hypothenar regions
4. Thenar–Muscular region at the base of the thumb
5. Hypothenar–Muscular region controlling the little finger

6. Carpal Crease–The fold where the palm and wrist meet
7. Writer's Palm–Side of the hand opposite the thumb.

It is more desirable to scan the entire hand in a single pass than to image various regions separately. At a minimum, an integrated scan can be faster and less error prone, since a series of individual images need not be reassembled and linked together. Yet, space and quality concerns often make it more practical to scan palm regions independently to assure best results. For illustration, consider that the cup region in the palm is within a concave space and will be more difficult to image than the prominent thenar region.

3.2 State of the Industry

The development of palm print scanners has evolved as a natural extension to livescan fingerprint devices. Product listings and solutions from 2000 to 2004 indicate robust vendor activity for fingerprint systems with palm scan capability. A closer examination reveals that much of the underlying scanner support is provided by a few vendors; differentiation occurs in the comparison software and systems packaging.

Industry consolidation and results from fingerprint performance evaluations have helped reduce the number of active companies providing palm print capabilities. Today, only a few vendors supply livescan equipment that can acquire palm imagery. Vendor acquisitions complicate some of these product lineups; models may still appear under prior companies in various literature.

Table 3-1. Industry Vendors for Palm print Scanners

Company	Models	Attributes	Comments
CrossMatch	ID 2500 LITE-UE 1000P 1000T	Various by model: 500 or 1000 DPI Full palm Upper/Lower palm Writer's palm FBI Certified	Acquired Smith Heimman Biometrics GmbH in 2005
L1 Identity Solutions	TouchPrint 3800	1000 DPI Full hand Full palm Writer's palm FBI Certified	Created by the merger of Viisage Technology Inc. and Identix Inc.
Green Bit S.p.A	PoliScan2 VisaScan3	500 DPI Half palm scanner Has an FBI Certified fingerprint scanner	Italian company

Company	Models	Attributes	Comments
Papillon Systems Ltd.	DS-40	500 DPI FBI Certified	Russian company

Well-known companies building livescan and Automated Fingerprint Identification Systems (AFIS) continue to design systems using the hardware listed above. Cogent Systems Inc. specifies scanners from Smith Heimann, now owned by CrossMatch. NEC Solutions has partnered with L-1 Identity Solutions for the TouchPrint line of scanners. Sagem Morpho Inc. does not identify the scanner models in their livescan systems, but they appear to be Smith Heimann (now CrossMatch) designs. Motorola Inc. utilizes various scanners from CrossMatch in their line of livescan systems.

Since palm print recognition is almost exclusively a law enforcement application and is closely associated with livescan fingerprint systems, it gets little commercial attention. Academic studies have proposed a number of approaches based not on friction ridges, but on hand shape or crease patterns [Duta, et al, 2002; Ribaric, et al, 2005; D. Zhang, 2004]. Consequently, when palm print technology is referenced, it is sometimes grouped with hand geometry and palm vein techniques.

3.3 Performance and Standards

Standards for the storage and interchange of palm data follow closely with those for fingerprint; they are often an extension of the latter. There are currently four standards that specifically identify palm acquisition and usage:

ISO/IEC 19794-4:2005 *Biometric data interchange formats Part 4 Finger Image Data* provides image exchange information for finger and palm datatypes

ANSI/INCITS 381-2004 *Finger Image-Based Data Interchange Format* provides image exchange information for finger and palm datatypes

ANSI/INCITS 398-2005 *Common Biometric Exchange Formats Framework (CBEFF)* identifies palm data as an exchangeable biometric payload

ANSI/NIST-ITL 1-2007 *Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information–Part 1* includes palm data as type-15 records. Can consist of full palm, upper half, lower half, thenar hypothenar and interdigital areas, and writer's palm impressions.

At this time, there have not been any large, independent evaluations of palm recognition. The National Institute of Standards and Technology (NIST) has conducted testing of latent fingerprints, and identified the difficulties in using palm prints as part of the NISTIR 7377

summary report. Presently, NIST plans to selectively collect palm print images, perhaps in conjunction with the development of latent applications within FBI/ CJIS.[37]

3.4 Simulation and Modeling

There is no known simulation or modeling of the ridge structure intrinsic to the palm region. The Synthetic Fingerprint Generation (SFinGe) software developed at the Biometric System Laboratory at the University of Bologna is an obvious candidate for future development in palm print simulation because of inherent similarities.

3.5 Forensic Capabilities

The detection and imaging of latent palm prints is similar to fingerprints, but with allowances for size and placement. One commonly quoted statistic asserts that one-third of all crime scenes involve latent palm prints. This has been misquoted to suggest that one-third of all latents are from the palm.[38] Regardless of the distinction, the friction ridge patterns from palm prints and full-case prints are logical extensions to fingerprints for forensic identification.

3.6 Privacy

The presence of abnormal creasing in the palm structure is often associated with a genetic disorder including Down syndrome, Aarskog syndrome, Cohen syndrome, and fetal alcohol syndrome [Adams, 2007]. Some may view these abnormal conditions to be medical information and hence subject to privacy considerations.

3.7 Vulnerabilities

3.7.1 References

Adams Wai Kin Kong. 2007. *"*Palmprint Identification Based on Generalization of IrisCode*."* *Doctor of Philosophy Thesis in Electrical and Computer Engineering*. University of Waterloo, Ontario, Canada. http://staffx.webstore.ntu.edu.sg/personal/adamskong/Shared%20Documents/publication/PhD_thesis_Adams_Final.pdf.

Duta, N., A. Jain, K. Mardia. 2002. "Matching of Palmprints." http://www.cse.msu.edu/cgi-user/web/tech/document?ID=451.

Kucken, M., A. Newell. 2005. *"*Fingerprint Formation*." Journal of Theoretical Biology 235.* http://math.arizona.edu/~anewell/publications/Fingerprint_Formation.pdf.

---

[37] NISTIR 7737 report. http://fingerprint.nist.gov/latent/ir_7377.pdf.

[38] Mark McDonals, ID/Latent Manager, Palm Beach County Sheriff's Office.

Ribaric, S., I. Fratric. November 2005. "A Biometric Identification System Based on Eigen-palm and Eigen-finger Features." *IEEE Transactions on Pattern Analysis and Machine Intelligence Volume 27, Issue 11*. p. 1698 -1709.

Zhang, D. 2004. "Palmprint Authentication System." *Handbook of Pattern Recognition and Computer Vision* (3rd Edition), Part 4: Human Identification. Chapter 4.3, p. 431-444, P. Wang (ed.).

4 Vascular Recognition

4.1 Technology Background

The discovery that vein structures could be used to identify individuals is commonly attributed to Joseph Rice in 1983 while he was working at Eastman Kodak in England [Rice, 2007]. At the time, he was experiencing label problems with an infrared barcoding system. At certain wavelengths, the labels became transparent to the scanner. Shortly thereafter, he was inspired to investigate the effects of this technology on his colleagues' skin and discovered that their vasculature appeared to be a distinctive trait. After some initial attention, Kodak executives lost interest in the economic viability of this promising biometric and the invention was signed over to the British Technology Group (BTG). Patent #4699149, *Apparatus for the identification of Individuals*, was issued to Joseph Rice on October 31, 1987.

Japanese biometrics vendors trace their technological history to a 1992 paper by Dr. K. Shimizu that discussed trans-body imaging using optical Computerized Tomography (CT) scanning [Shimizu, 1992]. He would later author a paper in 1996 with K. Yamamoto involving laser transillumination of physiological functions [Shimizu, 1996]. Starting around 2000, the transillumination work began to be cited in Japanese research that made specific reference to biometric [finger] identification. During this same period, patent issuance increased, suggesting that Japanese companies were engaged in the late 1990s.

Three dominant vascular recognition techniques have emerged. Fujitsu focuses on the palm of the hand, Hitachi uses the fingers and TechSphere uses the back of the hand. Vein recognition technologies have remained largely isolated to the Asia Pacific region, but rapid adoption within the financial sector in consumer-facing applications has encouraged the industry to expand elsewhere [Khan, 2006].

4.2 Vascular Imaging

Blood vessel development occurs in stages to create the network of arteries, veins, and capillaries needed for oxygen and nutrient transfer. Initially, the embryonic process of vasculogenesis creates the primary network of cells that form the major blood vessels. Later, the process of angiogenesis (i.e., growth of new blood vessels) fills in this structure to complete the smaller vessels and capillaries needed for the circulatory system.[39]

The underlying assumption behind vascular imaging techniques is that the veins exhibit different optical characteristics than the surrounding tissue, particularly in near infra-red wavelengths: the hemoglobin in the blood absorbs more and reflects less than other tissues. The spectral response of the hemoglobin in blood varies depending on the wavelength used and its oxygenated state (i.e., oxyhemoglobin-HbO_2 or deoxyhemoglobin-Hb). Figure 4-1, used by permission from Sassaroli,

[39] http://www.cancer.gov/cancertopics/understandingcancer/angiogenesis/Slide4.

shows the response of hemoglobin and water to differing wavelengths between 300 and 1300 nm. Since tissue is largely composed, it is easily differentiated from the vasculature.

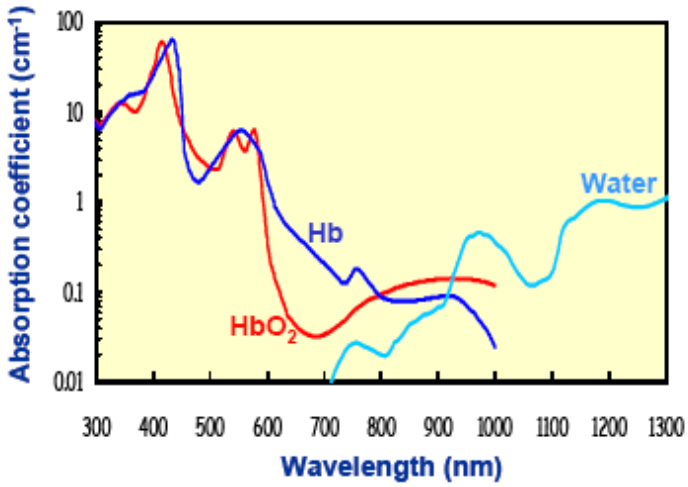


Figure 4-1. Spectral Response of Hemoglobin vs. Water [Sassaroli]

To distinguish vasculature from the tissue background, active methods must penetrate the desired area with sufficient energy to reveal the necessary detail. Beyond 900 nanometer (nm), the tissue permits only shallow or surface structures to be imaged. Below 600 nm, the hemoglobin limits deep imaging. The intervening 700 to 900 nm region is known as the "medical spectral window." It balances the need for hemoglobin detection and deep tissue imaging [Sassaroli].

The imaging process may be reflective or transmissive. Near infrared reflective techniques illuminate the surface of the skin at one or more predetermined angles with wavelengths beyond 750 nm. A sensor then detects the reflected light after the effects of scattering and absorption. This method is used for the palm and back of the hand. Transmissive methods illuminate the skin and sense the light that passes through the tissue, but not through the hemoglobin-rich vessels. Since this method has the illuminators and imaging sensors angled away from each other, it is more suitable for smaller regions such as the fingertips. Larger structures do not pass sufficient light.

Figure 4-2. Reflective Palm (Fujitsu) and Transmissive Finger (Hitachi)

Thermal imaging methods are possible. However, they are costly and sensitive to the temperatures of the subject and environment. No mainstream product vendor uses this technique.

Additional background on the physiology of vascular recognition technologies can be found in "The Hand Vein Pattern Used as a Biometric Feature" [Nadort, 2007].

4.3 Distinctiveness and Stability

Although there are claims of vascular distinctiveness in product descriptions and patent applications, it was not possible to find hard physiological evidence in the available literature. The process of vascular development in the embryo seems to exhibit many dynamic adaptations and suggests a distinctive structure and therefore subject differentiation [Eichmann, 2005].

After birth, the vascular structure grows with the skeletal structure for approximately 20 years. At this point, final bone fusion is roughly complete.[40] Figure 4-3 shows an x-ray of bone formation in the hand during youth and early adulthood. There are no known studies on vascular imagery patterns captured from the same subject over this growth period; however, it is reasonable to assume the changes would pose difficulties for recognition over time.

---

[40] "Basic [bone] Concepts: students," Washington, edu/alkim84/bioanth/files/basicconcepts.pdf.

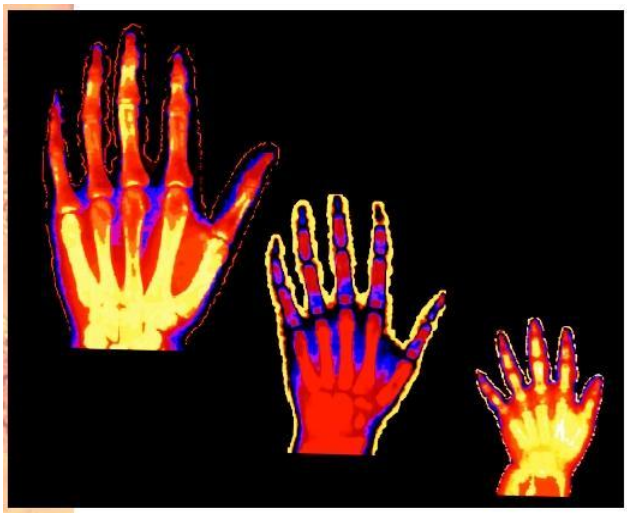


Figure 4-3. Bone Formation in the Hand for Males Ages 2, 6, and 19

Many factors can cause changes to the human vascular system, including tumors, atherosclerosis, diabetes, hypertension, and physical trauma. These factors can affect vascular recognition approaches in two ways:

- Affecting the structure and organization of the vasculature, thus introducing or removing information from the match decision
- Affecting the ability to sense, detect, or resolve the vasculature in sufficient detail to perform a match.

The affects of these conditions on vascular recognition technologies have yet to be studied. Privacy considerations and health disclosures will no doubt complicate such evaluation.

4.4 State of the Industry

The adoption of vascular recognition devices has been a recent phenomenon and is limited to the Asia-Pacific region. Most of the manufacturers are Japanese, with some activity in South Korea and the U.S. Fujitsu and Hitachi (Japan) appear to have cornered the market at this point. Techsphere, from South Korea, is not as well known, but their devices may undergo some rebranding.

4.4.1 Fujitsu

With its PalmSecure line of devices, Fujitsu Limited is the most well-known vein identification system vendor today. Available in Japan since 2005, the PalmSecure range of scanners has made

inroads into ATM/banking, access control, library, and public health applications. Estimates on the number of sensors deployed in Japan topped 15,000 as of September 2007, but the devices remain relatively unknown in the U.S.

The PalmSecure sensor is approximately 35x35 mm, and is packaged in a variety of configurations to assist in the proper positioning of the hand during operation (see Figure 4-4 for sample configurations). The sensor uses reflected near infrared wavelengths to illuminate the palm at the pre-established, optimal distance. The images below (Figure 4-4) are used by permission of Fujitsu.

Figure 4-4. Fujitsu PalmSecure Sensors (Fujitsu)

4.4.2 Hitachi

Hitachi markets finger vein systems for virtual and physical access applications; it has nearly the same visibility as Fujitsu. The company sold finger vein hardware since 2003, but launched a newer, more compact, and accurate line of sensors in late 2006. The physical access control device is an artist's representation and not the actual device. The images below (Figure 4-5) are used by permission of Hitachi.

Figure 4-5. Hitachi Finger Sensors (From Hitachi)

Hitachi uses a transmissive imaging technology that shines infrared light through the finger tissues to image the hemoglobin-filled blood vessels. Hitachi product literature recommends that the thumb not be used for enrollment and recognition.

4.4.3 Techsphere

Techsphere is an access control company from South Korea. They make readers that authenticate users based on the vein pattern on the back of the hand. The Vascular VP-II scanner seen in the figure below is configured as a door access unit. It can be reconfigured with a card scanner for time and attendance applications or other scenarios involving a physical token.

Figure 4-6. Identica Vascular VP-II Scanner

The company website (http://www.tech-sphere.com/) provides minimal information on the technical merits of the product. Throughput is exceptionally slow at only 10 comparisons per second.

4.4.4 Others

Several other companies are involved in the vascular recognition market, but their presence is currently less established compared with the three main technology providers.

Table 4-1. Other Vascular Vendors and Relationships

Vendor	Product	Notes	Reference
Fit-Design System Co., Ltd.	Finger Vein Auth. Reader	Japanese, small company	http://www.fit-design.com
Bionics Co., Ltd	VA100, VA200	Japanese	http://www.bionics-k.co.jp
Internal Biometrics Corporation	Spartan Shield	Arizona, USA Information is 2½ years old	http://internalbiometrics.com/index.html
PosID Incorporated	Thermo-ID	Maryland, USA Patented, but no product	http://www.posidinc.com/index.cfm
Apogee Biometrics	Livegrip	Washington State, USA	Defunct
TDSi	PalmGarde	United Kingdom Fujitsu based	http://www.tdsi.co.uk/index.php
iAccess	n/a	California,	http://www.iaccess-systems.com/

Vendor	Product	Notes	Reference
Systems LLC		USA Bionics Reseller	
Identica	n/a	Florida, USA Techsphere reseller	http://www.identicacorp.com/
NeuSciences LTD	Veincheck	United Kingdom Used in CESG evaluation	http://www.neusciences.com Product no longer exists
SnowFlake Technologies	VeinViewer (heathcare application) Prototype vein verification system	Owned by Luminetx Corporation, Memphis TN, USA	http://www.luminetx.com/Biometrics/SnowflakeTechnologies/ Prototype vein verification system announced in Gizmag, http://www.gizmag.com/vein-pattern-recognition-snowflake/8920/gallery/ (viewed 04 March, 2008)

4.5 Growth and Markets

Until recently, the development and deployment of vein recognition systems has been limited to the Asia Pacific region, with a strong presence in Japan. According to the Biometric Security Consortium (BSC), established to promote the growth of biometric technologies and infrastructure in Japan, fingerprint and vein biometrics will be the primary modes over the next five years.[41] Figure 4-7, from the Biometrics Security Consortium, shows the estimated market penetrations until 2010.

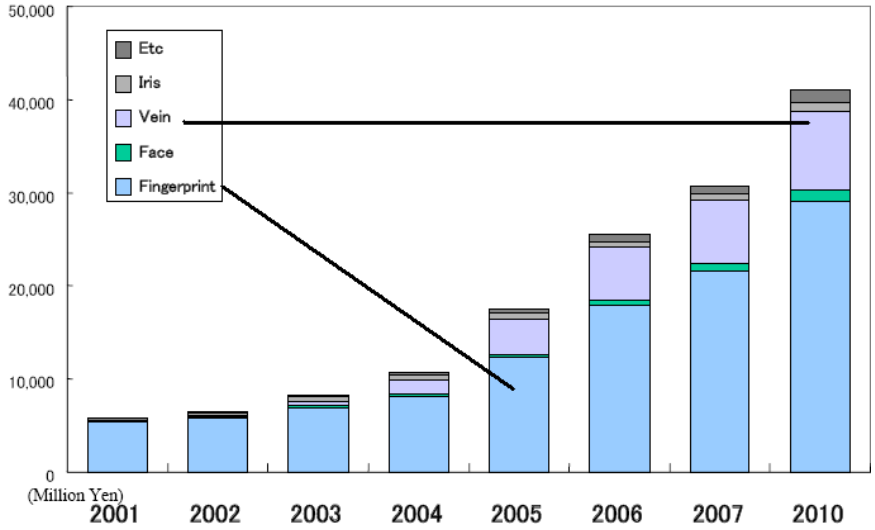


Figure 4-7. Japanese Biometric Growth

Further analysis shows that fingerprint growth is almost entirely allocated to mobile phone applications. Vein growth is allocated to information security and ATM (Automated Teller Machine) banking applications. If these predictions are true, the bulk of Japanese biometric growth in larger systems will not take place using established biometric modes.

4.6 Performance and Accuracy

Available literature has referenced three evaluations of vein recognition systems.

The first was performed by Fujitsu for their PalmSecure line of scanners using 140,000 palm profiles from 70,000 subjects. The enrollment process stipulated that the subjects should hold their palm over the sensor three times. Fujitsu conformed to the "Evaluation Method for Accuracy of Vein Authentication Systems (TRX0079)" proposed standard. This standard was put forth by the Information Technology Research and Standardization Center (INSTAC) within the Japanese Standards Association. The Fujitsu data does not appear to be publicly available. No sample imagery could be found.

The second evaluation was conducted by the Communications Electronics Security Group (CESG) and distributed as the "Biometric Product Testing Final Report" in March 2001. It compared several biometric modes including face, iris, fingerprint, voice, and vein. The study

[41] Biometrics Security Consortium, "Status of the biometrics market in Japan," http://www.bsc-japan.com/en/index.html.

consisted of checking 200 volunteers over three months. The device used in the study was a development prototype called Veincheck. The product is no longer marketed.

The third evaluation was performed in 2006 by the International Biometric Group (IBG) and released as the "Comparative Biometric Testing Round 6 Public Report." This evaluation compared the Fujitsu PalmSecure, Hitachi UBReader TS-E351, and IrisGuard H-100 biometric scanners. Data collection occurred over two months (May-June 2006). Samples were taken in two sessions from 650 distinct subjects. The subjects were recruited from the general New York City population. Nearly 20,000 samples from each reader were analyzed. This is the only *public* evaluation providing information on commercially available readers.

4.7 Match Error Rates

For all biometric technologies, error rates are highly dependent upon the population and application environment. The technologies do not have known error rates outside of a controlled test environment. Therefore, any reference to error rates applies only to the test in question and should not be used to predict performance in a different application.

The IBG laboratory evaluation measured the True Accept and False Accept Rates for the Hitachi and Fujitsu sensors, but with a caveat that makes direct comparison slightly more difficult. The Hitachi unit reported raw similarity scores between template comparisons and thus gave a more complete picture of the error tradeoffs. Note that the Fujitsu unit was evaluated at three discrete thresholds (high, default, and low security) and does not provide a full Receiver Operator Curve (ROC). Comparison at other thresholds are approximate and do not represent observed values.

Table 4-2. True and False Accept Rates for Different-Day Samples (IBG and Vendors)

Device	Vendor Claim		IBG Result (Attempt Level)		IBG Result (Transaction Level)[42]	
	True Accept Rate	False Accept Rate	True Accept Rate	False Accept Rate	True Accept Rate	False Accept Rate
Hitachi TS-E3F1	99%[43]	1 in 10,000	95.28%	1 in 10,000	97.23%	1 in 10,000
Fujitsu PalmSecure[44]	99%[45]	< 1 in 10,000	approximate 91%	approximate 1 in 10,000	Approximate 99%	approximate 1 in 10,000

[42] A transaction consists of up to six possible attempts in the course of a recognition decision.

[43] Hitachi internal testing specified the Japan Industrial Standard (JIS) for evaluation. It was not possible to determine whether error rates were calculated at a transaction or attempt granularity.

[44] Fujitsu results were calculated at fixed thresholds. The TAR/FAR values are linearly interpolated from the graphs in the IBG report using the discrete thresholds that were available.

[45] Fujitsu permitted one rescan attempt for recognition. Individual attempt granularity results will be lower.

Device	Vendor Claim		IBG Result (Attempt Level)		IBG Result (Transaction Level)[42]	
	True Accept Rate	False Accept Rate	True Accept Rate	False Accept Rate	True Accept Rate	False Accept Rate
Fit-Design Reader(s)	99%	1 in 10,000	n/a	n/a	n/a	n/a
Bionics VA100/200	99%	1 in 10,000	n/a	n/a	n/a	n/a
Techsphere Vascular VPII	99.99%	1 in 10,000	n/a	n/a	n/a	n/a

The error rates presented in Table 4-2 show how human factors of the single finger and full palm scanning methods impact error rates. The Hitachi single-finger scanner is more accurate than the Fujitsu full-palm scanner for single attempts. This accuracy may be attributed to the ease and consistency of finger placement relative to the full palm scanner. Once multiple attempts are permitted (a transaction), the Fujitsu palm scanner jumps to 99 percent true accepts, while still maintaining its 1 in 10,000 False Alarm Rate (FAR). Such a jump is not seen in the finger scanner when multiple attempts are allowed.

A likely explanation is that the Fujitsu palm guide provides reasonable, but not ideal, positioning feedback to the subject. Repeated recognition attempts mitigate the placement of the hand.

The CESG study provided a Detection Error Tradeoff plot of various biometric modes. The performance of the Veincheck system shown in Figure 4-8 (red line) indicates that it was one of the bottom performers. Since The NeuSciences Veincheck system was a development prototype and is no longer available, these results are unlikely to be indicative of any commercial-grade technology.

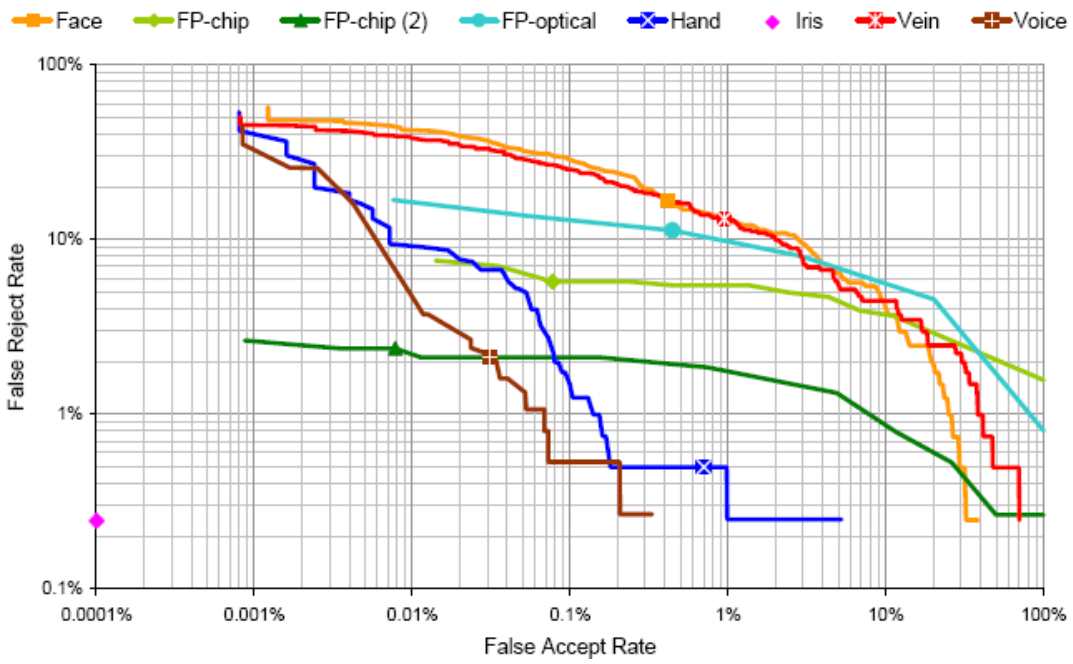


Figure 4-8. DET Curve for CESG Study (Vein in Red)

4.8 Enrollment and Acquisition Error Rates

The CESG study of vein recognition reported a failure to enroll (and acquire) rate of 0.0 percent in their test scenario. The report notes that, in cases of difficulty, the subject was permitted an unspecified number of additional enrollment attempts.

The IBG protocol distinguished the inability to acquire any or all samples during the laboratory enrollment process. As a matter of policy, it may be permissible to enroll less than the desired number of fingers or palms; in this case, failure to enroll is defined as the inability to acquire *all* of the desired samples (for IBG Vein Systems, this is two instances).

Both the Fujitsu palm scanner and Hitachi finger scanner had similar Failure to Enroll (FTE) rates of 1.63 percent and 0.55 percent, respectively

The Fujitsu palm scanner provided a median enrollment time of 61.7 seconds (66.8 seconds mean) under these test protocols in this environment. The Hitachi finger scanner performed enrollments nearly twice as quickly with a 33.3 second median time (38.4 seconds mean).

Acquisition times for any given recognition attempt were low for both systems. The Fujitsu palm scanner performed at 2.13 seconds median (2.14 seconds mean). The Hitachi finger scanner completed acquisitions in roughly half the time with 1.23 seconds median (1.77 seconds mean).

4.9 Conclusions

The IBG report concluded from their trial of finger, palm, and iris modes that:

Each was a high performer for the types of applications intended (verification).

All the systems had low failure to enroll and low failure to acquire rates in a laboratory environment with their volunteer participants.

Finger vein (and palm to a lesser degree) acquisition and enrollment times were comparatively short and suggested positive usability for a large part of the test population.

Vascular recognition is a serious competitor to fingerprint, hand geometry, and certain iris recognition systems used in 1:1 access control scenarios.

4.10 Standardization and Interoperability

The ISO/IEC published the first edition of a vascular image data standard in March 2007. The full standard is entitled: ISO/IEC 19794-9 "Information Technology–Biometric Data Interchange Formats–Part 9: Vascular image data."

The standard, along with the other biometric documents in the 19794 series, are classified as "International standard published," after having successfully undergone review and approval. Approximately three years after publication, they will undergo a review cycle by all ISO member bodies. At this point, the participants will decide whether the standard should be reconfirmed, revised, or withdrawn. Currently, several of the 19794 biometric standards are beginning this periodic review.

The Part 9 standard specifically addresses the image exchange requirements for vascular biometric technologies involving the back of the hand, palm, and finger. It defines the record format, attributes, and conformance criteria necessary for the transmission and interoperability of vascular data.

The standard has recently been adopted as a U.S. National Standard, however, is too recent to assess adoption by the vascular user and vendor communities.

The InterNational Committee for Information Technology Standards (INCITS) sought comments and recommended the adoption of 19794-9 as an INCITS standard upon its publication. The incits.org website currently lists INCITS/ISO/IEC 19794-9 as an identical national adoption of the ISO standard dated August 17, 2007.

4.11 Image Capture Requirements

The standard lays the basic general requirements for imaging the three vascular modes. Table 4-3 summarizes the main points for image capture. For complete information, refer to the standard.

Table 4-3. ISO/IEC 19794 Image Capture Synopsis

Capture Aspect	Commentary
Spatial Resolution	No minimum specification stipulated, due to inherent differences in the vascular detail needed for larger (palm) and smaller (finger) areas.
Grayscale Depth	Must have a dynamic range spanning a minimum of 128 values (7 bits) stored in 1 or 2 bytes.

Capture Aspect	Commentary
Illumination	Standard acknowledges that the variety of possibilities (e.g., reflected, transmissive, different wavelengths) prohibit a minimum requirement. The Illumination type used must be noted in the header and includes Undefined, Near Infrared, Mid Infrared, Visible, and Others. Illumination combinations are possible. The imaging method (e.g., reflective, transmissive) must also be noted.
Aspect Ratio	The pixel aspect ratio default is 1-to-1 (i.e., square pixels). Deviations must be described in the format header.
Projection Normalization	Orthographic
Image Compression	Supported: raw, JPEG, Lossless JPEG, JPEG 2000. A compression factor of 4:1 or less is recommended.
Imaging Area/Poses	Fingers (thumb, index, middle, ring, little), palm, and back of hand. Dorsal sides of the finger are supported (i.e., back of finger). Other physical areas are reserved, but not enumerated, in the standard.
Coordinate Systems	Coordinate systems are described for hand and finger modes. Other systems are reserved by the standard, but not enumerated.

4.12 File Format Requirements

Vascular biometric data conforming to the 19794-9 image capture requirements is intended to be embedded in a CBEFF compliant Biometric Data Block. CBEFF is specified in ISO/IEC 19785-1.

4.13 Vulnerabilities

Vascular systems are currently only used in positive-claim applications. Consequently, we will not discuss possible methods for obscuring vascular patterns from imaging devices.

4.13.1 Spoofing

The spoof ability of vein recognition methods in positive claim applications was evaluated by FIDIS (Future of Identity in the Information Society) in January 2006. FIDIS is a network of commercial and academic organizations supported by the European Union whose charter is to understand forensic, interoperability, and security issues of identification technologies. The TechSphere hand vein recognition system was included in a report entitled “Forensic

Implications of Identity Management Systems." This report speaks broadly on biometrics issues and addresses fingerprint, iris, hand geometry, and hand vein modalities.[46]

The FIDIS evaluation took a visible image of the back of a subject's hand and extracted the vein pattern using image processing software. The resulting pattern was carefully matched in size to the subject's physical hand dimensions and printed out. Veins not sufficiently prominent and discernable from a visible photograph could be captured using a camcorder operating in infrared (nightshot) mode. Sample acquisition images, from FIDIS, are shown in the figures below.

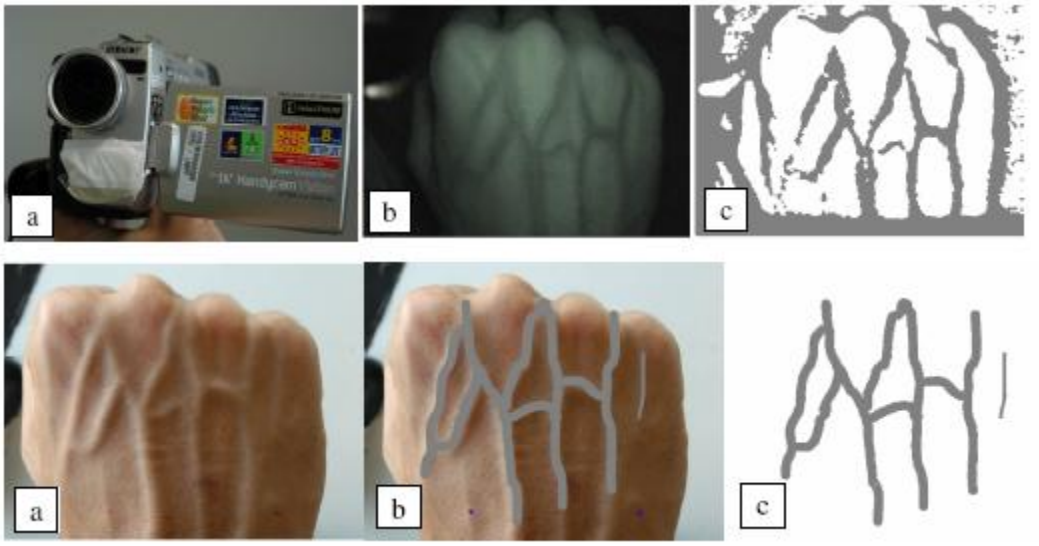


Figure 4-9. Hand Vein Spoof Acquisition

The replicated pattern was then placed on a water bottle or an actual hand and presented to the hand scanner as shown in Figure 4-10. Spoof for Techsphere (Back of Hand) Vein Scanner."

Figure 4-10. Spoof for Techsphere (Back of Hand) Vein Scanner

[46] FIDIS (Future of Identity in the Information Age). *D6.1 Forensic Implications of Identity Management Systems*. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp6-del6.1.forensic_implications_of_identity_management_systems.pdf

The hand scanner permitted the ability to disable liveness detection independently for enrollment and verification. These settings were evaluated with the two presentation methods above to discover the liveness combinations that failed.

The FIDIS paper concluded that a partial spoof was successful. With liveness detection disabled, the scanner did not distinguish the vein pattern copy from the real hand, and was unwilling to reject a latex glove on a water bottle. But, even with liveness detection enabled, it was possible to enroll with a paper copy and verify using the real hand; the latex glove continued to function, despite liveness being enabled.

Similar spoofing studies have been recently conducted by Prof. Tsutomu Matsumoto of Yokohama National University. His work demonstrated that artifacts fabricated from vegetable sticks could be enrolled and verified. With knowledge of target vein patterns, defeats were also possible against real enrolled hand vein patterns.

4.14 Future Capabilities

- The rapid commercialization of vascular recognition technologies in Japan and Korea, coupled with intellectual property restrictions (patents), is limiting active research. Future capabilities might include:

Increasing the imaging space, resolution, and range of vascular sensors

Integrating vascular techniques with fingerprint (flats or slaps) and hand for match fusion or liveness detection

Realizing viable use cases for other vascular structures from regions such as the face, neck, wrists, or chest.

4.15 CJIS Technology Gaps and Challenges

Although no major U.S. government identification application currently collects vascular images, there is interest and increased use vascular recognition in other markets. The opportunity for simultaneous capture with palm and other “hand biometric modalities” has been noted by researchers, and there may come a day when vein patterns are adopted in the financial sector for authentication and to help thwart identity fraud. In preparation for expanded use in the commercial sector, CJIS should consider activities to:

- Develop an expansion path for vascular images to be included in standards (ITL and Electronic Biometric Transmission Specification)
- Provide reference data for identification assessments, fusion with other hand biometric modalities, and to stimulate fundamental research (e.g., secondary veins or three dimensional vascular structures)
- Current vascular imaging sensors are mostly driven by the Asian market for verification applications. There currently is no real market demand for sensors that output image for interoperability and vendor neutral storage.

4.15.1 References

Eichmann, A., L. Yuan, D. Moyon, F. Lenoble, L. Pardanaud, C. Breant. 2005. "Vascular Development: From Precursor Cells to Branched Arterial and Venous Networks." *Int J Dev Biol* 49. p. 259-267.

Khan, I. December, 2006. *Vein Pattern Recognition–Biometrics Underneath the Skin.* http://www.findbiometrics.com/article/320.

Nadort, A. May, 2007. *The Hand Vein Pattern Used as a Biometric Feature. Masters Thesis.* http://www.forensischinstituut.nl/NR/rdonlyres/98611DD2-9D57-499B-A14D-9C1ABEA6217A/27198/Thesis_Annemarie_Nadort1.pdf.

Rice, J. May 2007. *"*The Future of Vein Recognition*." Biometric Watch.* Vol. 5, Issue 5. http://www.biometricwatch.com/BW_41_May_2007/BW_41_Future_Of_Vein_Recognition.htm.

Sassaroli, A., et al. *"Near-Infrared Spectroscopy for the Study of Biological Tissue."* http://ase.tufts.edu/biomedical/research/Fantini/researchAreas/NearInfraredSpectroscopy.pdf.

Shimizu, K. 1992. "Optical Trans-Body Imaging – Feasibility of Optical, CT and Functional Imaging of Living Body." *Medicina Philosophica*. 11:620-629.

K. Shimizu, K., K.Yamamoto. 1996. "Imaging of Physiological Functions by Laser Transillumination." *OSA TOPS on Advances in Optical Imaging and Photon Migration*. Vol. 2. p. 348-352.

5 Standards

5.1 History and Organizations

The earliest electronic standardization efforts can be traced to the mid-1980s when the NIST and the FBI developed the *Data Format for the Interchange of Fingerprint, Facial, Scar Mark, and Tattoo (SMT) Information*. This standard was adopted by major law enforcement agencies in the United States and formed the basis of future work. The rapid emergence of biometrics outside of a law enforcement context has necessitated broader standardization efforts, international scope, and the capability of embracing many commercial applications.

Biometrics standardization organizations can be partitioned into two camps. The first consists of industry and academic consortia; it acts in an informal way to promote open standards and interoperability. The second represents the official standards bodies that may be national or international in scope; they are often funded by governmental agencies. As biometric technologies mature, international bodies become increasingly important to ensure broad interoperability. This is especially true for credentialing and identity management applications that may span national borders.

Table 5-1 provides a listing of standards bodies and how they act within the biometrics community. The list is a sampling of some of the major players routinely encountered when researching biometrics, surveillance, and related technologies.

Table 5-1. Standards Bodies, Role and Scope

Body	Role	Biometrics Scope
American National Standards Institute (ANSI)	A nonprofit body that oversees standards development and consensus within the United States.	Accredits the activities of INCITS in paralleling the development of international standards
International Civil Aviation Organization (ICAO)	An agency of the United Nations responsible for civil aviation, border crossing procedures, and accident investigation.	Defined the standards for machine readable and electronic passports containing biometric records.
International Committee on Information Technology Standards (INCITS)	Coordinates various standards activities between ANSI in the United States and the ISO/IEC worldwide.	Most biometric ISO/IEC standards have an INCITS equivalent. The M1 technical committee closely parallels the activities of the ISO/IEC SC 37 subcommittee.

Body	Role	Biometrics Scope
International Electrotechnical Commission (IEC)	A nonprofit, nongovernmental standards organization that broadly addresses electronics technologies.	Jointly publishes or develops standards with other organizations such as the IEEE and ISO.
International Organization for Standardization (ISO)	International standard body comprised of representatives from national standards bodies.	In cooperation with the IEC, a Joint Technical Committee (JTC1) develops IT standards. Biometrics falls under the SC 37 subcommittee.
International Telecommunications Union (ITU)	An international organization established to standardize international telecommunications. Part of the United Nations.	Participates in ISO/IEC JTC1 SC 27 subcommittee (Information technology Security Techniques). Collaborates with SC 37 biometrics.
Organization for the Advancement of Structured Information Standards (OASIS)	International nonprofit promoting the adoption of open standards for the global information society.	Defined XML encoding rules for biometric data originally specified as CBEFF structures. Product: XML Common Biometric Format (XCBF) 1.1.

5.2 Applicable Biometrics Standards and Evaluations

Biometric standards typically fall into a limited set of categories, depending on what aspect of the biometric lifecycle is being addressed. While it is desirable to standardize on sensors, features, and interchange formats in a linear fashion, based on objective performance evaluation and interoperability tests, there are often gaps due to limited deployment and availability. For example, not all of the data interchange series, including several recently moved from INCITS to their ISO counterparts, have automated tools and methods for conformance. Biometrics markets also tend to align vertically and oppose standardization until such time as there is strong incentive for horizontal integration.

CR: Credential Operation
Pertains to biometrics as implemented on smartcards and passports.

ID: Image data formats
Relating to the acquisition and storage of raw sample data prior to analysis

TR: Template representations
Dealing with the processed biometric in its concise, matchable form

DS: Data storage and interchange
Relates to how the biometric data is packaged, stored, and transmitted across systems

AQ: Acquisition quality and equipment guidelines
Guidelines for establishing best practices, approved hardware, and sample acceptability

TE: Testing and evaluation
Any aspect of performance testing, error analysis, or operational validation.

Table 5-2. Summary and Status of Recent Standards

Standard	Title	Status	Type
ISO/IEC 19794-2	Information Technology Biometric data interchange formats Finger minutiae data	Under revision, ballot initiated on 2008-08-21	TR
ISO/IEC 19794-3	Information Technology Biometric data interchange formats Finger pattern spectral data	To be revised as of 2007-12-04	ID
ISO/IEC 19794-4	Information Technology Biometric data interchange formats Finger image data	To be revised as of 2007-08-14	ID
ISO/IEC 19794-5	Information Technology Biometric data interchange formats Face image data	To be revised as of 2007-08-14	ID
ISO/IEC 19794-6	Information Technology Biometric data interchange formats Iris image data	To be revised as of 2007-08-14	ID
ISO/IEC 19794-9	Information Technology Biometric data interchange formats Vascular image data	Revised and published 2007-03-01	ID
ISO/IEC 7816-4:2004	Identification cards Integrated circuit cards Inter-industry commands for interchange	Revised and published in 2005	CR

Standard	Title	Status	Type
ISO/IEC 7816-11:2004	Identification cards Integrated circuit cards Personal verification through biometric methods	2004-04-01	CR
ANSI/INCITS 358-2002	Information technology The BioAPI specification	Revised in 2007	DS
ANSI/INCITS 377-2004	Information technology Finger pattern based interchange format	2004-01-23	ID
ANSI/INCITS 378-2004	Information technology Finger minutiae format for data interchange	2004-02-20	TR
ANSI/INCITS 383-2004	Biometric Profile interoperability and data interchange Verification and identification of transportation workers	Revised 2008	??
ANSI/INCITS 385-2004	Information technology Face recognition format for data interchange	2004-05-13	ID
ANSI/INCITS 385-2004 Amend 1	Information technology Face recognition format for data interchange Amendment 1: 3D Face	Pending draft as of 2006	ID
ANSI/INCITS 394-2004	Application profile for interoperability – data interchange and data integrity of biometric-based personal identification for border management	2004-10-05	??
ANSI/INCITS 398-2005	Information technology Common biometric exchange formats framework (CBEFF)	Revised 2008	DS
ANSI/INCITS 409.x-2005	Biometric Performance Testing and Reporting Parts 1-4: Principles framework, technology testing methodology, scenario testing methodologies, operational testing methodologies	2005-10-25	TE
ANSI/INCITS 421-2006	Biometric profile interoperability and data interchange DoD Implementers	2006-12-01	DS

Standard	Title	Status	Type
ANSI/INCITS 422-2007	Application profile for commercial biometric physical access control	2007-02-01	??
ANSI/NIST-ITL 1-2007	Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1	2007-04-20, added part 2 - XML	DS
ANSI/NIST CDEFFS	Committee to Define an Extended Fingerprint Feature Set	Draft	ID DS
IAFIS-DOC-01078-8.001	Electronic biometric transmission specification	Draft	DS
IAFIS-DOC-01078-8.002	Electronic fingerprint transmission specification	Revised April 2008	DS
ICAO LDS 1.7	Machine readable travel documents Development of a logical data structure	2004-05-18	CR DS
NISTIR 7151	Fingerprint image quality	2004-08-19	AQ
NISTIR 7296	MINEX – Performance and interoperability of the INCITS 378 fingerprint template	2006-03-21	TE TR DS
OASIS XCBF 1.1	XML common biometric format	2003-09-03	DS

5.2.1 Synopsis of FBI Electronic Biometric Transmission Specification

Background

For the past century, fingerprints have been the used by the law enforcement community for identification purposes. The primary means of gathering and transporting fingerprints was by ink and paper. The FBI developed the Integrated Automated Fingerprint Identification System (IAFIS) to support the paperless transmission and automated matching of fingerprints. As IAFIS was developed, the National Crime Information Center (NCIC) Advisory Policy Board (APB) Identification Services Subcommittee recognized the need for the standardization of electronic transmission of fingerprints[47].

[47] IAFIS-DOC-01078-8.001, FBI CJIS "Electronic Biometric Transmission Specification." October 24, 2007. http://www.fbibiospecs.org/fbibiometric/biospecs.html.

The FBI, working with the NIST and the fingerprint identification community, developed the ANSI/NIST ITL. This standard provided the guidelines for the electronic exchange of fingerprint information among various law enforcement systems. To further define requirements for doing business with the FBI IAFIS, the FBI developed the Electronic Fingerprint Transmission Specification (EFTS). EFTS, based on the logical record structure set forth by the ANSI/NIST ITL, defines the types of transactions and data requirements used to perform tenprint identification and maintenance services, thus acting as the Interface Control Document for IAFIS.

With the advances in biometric technology, the ANSI/NIST ITL standard has evolved into the "Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information" (ANSI/NIST-ITL 1-2007). Similarly, the FBI is revising EFTS to include multimodal biometric services as well as expanding maintenance services; this revision is known as the Electronic Biometrics Transmission Specification (EBTS).

Scope

EBTS specifies the file and record content, format, and data codes necessary for the exchange of biometric information among federal, state, and local users, and the FBI. Biometric modalities defined in EBTS include fingerprint, palm print, facial, and iris; also included is the ability to transmit other biometrics. Per ANSI/NIST ITL, biometrics for which there is no delineated record should be included in Type 99 records in CBEFF.

EBTS defines the types of transactions (TOTs) and the use cases for fingerprint and other identification services. Descriptions of these requests and their respective responses are also provided. EBTS lists the following services and provides the descriptions for each:

Tenprint Services

Latent Services

Special Population Services

Image Services

Palm print Services

Photo Services

Facial Recognition Services

Iris Services

Rap Back Services

Other Biometric Services.

Several services are currently supported in EFTS, including Tenprint, Latent, and Image; these services are expanded in EBTS. Other services have been, or will be, implemented as part of NGI.

EBTS Status

EBTS is in draft form; the current release is EBTS 8.001, dated October 24, 2007. This specification has had external, IAFIS Interface Evaluation Task Force (IIETF), and APB review cycles. EBTS is being updated to incorporate comments. There are several TOTs that are yet undefined in the current release of EBTS. These TOTs will be described in future releases.

Maturity

Table 5-2. Summary and Status of Recent Standards enumerates the many standards available within the biometrics domain. This past year a series of data interchange format standards were withdrawn, or succumbed into their ISO counterparts. Not all biometric modalities have achieved the same level of standards development. In many instances, this is because the biometric is relatively new and not broadly embraced within the community. In other cases, the biometric may be limited by proprietary implementations or patent constraints. Biometric modes that do not rely on common features with scientific studies supporting their uniqueness and permanence are unlikely to have open reference tools for image quality conformance or proceed beyond the more basic "image format" standards.

The following table summarizes the major biometric modes and their degree of standardization. Green indicates most mature and red indicates the least mature. DNA standards are developed through different communities than 'biometrics standards' but are illustrated for comparative purposes. "No CPL" (Certified Product List) is directly related to the lack of standard template representations. With no common agreement on the features that constitute individuality for a particular biometric, there can be little agreement on the proper resolution and imaging technology to best capture those biometric characteristics. The relatively mature support for fingerprint livescan technology that is illustrated does not yet fully extend to latents and mobile identification applications.

Table 5-3. Summary of Standards by Modality and Purpose

Biometric Mode	Credential operation	Image or file data formats	Template representations	Transaction, transmission, and encoding	Acquisition Quality & equipment Guidelines	Testing and Evaluation (data and methods)
Face				Quality estimation and encoding	NO CPL	Representative data needed
Iris				Quality estimation and encoding	Not all sensors output images NO CPL	Representative data needed
Vasculature	Financial community				Not all sensors output images NO CPL	Limited data
Voice	Financial community	Audio files		Quality estimation and encoding	Need subject acquisition profiles NO CPL	Representative data needed
Palm	N/A					Limited data
Fingerprint				slap/seg and compression	Image quality based CPL, widely used	
Handwriting					Need subject acquisition profiles NO CPL	Limited data
DNA	N/A				Certification of lab process and equipment	

Standards exist and are used in some large applications
Standards are emerging, in progress, or not yet broadly adopted
Standards don't exist or are not used

5.3 Vulnerabilities

Every system utilizing public interchange and storage formats is vulnerable to attack by an adversary. The attack vector usually involves the clever manipulation of interchanged data to expose bugs in either the standard itself or in its implementation. The result can vary based on intent, but may involve any of the following:

Denial of service at receiver due to crash or error conditions

Undesirable insertion, deletion, or modification of data records

Execution of malicious software instructions (code)

Escalation of privileges, rights, or other security aspects.

One of the most common examples of malicious code development involves the exploitation of "buffer overflow" conditions. This occurs when memory addresses are corrupted by data that either exceeds its usual size or had its length misrepresented. Software that does not adequately scrutinize incoming data for consistency, size, and integrity can be tricked into executing malicious code that should be treated as imagery, text, or other data. A common sign that software is vulnerable to malicious code injection is that it has crashed in the past when presented with

poorly formatted data. The crash is a random response to garbage instructions that could have been crafted to do something malicious instead.

A [biometric] standard cannot prevent poorly implemented software from being vulnerable to attack. However, a poorly written standard with ambiguous descriptions, contradictory use cases or ill-considered extensions can make the attacker's job easier. Vulnerabilities are often found in functions that are rarely used and poorly tested. A large standard that offers great flexibility may be exposing significant amounts of untested and insecure functionality.

Biometric systems have not undergone the ubiquitous deployment that attracts the interests of hackers. Greater use of biometrics will bring greater economic or social incentives to those who can benefit from successful attacks. For now, incentives remain low, and standards and implementations have not been challenged from this perspective.

5.3.1 Recent Exploits

In August 2007 at the Black Hat security conference in Las Vegas, researchers were able to crash Radio Frequency Identification (RFID) passport readers by storing a specially crafted JPEG image on an E-Passport. This is nothing new. Corrupted and malformed image files have always been a challenge for software to process without error. Now, the vector is a smartcard containing a biometric image of a person's face. The crashing behavior is the proof-of-concept of a vulnerability; exploiting this vulnerability requires additional work e.g. malicious code.

In 2006, Will Carsola and Dave Stewart exposed glaring deficiencies in the Virginia State driver's license re-issuance process. In a prank designed for an internet movie, they obtained new licenses with photos featuring themselves in outlandish disguises with no likeness to their true appearance. While a source of embarrassment for the State, the prank contains a more serious message that photos and other biometric information on identification documents cannot be updated or swapped in haphazard manner. Bruce Schneier comments on the incident [Scheier, 2006], as does Michelle Malkin [Malkin, 2006]. Malkin opined the pranks provided a valuable service and goes on to state, *"… few dissertations and policy analyses drive the message home more effectively than these two damning videos".*

5.4 Gaps and Recommendations

Standards are one of the few available tools for maintaining and enhancing the interoperability and accuracy of biometric technologies. Table 5-4 provides a SABER investment perspective for engaging and leading in the development of critical standards while supporting or remaining aware of others. The dollar symbols suggest the relative importance:

- $$$: leadership in the form of authoring, contributing or close engagement; high relevance for current systems, technical impact studies per NGI or Certified Product List (CPL) or other performance studies
- $$: Support in the form of engagement or select impact studies and limited adoption
- $: Monitoring in the form of situational awareness and possible information exchanges.

Table 5-4. Recommended Standards Roadmap

Standard	Title	SABER
ISO/IEC 19794-2	Information Technology Biometric data interchange formats Finger minutiae data	$$$ (NGI/CPL)
ISO/IEC 19794-3	Information Technology Biometric data interchange formats Finger pattern spectral data	$$$ (NGI/CPL)
ISO/IEC 19794-4	Information Technology Biometric data interchange formats Finger image data	$$$ (NGI/CPL)
ISO/IEC 19794-5	Information Technology Biometric data interchange formats Face image data	$$$ (NGI/CPL)
ISO/IEC 19794-6	Information Technology Biometric data interchange formats Iris image data	$$$ (NGI/CPL)
ISO/IEC 19794-9	Information Technology Biometric data interchange formats Vascular image data	$$ (NGI/CPL)
ISO/IEC 7816-4:2004	Identification cards Integrated circuit cards Inter-industry commands for interchange	$$ (id programs, cyber crime)
ISO/IEC 7816-11:2004	Identification cards Integrated circuit cards Personal verification through biometric methods	$$ (id programs, cyber crime)
ANSI/INCITS 358-2002	Information technology The BioAPI specification	$
ANSI/INCITS 377-2004	Information technology Finger pattern based interchange format	$$$ (NGI/CPL)

Standard	Title	SABER
ANSI/INCITS 378-2004	Information technology Finger minutiae format for data interchange	$$$ (NGI/CPL)
ANSI/INCITS 379-2004	Information technology Iris image interchange format	$$$ (NGI/CPL)
ANSI/INCITS 381-2004	Information technology Finger image-based data interchange format	$$$ (NGI/CPL)
ANSI/INCITS 383-2004	Biometric Profile interoperability and data interchange Verification and identification of transportation workers	$
ANSI/INCITS 385-2004	Information technology Face recognition format for data interchange	$$$ (NGI/CPL)
ANSI/INCITS 385-2004 Amend 1	Information technology Face recognition format for data interchange Amendment 1: 3D Face	$$$ (NGI/CPL)
ANSI/INCITS 394-2004	Application profile for interoperability–Data interchange and data integrity of biometric-based personal identification for border management	$$ (interop)
ANSI/INCITS 395-2005	Information technology Biometric data interchange format–Signature/sign data	$$ (doc forensics, id fraud)
ANSI/INCITS 396-2005	Information technology Hand geometry interchange format	$$ (NGI)
ANSI/INCITS 398-2005	Information technology Common biometric exchange formats framework (CBEFF)	$
ANSI/INCITS	Biometric Performance Testing and Reporting	$$

Standard	Title	SABER
409.x-2005	Parts 1-4: Principles framework, technology testing methodology, scenario testing methodologies, operational testing methodologies	(scenario testing)
ANSI/INCITS 421-2006	Biometric profile interoperability and data interchange DoD Implementers	$
ANSI/INCITS 422-2007	Application profile for commercial biometric physical access control	$
ANSI/NIST-ITL 1-2007	Data Format for the Interchange of Fingerprint, Facial, and Other Biometric Information–Part 1	$$$ (NGI)
IAFIS-DOC-01078-8.001	Electronic biometric transmission specification	$$$ (NGI, CPL)
ICAO LDS 1.7	Machine readable travel documents Development of a logical data structure	$
NISTIR 7151	Fingerprint image quality	$$$ (PIV, NGI)
NISTIR 7296	MINEX–Performance and interoperability of the INCITS 378 fingerprint template	$$$ (PIV, NGI)
OASIS XCBF 1.1	XML common biometric format	$

6 Other Technologies of Interest

There are relevant technology trends pushing the state-of-the-art in imaging, image processing, and computer vision. These technologies may enable significant opportunities in terms of new data sources and computational advancements for biometrics. Some select examples follow.

6.1 Gigapixel Imaging

Gigapan is a project that is applying and developing commercially affordable gigapixel photography and processing techniques. The project is joint research involving Carnegie Melon University, NASA/Ames Research Center, Google Corporation, Charmed Labs LCC, and DeepLocal Inc.

Large, high-quality, reference images of an area over time enable powerful forensic capabilities. Depending on the application environment, some degree of automation can be achieved by utilizing and combining image detection and extraction technologies for faces, vehicles, and other image content. References and examples follow (viewed December 09, 2007):

- Gigapan project, http://gigapan.org/
- Charmed Labs, http://www.charmedlabs.com/
- Carnegie Mellon University, http://www.cs.cmu.edu/~globalconn/overview.html.

6.2 Next Generation Commodity Hardware

The gaming and computer graphics industries continue to help advance and consume hardware platforms that provide high performance image processing. With the exception of some first generation match-on-card fingerprint devices, dedicated hardware solutions have seen only limited adoption in biometrics systems. Examples of specialized hardware platforms include multi-core processors, Graphics Processing Units (GPUs), and Field Programmable Gate Arrays (FPGAs).

With the FBI's desire to move to open standards and open architecture systems, it becomes increasingly feasible to consider embedded implementations on dedicated, low-cost, high-performance commodity hardware. References and examples follow:

- NCSU Playstation Cluster, http://news.ncsu.edu/releases/2007/march/041.html
- NVIDIA CUDA, http://developer.nvidia.com/object/cuda.html
- Xilinx FPGAs, http://www.xilinx.com/
- The MITRE Corp., www.mitre.org/news/events/tech07/3064.pdf.

6.3 Super-Resolution Image Reconstruction

Super-resolution (SR) uses image reconstruction techniques to obtain a high-resolution image from multiple lower-resolution images. Spatial resolution in images is degraded by motion blur, aliasing, and optical distortions during digital recording. The goal of SR is to overcome these artifacts.

A related trend and application for SR techniques is in the use of camera systems comprised of multiple sensors in array with overlapping regions. The overlapping regions provide redundant frame information that can potentially be fused in to a single image of higher spatial resolution (and less temporal resolution).

Some definitions consider SR to be any technique that provides improvement in image resolution or visibility. Stricter definitions consider only techniques and applications that surpass the limitations of defraction from the imaging system that generated the images.

Appendix A Acronyms

ABIS	Automated Biometric Identification System
ACE-V	Analysis Comparison Evaluation Verification
AFIS	Automated Fingerprint Identification Systems
ANSI	American National Standards Institute
APB	Advisory Policy Board
API	Application Program Interface
AQ	Acquisition Quality
ATM	Automated Teller Machine
BAT	Biometrics Automated Toolkit
BSC	Biometric Security Consortium
BTF	Biometric Task Force
BTG	British Technology Group
CBEFF	Common Biometric Exchange Formats Framework
CCH	Computerized Criminal History
CDEFFS	Committee to Define an Extended Fingerprint Feature Set
CESG	Communications Electronics Security Group
CJIS	Criminal Justice Information Systems
CMC	Cumulative Match Characteristic
CODIS	Combined DNA Index System
COE	Center of Excellence
CPL	Certified Products List
CR	Credential Operation
CT	Computerized Tomography
DHS	Department of Homeland Security
DNA	Deoxyribonucleic Acid
DoD	Department of Defense
DoJ	Department of Justice
DoS	Department of State
DS	Data Storage
EBGM	Elastic Bunch Graph Matching
EBTS	Electronic Biometrics Transmission Specification
EFTS	Electronic Fingerprint Transmission Specification

ELFT	Evaluation of Latent Fingerprint Technologies
FAR	False Alarm Rate
FBI	Federal Bureau of Investigation
FEARID	Forensic Ear ID
FFRDC	Federally Funded Research and Development Center
FIDIS	Future of Identity in the Information Society
FIQM	Fingerprint Image Quality Measurement
FOCI	Foreign Ownership Control and Influence
FPGA	Field Programmable Gate Arrays
GOTS	Government Off-The-Shelf
GPU	Graphics Processing Units
HSPD	Homeland Security Presidential Directive
IAFIS	Integrated Automated Fingerprint Identification System
IAI	International Association for Identification
IBG	International Biometric Group
ICAO	International Civil Aviation Organization
ID	Image Data
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIETF	IAFIS Interface Evaluation Task Force
INCITS	International Committee for Information Technology Standards
INCITS/M1	International Committee for Information Technology Standards Technical Committee (M1)
INSTAC	Information Technology Research and Standardization Center
ISO	International Standards Organization
IT	Information Technology
ITAR	International Traffic and Arms Regulations
ITL	Information Technology Laboratory
ITU	International Telecommunications Union
JPEG	Joint Photographic Expert Group
JTC1	Joint Technical Committee

KST	Known and Suspected Terrorists
LDA	Linear Discriminate Analysis
MA	Massachusetts
MBARK	Multimodal Biometric Application Resource Kit
MINEX	Minutiae Interoperability Exchange
MPS	Ministry of Public Security
MSc	Message Sequence Chart
NBIS	NIST Biometric Image Software
NCIC	National Crime Information Center
NEC	Nippon Electric Company
NFIQ	NIST Fingerprint Image Quality
NGI	Next Generation Identification
NISP	National Industrial Security Program
NISPOM	NISP Operating Manual
NIST	National Institute of Standards and Technology
NISTIR	National Institutes of Standards and Technology Interagency Report
NSTC	National Science and Technology Council
OASIS	Organization for the Advancement of Structured Information Standards
ONR	Office of Naval Research
OS	Operating System
PC	Personal Computer
PIV	Personal Identity Verification
PPI	Pixels Per Inch
R&D	Research and Development
RAM	Random Access Memory
RCMP	Royal Canadian Mounted Police
RFID	Radio Frequency Identification
ROC	Receiver Operating Characteristic
ROI	Regions of Interest

SA	Special Agent
SABER	State of the Art Biometrics Excellence Roadmap
SC37	ISO/IEC/JTC1 Standards Committee on Biometrics
SDK	Software Development Kit
SFCD	Supplemental Fingerprint Card Data
SFinGe	Synthetic Fingerprint Generation
SMT	Scar Mark and Tattoo
SOA	Services Oriented Architecture
SOP	Standard Operating Procedures
SWGFAST	The Scientific Working Group for Function Ridge, Anaylsis, Study, and Technology
TAR	True Accept Rate
TE	Testing and Evaluation
TOT	Types of Transactions
TS	Technical Specification
U.S.	United States
UK	United Kingdom
ULW	Universal Latent Workstation
VTB	Verification Test Bed
WAN	Wide Area Network
WSQ	Wavelet Scalar Quantization
XCBF	XML Common Biometric Format
XML	Extended Markup Language

Appendix B Glossary

Term	Definition
Candidate List	The list of potential mates listed in descending order of their matching scores as determined by the matching process within the Fingerprint Minutiae Matcher. A candidate list can be produced by III automated subject search.
Coder	Term for hardware, software or both used to detect minutiae in a finger image
Encoding	AFIS process used to record minutiae
Features Extraction	The system capability to identify, from a scanned fingerprint digital image, separately definable attributes that may be discretely stored and used to classify and uniquely identify that fingerprint. The AFIS/FBI design provides a means of automated features extraction.
Fingerprint Features	Unique physical characteristics of a fingerprint that are used to perform automated fingerprint searches.
Fingerprint Minutiae Matcher	The matching subsystem equipment that compares the minutiae data-based features of a search print with fileprints, and selects the fileprint that comes closest to matching the search print.
Fingerprint Plain Impressions	Fingerprint impressions taken by simultaneously capturing all of the fingers of each hand and then the thumbs without rolling, using a pressed or flat impression.
Fingerprint Rolled Impressions	The impressions created by individually rolling each inked finger from side to side, in order to obtain all available ridge detail.
Latent Fingerprint	A fingerprint impression left at a crime scene by touching, holding, or moving an object that has a firm surface. Typically, several latent fingerprints are overlaid and/or only portions of the print are available.
Livescan	An electronic method of taking and transmitting fingerprints without using ink that produces fingerprint impressions of high quality to perform identification processing.
Lights Out	An AFIS search without any human intervention at verification, also known as unsupervised matching.

Matcher	An AFIS component that compares the minutiae database features of a search print with file prints and selects the file print that comes close to matching the search print.
Minutiae	Friction ridge characteristics used to individualize a print. Minutiae occur at points where a single friction ridge deviates from an uninterrupted flow. Deviation is either in the form of a ridge ending or dividing into two or more ridges (bifurcation).
Palm prints	An inked and rolled or Livescan of the palm prints of both hands. May include the side of the hand, referred to as the writer's palm.
Rolled Impression	Fingerprint impressions created by individually rolling each finger from side-to-side (nail-to-nail) to obtain all available friction ridge detail. The images appear in the individual print boxes on the tenprint card.
Upgrade	Introduction of new software and/or hardware into an existing system. The upgrade may be to fix certain known problems unique to one AFIS customer; fix known problems applicable to all customers; an improvement to the AFIS system not related to a problem, or a move to a new platform such as from a Windows-based system to Linux, or Windows XP to Windows VISTA. The upgrade may require extensive on-site testing prior to installation on the live system.

Appendix C References

Adler A., J. Maclean. September 20-22, 2004. *Performance Comparison of Human and Automatic Face Recognition.* Biometrics Consortium Conference. Washington, D.C.

Authenti-Corp. 2006. *IRIS recognition study 2006 (IRIS06) aka Standards-Based Performance and User Cooperation Studies of Commercial Iris Recognition Products (version. 0.40)*. Phoenix, AZ. March 31, 2007. p. 1-168.

Bledsoe W.W. 1966. "*Man-machine facial recognition."* Tech. Rep. PRI:22, Panoramic Res., Palo Alto, CA, August 1966.

Bouchard, A.M., G.C. Osbourn. 1998. U.S. Patent 5,787,187. *"Systems and Methods for Biometric Identification Using the Acoustic Properties of the Ear Canal."* Awarded July 1998 to the Sandia Corporation, Albuquerque, NM.

Burge, M., W. Burger. 1999. "Ear Biometrics." Chapter 13 of *Biometrics: Personal Identification in a Networked Society*. Ed. Jain, A. et al., Kluwer Academic Publishers.

Carreira-Perpinan, M.A. 1995. "Compression Neural Networks for Feature Extraction: Application to Human Recognition from Ear Images" (Spanish). MSc Thesis, Faculty of Informatics. Technical University of Madrid. Spain.

Centre for Mathematics and Scientific Computing, National Physical Laboratory. 2001. *Biometric Product Testing Final Report.* Middlesex, UK. p. 1-22.

Cieri, C., J. Campbell, H. Nakasone, D. Miller, K. Walker. *The Mixer Corpus of Multilingual, Multichannel Speaker Recognition Data.* University of Pennsylvania, Linguistic Data Consortium, Philadelphia, PA. MIT Lincoln Laboratory, Lexington, MA. Federal Bureau of Investigations, Quantico, VA.

Daon Systems. 2007. *"Biometrics and Identity Assurance Standards and Middleware."* Presentation by Cathy Tilton to the MITRE Corporation. November 19, 2007.

Daubert vs. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).

Federal Bureau of Investigations and National White Color Crime Center. Internet Crime Complaint Center. January 1, 2006-December 31, 2006. *2006 Internet Crime Report.* http://www.ic3.gov/media/annualreport/2006/_IC3Report.pdf

Grother, P. 2002. *Face Recognition Vendor Test 2002 Supplemental Report NISTIR 7083*. p. 1-32.

Grother, P., E. Tabassi. April 2007. "Performance of Biometric Quality Measures." *IEEE Transactions of Pattern Analysis and Machine Intelligence*, 29(4). p. 531-543.

Hu, Q. 2005, 2006. *Audio Hotspotting for Tactical and Intelligence Applications.* The MITRE Corporation, McLean, VA. (MITRE Technology Program, Army Contract Mission Oriented Investigation and Experimentation).

International Biometrics Group. 2006. *Comparative Biometric Testing, Round 6 Public Report.* New York, NY. p. 1-117.

International Biometrics Group. 2005. *Independent Testing of Iris Recognition Technology.* New York, NY. p. 1-242.

Malkin, M. December 21, 2006. *Pranking the DMV.* http://michellemalkin.com/2006/12/21/pranking-the-virginia-dmv/ [viewed December 14, 2007].

R. Martin and J. Barresi (eds.), 2002. *Personal Identity*. Oxford: Blackwell Publishing.

Mayer-Splain, J. 2006. *A World of Biometric Standards: A Primer and Update.* Mitretek Systems Center for Information and Telecommunications Technologies. Falls Church, VA. p. 1-30.

Meijerman, L. 2006. *Earprints as Evidence.* Leiden University. http://research.leidenuniv.nl/index.php3?c=160

National Institute of Standards and Technology. NIST Speech Group. http://www.nist.gov/speech/

National Science and Technology Council Subcommittee on Biometrics. August 2006. *National Biometrics Challenge Document.* National Science and Technology Council.

H.W. Noonan, 2003. *Personal Identity*, 2nd ed., Routledge.

O'Toole, A.J., J. Phillips, F. Jiang, J. Ayyad, N. Pennard, H. Abidi. *Face Recognition Algorithms Surpass Humans'.*

Penev, P.S., J.J Attick. 1996. "Local Feature Analysis: A General Statistical Theory for Object Representation." *Neural Systems*, 7:477.

Phillips, P.J., W.T. Scruggs, A.J. O'Toole, P.J. Flynn, K.W. Bowyer, C.L. Schott, M. Sharpe.. 2007. *FRVT 2006 and ICE 2006 Large-Scale Results.* National Institute of Standards and Technology: Gaithersburg, MD. p. 1-56.

Phillips, P.J., W.T. Scruggs, A.J. O'Toole, P.J. Flynn, K.W. Bowyer, C.L. Schott, M. Sharpe.. 2007. FRVT 2006 and ICE 200666 Large Scale-Results. National Institute of Standards Technology: Gaitherburg. MD. p. 1-56.

Physorg.com. *Earprints as evidence?* http://www.physorg.com/printnews.php?newsid=11177 [viewed December 9, 2007].

Schneier, B. December 22, 2006. *Schneier on Security.* http://www.schneier.com/blog/archives/2006/12/not_paying_atte.html [viewed December 14, 2007].

L. Sirovich and M. Kirby. 1987. ``Low-dimensional procedure for the characterization of human faces", *Journal of the Optical Society of America*, 4(3), 519-524.

S. Shoemaker and R Swinburne, 1984. *Personal Identity*, Blackwell.

Ulery, B., A. Hicklin, C. Watson.. 2006b. *Studies of Biometric Fusion Appendix A: Terminology, Experimental Design and Data Description.* National Institute of Standards and Technology Gaithersburg, MD. p. 1-20.

University of Notre Dame. 2007. *Image Understanding for Iris Biometrics: A Survey.* Notre Dame, Indiana.

University of Pennsylvania. Linguistic Data Consortium. http://www.ldc.upenn.edu/

Watson, C.I., C.L. Wilson. 2005. Effect of Image Size and Compression on One-to-One Fingerprint Matching NISTIR 7201. p. 1-40.

Wilson, C.L., C.I. Watson, M.D. Garris, A. Hicklin. Studies of Fingerprint Matching Using NIST Verification Test Bed (VTB). p. 1-99.

L Wiskott, J.M. Fellous, N. Kruger, C. vonder Malsburg 1997 "Face Recognition by Elastic Bunch Graph Matching, Lecture Notes In Computer Science" Vol. 1296 archive
Proceedings of the 7th International Conference on Computer Analysis of Images and Patterns
Pages: 456 – 463.