Biometrics Overview of the PATRIOT Act

C. L. Wilson
Manager, Image Group

Statutory Mandates

- USA Patriot Act (PL 107-56)
- Enhanced Border Security and Visa Entry Reform Act (PL 107-173)
- Develop and certify technology standard to
  - verify identity of foreign nationals applying for a visa
    - visa application at embassies and consulates
    - background check against FBI criminal database and DHS databases and “watch lists”
    - ensure person has not received visa under a different name
  - verify identity of persons seeking to enter the U.S.
    - verify that the person holding the travel document is the same person to whom the document was issued
    - airports, land border crossings, sea entry points

Statutory Mandates (cont)

- NIST worked together with Dept of Justice (including FBI & JMD) Dept of Homeland Security and Dept of State to develop a report on these activities to Congress under section 303a of the Border Security Act
- NIST must determine estimates of the accuracy of biometrics in the 303a report and subsequent mandatory reports.
- NIST must establish document authentication standards for tamper-resistant travel documents in the 303a report which should not conflict with ICAO mandates
- NIST must provide interoperability standards

Status of NIST Patriot Act Projects

- Biometric accuracy determination requires use of large-scale databases for testing.
- Large realistic test samples of images have been obtained from the State Department, Homeland Security and Justice Departments and Texas, Ohio, and California.
- Initial testing will be of face and fingerprints. A large sample of iris data is presently being planned.
- All tests conducted by NIST use image-based biometrics. No tests using templates for face and fingerprint have been conducted. Most vendors state that their products only work when their proprietary templates are used.

Results Presented in the Report to Congress

- Results show that fingerprints and face provide similar accuracy for verification when image quality is well controlled. Uncontrolled face image quality results in a rapid accuracy decrease to less than 50%.
- Using realistic DHS (INS) data, one index fingerprint can provide 90% probability of verification with a 1% probability of false acceptance for verification using current commercial technology.
- Tests show that for the best commercial systems using well controlled State Department data, face recognition can provide 90% probability of verification with a 1% probability of false acceptance for verification. Outdoor illumination results in 47% probability of verification.
- Large scale identification requires four or more fingerprints. Ten flat fingerprints were recommended.

BIOMERTIC TESTING IS SCALE DEPENDENT

- SAMPLE SIZE 100-1,000
  Proves feasibility
- SAMPLE SIZE 1,000-10,000
  Measures subject variation
- SAMPLE SIZE 10,000-1,000,000
  Measures operational quality control
- Existing government databases contain millions of entries and have widely varying quality.

ONLY IMAGE BASED BIOMETRICS ARE INTEROPERABLE

- All fingerprint vendors claim significant accuracy loss using templates that are not their own unique proprietary pattern or minutia based templates.
- No common face template has been accepted.
- The only Iris template in use is proprietary. After these projects started an image based iris exchange standard was developed.

DATA QUALITY IS CRITICAL

- Existing high quality public database will yield optimistic results.
- Archival databases contain data of widely variable quality.
- Demographic factors will affect the accuracy of future systems.

Fingerprint Data Sets

NAME	SCAN TYPE	PLAIN	ROLL	TESTS	SIZE	QUALITY
SD 14 (V2)	Ink/live		10	Roll:Roll	2,700 Card Pairs	Medium
SD 24	Live (DFR-90)	10		Plain:Plain	80 Fingers	Good
SD 29	Ink	10	10	Roll:Roll Plain:Plain Plain:Roll	216 Card Pairs	Medium
BICE INDEX	Live	Index		Plain:Plain	620K Subjects 3M Images	Operational
STATE INDEX	Live	Index		Plain:Plain	6M Images	Operational
BICE CRIMINAL	Live	10	10	Plain:Roll	100K Cards	Operational
TX	Ink/live	10	10	Plain:Roll	600K Cards	Operational
IAFIS	Ink/Live		10	Roll:Roll Plain:Roll	1.2M Cards	Operational
ESD	Live	10	10	Plain:Roll	3K Cards	Good

Face Data Sets

NAME	IMAGE TYPE	VIEWS	SIZE	QUALITY
INS FACE	JPEG	2	620K Subjects 1.25M Images	Operational
STATE	JPEG	1 or 2	6.3M Images 388K Pairs	Operational
HUMANID	JPEG	20	859 Subjects	Controlled
FERET	TIFF	12	1204	Controlled

FINGERPRINT STUDIES

- Data quality determines the results
- Lab Quality Data
  - NIST SD published data
  - Used to investigate Rolled-Rolled, Plain-Rolled, and Plain-Plain matching
- Operational Quality Data
  - New live scan data
  - Typical law enforcement data
  - Low quality data
- Operational Systems
  - Track NIST public domain matcher but with similar accuracy.

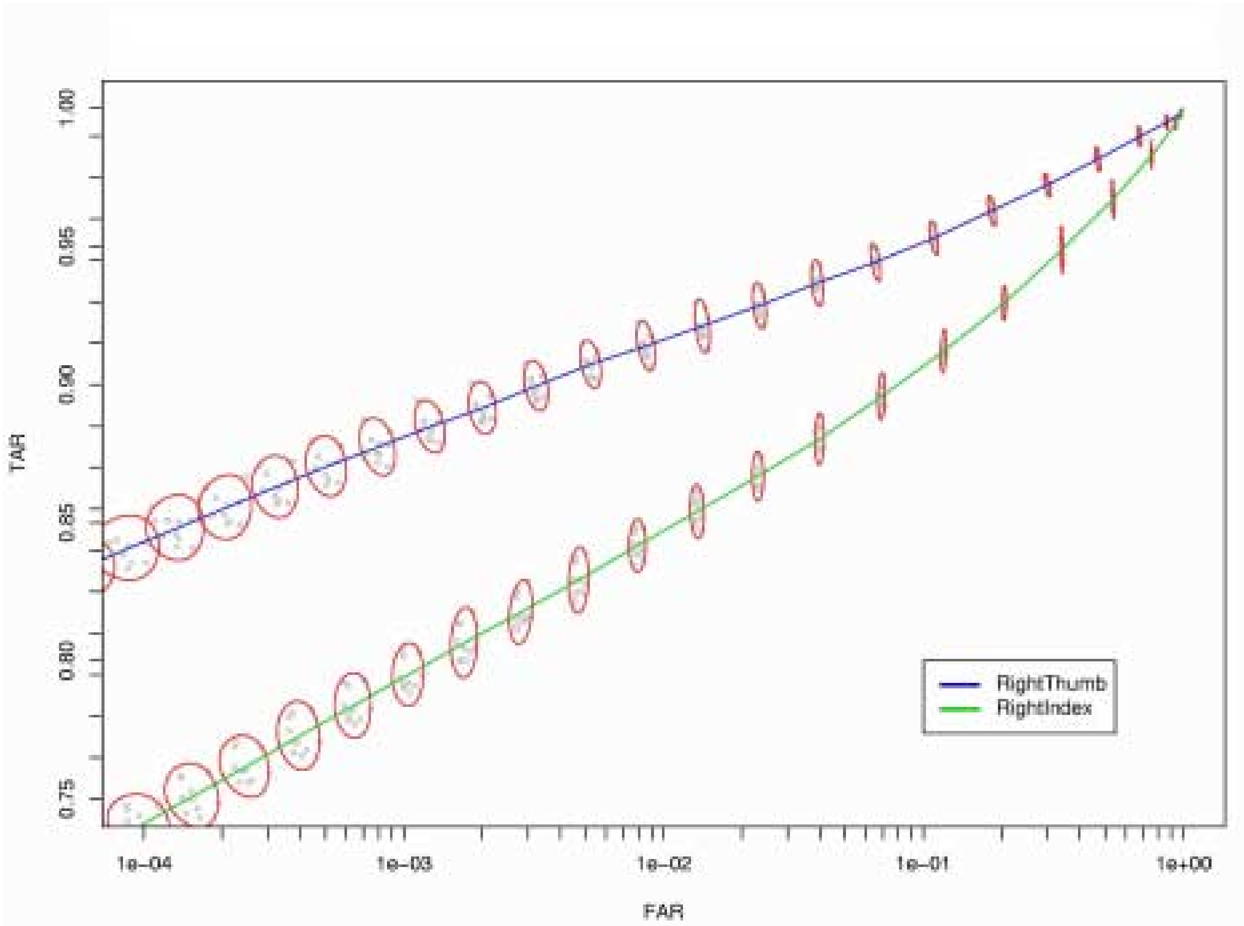
FINGERPRINT EVALUATION IS MULTIVARIENT

- Image quality is a very critical parameter see: ftp://sequoyah.nist.gov/pub/nist_internal_reports/ir_7020.pdf
- Algorithms are important but vary widely in sensitivity to image quality.
- Multi finger fusion is required for many applications.

Operational Fingerprint Data

- May include failure to register data
- Can be nonstationary in the usual time series sense
- Has demographic variations which may be or may not be nonstationary
- Usually contains source specific factors which cause variations

Comparison of Thumb and Index Finger Verification Using DHS 10 Print Data



Large Scale Identification

- Database sizes will approach 50M
- Existing AFIS system
  - Use 10 rolled fingerprints
  - Filter the database to reduce the required matches
- NIST tests track with known IAFIS results
  - hard and easy data sets are still hard and easy
  - failure to acquire rates are similar

Commercial AFIS Testing Is More Complex

- Commercial system usually have data screening, a primary matched, and multi-finger score resolution.
- Commercial systems use data screening to reduce database size.
- The primary matcher then matches the reduced database.
- Additional matches are used to resolve near matches.

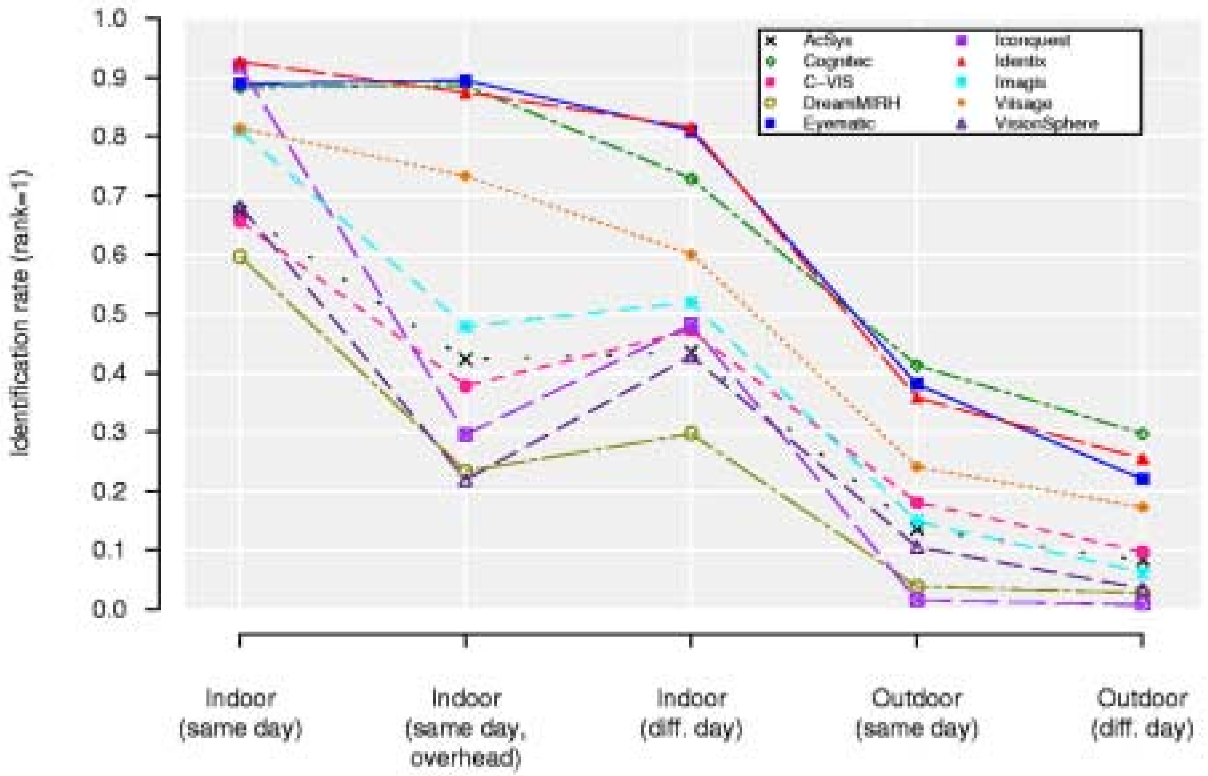
FACE STUDIES

- FRVT 2002 established a baseline for the capabilities of existing commercial technology.
- Demographic sources of variation were characterized using operational DOS data.
- Error rates were cut in half from the FRVT 2000 test.

Factors Beyond the Control of the System Developers Are Important

- Demographic
  - Age
  - Gender
- Source Conditions
  - Time Since Image Capture
- Archival
  - Illumination
  - Type of Input Device

Identification as a Function of Illumination



FACE VERIFICATION

- Used 3 copies of 37,437 well controlled visa images from the State Department
- Achieved 90% probability of verification at 1% false accept rate
- Achieved 70% probability of verification at 0.01% false accept rate
- Using outdoor illumination, face achieves 47% probability of verification at 1% false accept rate

IDENTIFICATION USING FACES

- Used 37,437 well control1ed State Department visa pictures.
- Achieved 86% probability of identification at rank one on a gallery size of 500.
- Achieved 77% probability of identification at rank one on a gallery size of 10,000.

NIST 303a Conclusions

- Not all subjects can be easily fingerprinted with existing technology. About 2% of subjects have damaged friction ridges.
- The intelligence community often only has face data.
- This indicates that a dual biometric system including two fingerprint images and a face image is needed to meet existing verification system requirements.

NIST 303a Conclusions

- For identification 10 flat fingerprints were recommended and at least four are essential. Existing sensor technology dictates 8 or 10.
- Face may be used for hard to fingerprint individuals.

Expect New Results

- Analysis and testing for both face and fingerprints is continuing.
- New questions are being raised by both the entry-exit agencies and Congress.
- New data is being acquired.
- New test are performed - FpVTE

SDK Testing - 8 Algorithms, 12 datasets, 3.46G matches