Biometrics of Fingerprint and Facial Images

C. L. Wilson

Image Group

IAD-ITL

Outline

- Statutory mandates for Patriot Act testing
- NIST Patriot Act recommendations
- Tests of COTS biometric accuracy
  - FpVTE
  - SDK tests
  - IDENT
- Image quality

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

NIST Patriot Act Recommendations

- One-to-One Matching
  - Two Index Finger Images and One Face Image
  - Fingerprint provide biometric accuracy, the face is for human verification.
- One-to-Many Matching
  - Ten Slap (Flat) Fingerprint Images
  - Existing larger archival government database will require ten prints because of archival image quality

How Were These Recommendations Decided?

- Both the Patriot Act and HSPD-12 schedules require COTS solutions.
- Competitive multi-vendor solutions are needed.
- The biometric components must be part of an integrated interoperable system.
- NIST must test these components to a Daubert (expert witness) standard.

What Test Sample Specifications are Required?

- Data should reflect the image quality that can be achieved using existing sensors in operational government applications.
- One-to-One: Test sample sizes should be 5,000-10,000 individuals.
- One-to-Many: Test sample sizes should be order of 1,000,000 individuals.
- Test samples must contain images of realistic quality .

Why Face and Fingerprints?

- ICAO specified face, fingerprints, and iris.
- Large operational quality samples of face and fingerprint data are available for test.
- No equivalent sample of vendor-neutral iris data exists.
- Face and fingerprints can operate with 0% Failure to Acquire rates. This rate is unknown for iris.

FpVTE

- The evaluations were conducted to
  - Measure the accuracy of fingerprint matching, identification, and verification systems
  - Identify the most accurate fingerprint matching systems
  - Determine the viability of fingerprint systems for near-term deployment in large-scale identification systems
  - Determine the effect of a wide variety of variables on matcher accuracy
  - Develop a well-vetted set of a variety of operational data for use in future research

FpVTE (continued)

- The evaluations were ***not*** intended to
  - Measure system throughput or speed
  - Evaluate scanners or other acquisition devices
  - Directly measure performance against very large databases
  - Take cost into consideration

FpVTE- Comparison of Systems

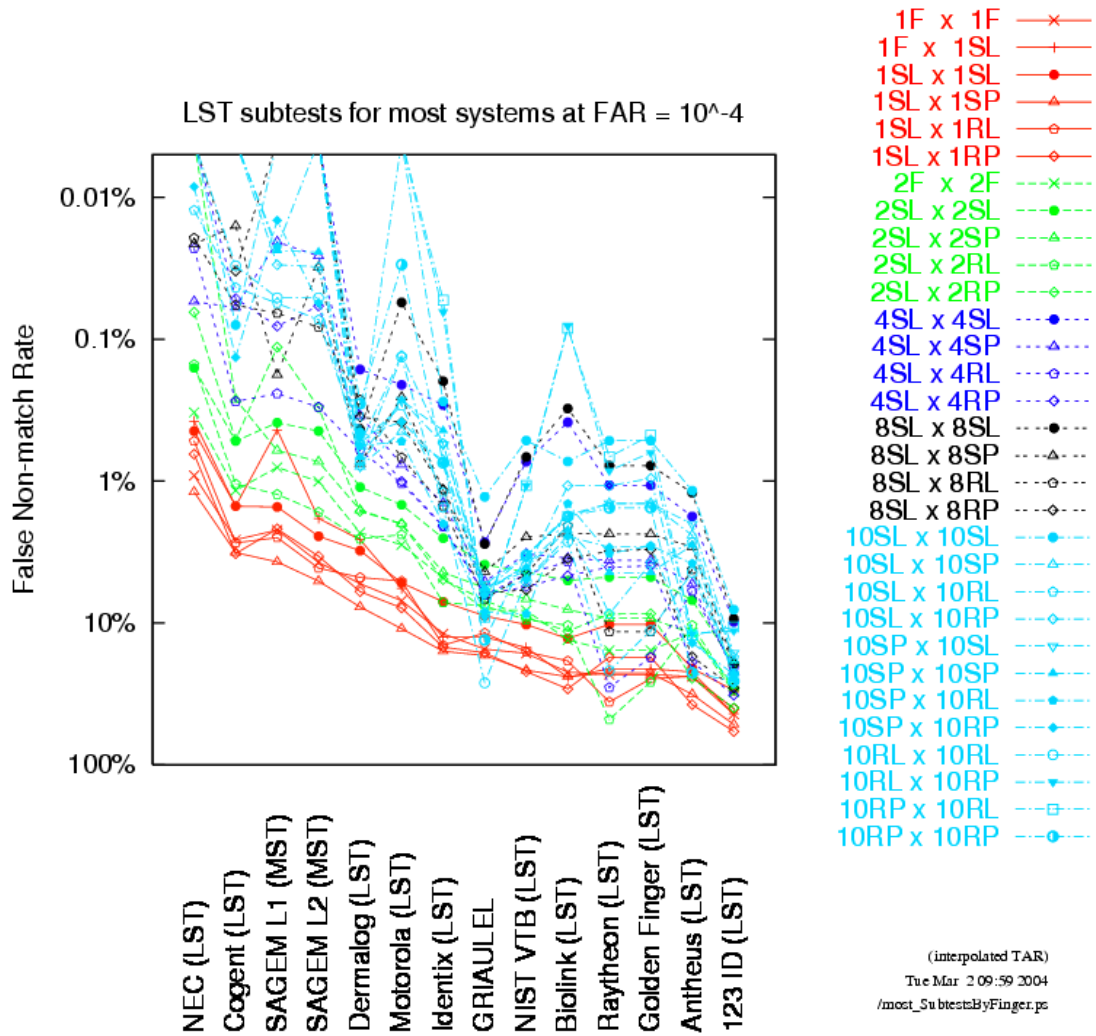
- There is a substantial difference in accuracy between the best systems and the average or worst systems
- The most accurate system were submitted by Cogent, NEC, SAGAM
- The top tier systems are more consistent in performance than the other systems
  - They perform consistently well over a variety of data, and are less affected by fingerprint quality and other variables
- The performance of the most accurate systems has been verified by SDK testing.

FpVTE Comparison with Face

The most accurate fingerprint systems are far more accurate than the most accurate face recognition systems. Fingerprints were evaluated on operational data from DOJ, DHS, and DOS. Faces were evaluated on DOS BCC data.

- The most accurate face systems:
  - 0.72 true accept rate @ 10^{-4} false accept rate
  - 0.90 true accept rate @ 10^{-2} false accept rate.
- The most accurate fingerprint system, using operational quality single fingerprints:
  - 0.994 true accept rate @ 10^{-4} false accept rate
  - 0.999 true accept rate @ 10^{-2} false accept rate

More Finger Are More Accurate



SDK Tests

Medium scale evaluation of
one-to-one matching for:
16 software matchers
20 single finger datasets

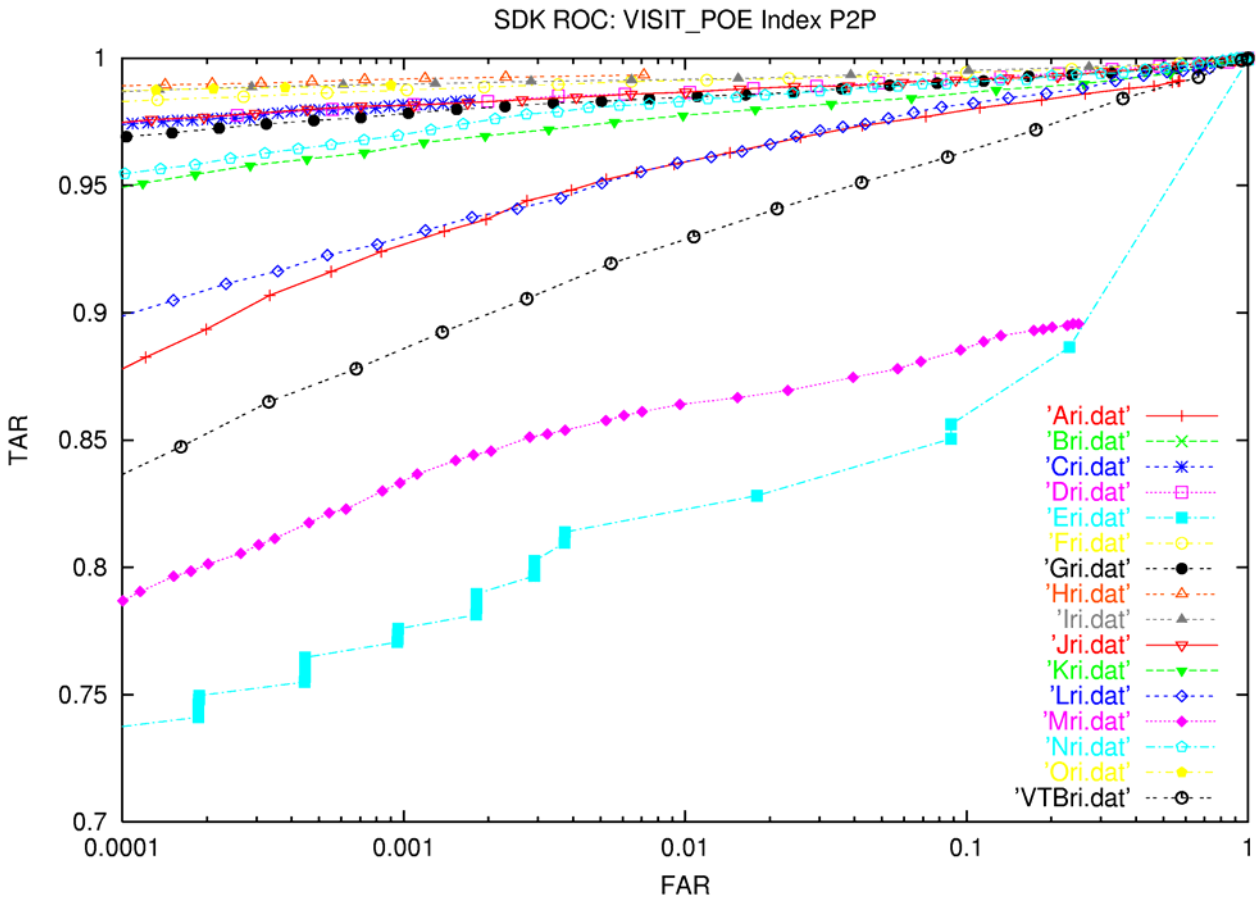
What were the goals of the test?

- Determine the feasibility of verification matching in the US-VISIT and DOS clients
- Evaluate vendor accuracy variability
- Evaluate vendor sensitivity to image quality
- Also used to scale the MST in FpVTE

Scale of Tests

- Each test involved 36M matches on a 3GHz Pentium platform.
- Gallery 6K probe 6K
- Match time must be less than 10ms per fingerprint pair
- Each test results in an ROC curve

SDK Testing - 16 Algorithms, POE right index, 0.576G matches



SDK LETTER	VENDOR NAME
A	Name Not Released
B	Name Not Released
C	NEC
D	Cogent Systems, Inc.
E	Name Not Released
F	Cogent Systems, Inc.
G	SAGEM Morpho, Inc.
H	NEC
I	Cogent Systems, Inc.
J	SAGEM Morpho, Inc
K	Neurotechnologija Ltd.
L	Name Not Released
M	Name Not Released
N	Dermalog
O	NEC
VTB	NIST

SDK - Conclusions

- All vendors are sensitive to image quality.
- Three algorithms vendors are clearly more effective.
- Combining two fingers will provide very effective one-to-one verification for the US-VISIT program TAR 99.6% FAR 0.1%
- The NIST VTB algorithm is better than many commercial products.

US-VISIT IDENT System

- IDENT is the primary fingerprint matcher for US-VISIT
- Three functions:
  - Watch list checking at enrollment
  - Duplicate identification check for visa holders
  - One-to-one verification for enrolled travelers

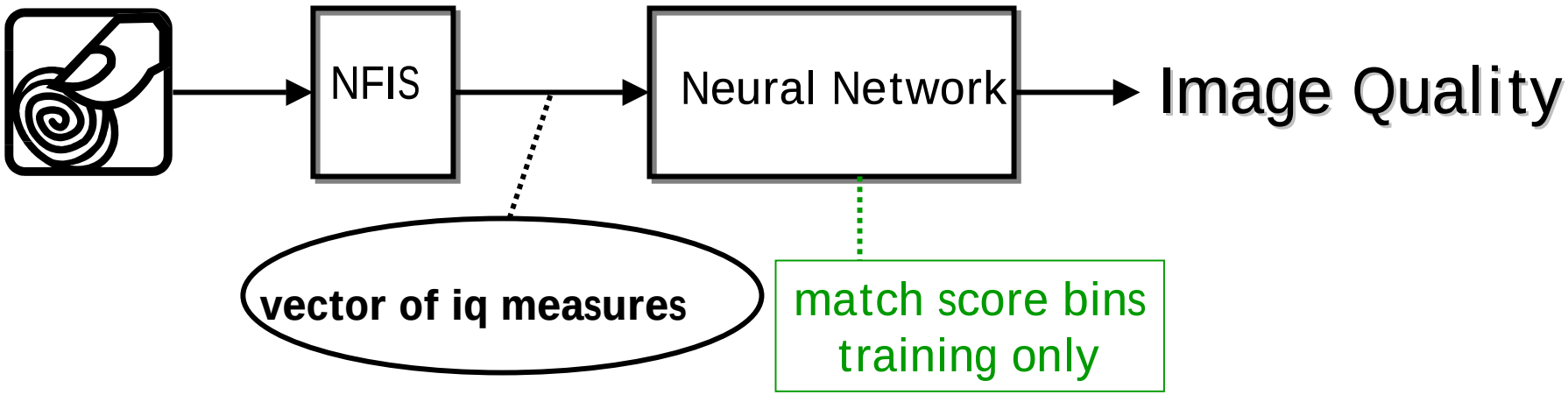
Conclusions On Accuracy of US-VISIT

- One-to-One
  - TAR of 99.6% at a FAR of 0.1%.
  - This has been tested operationally with an 800K sample size.
- One-to-Many
  - TAR 96% at a FAR of 0.09%
  - This has been tested on a database of 6,000,000
- The System Works

NIST Image Quality

- Define and develop a fingerprint image quality measure that can predict fingerprint recognition performance
- Use the ranking of ROC curves derived from different qualities of data to check the effectiveness of the quality measure.
- Not in terms of traditional image processing (contrast, SNR, …)
- BUT quality in terms of characteristics and features of a fingerprint that convey information for a matching algorithm

Predicting Performance From Image Quality



A fingerprint with image quality *n* {1,2,3,4,5} means that the match score for that fingerprint with be in bin *n*.

This Image Quality Measure Works

- The method has been tested by ranking ROCs from 14 SDK algorithms.
- The method has been tested using all 20 SDK datasets.
- In all 280 cases the image quality rank predicted matching performance.

Both Face and Fingerprints Are Dependent on Image Quality

- Face is pose and illumination dependent
  - Accuracy for face recognition falls as the angle with the camera increases.
  - Accuracy drops from 90% with controlled illumination to 53% with natural illumination.
- Fingerprint accuracy depends on the ability to detect ridge structure.
  - All tests discussed here assume 500 dpi resolution with eight bits of gray.
  - As NFIQ goes from 1 to 5 matching accuracy falls from 99.6% to 26%

NIST Image Quality Is Publicly Available

- The software is free but export controlled.
- All source code is provided.
- Contact: Craig.Watson@NIST.gov
- NIST image quality will be mandatory for FBI slap fingerprint submissions in March 2005
- A conformance test is being developed.
- All reports can be obtained from:
  fingerprint.nist.gov