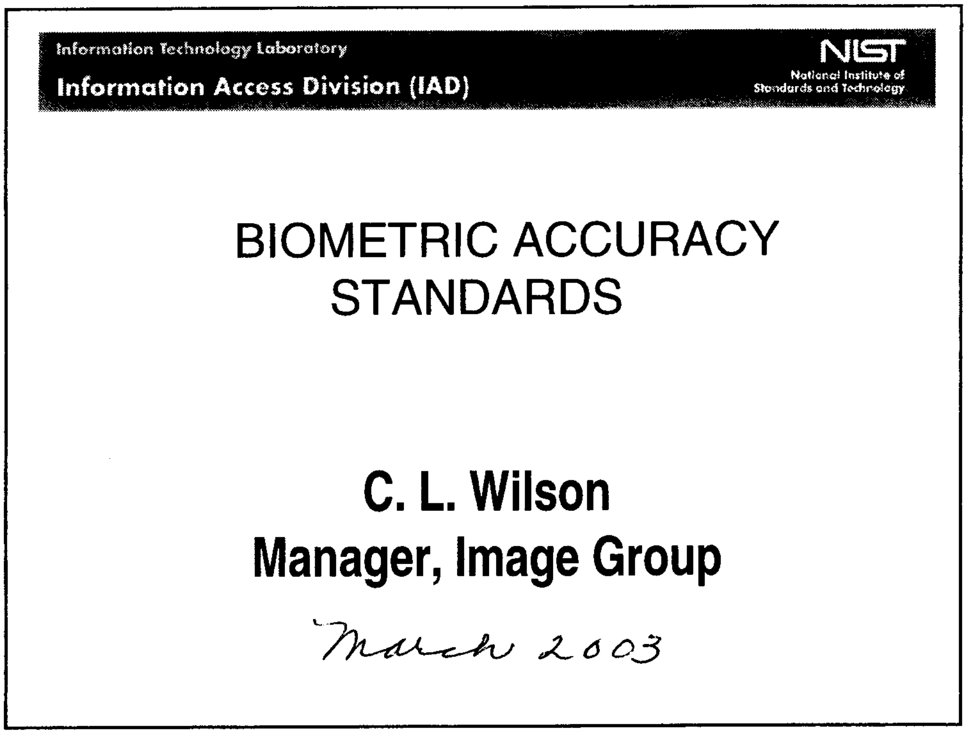


Information Technology Laboratory

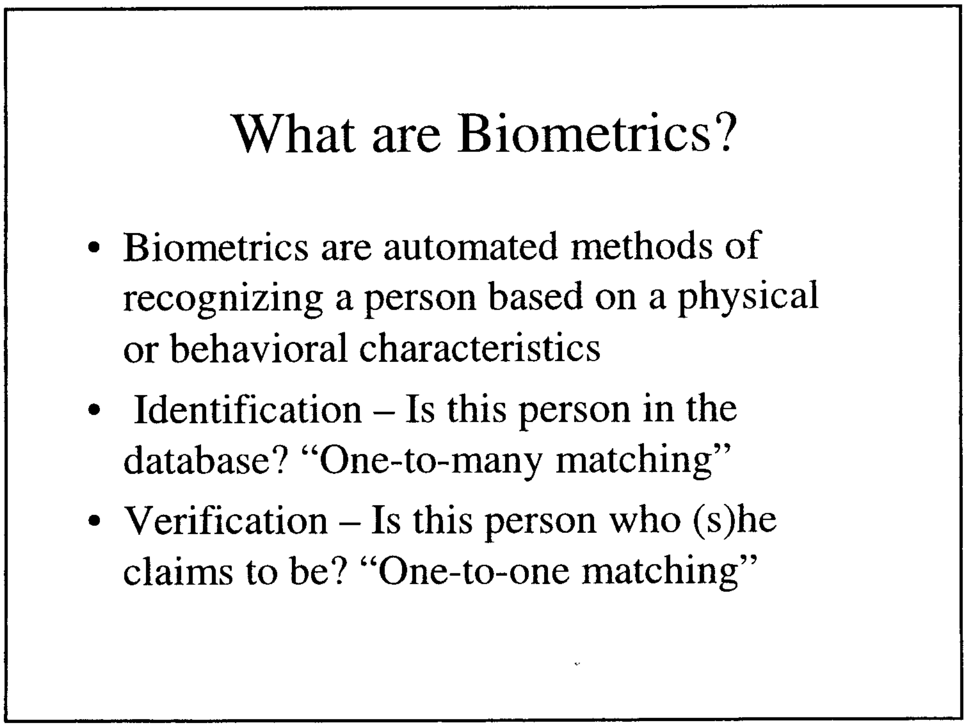
Information Access Division (IAD)

NIST
National Institute of Standards and Technology

BIOMETRIC ACCURACY STANDARDS

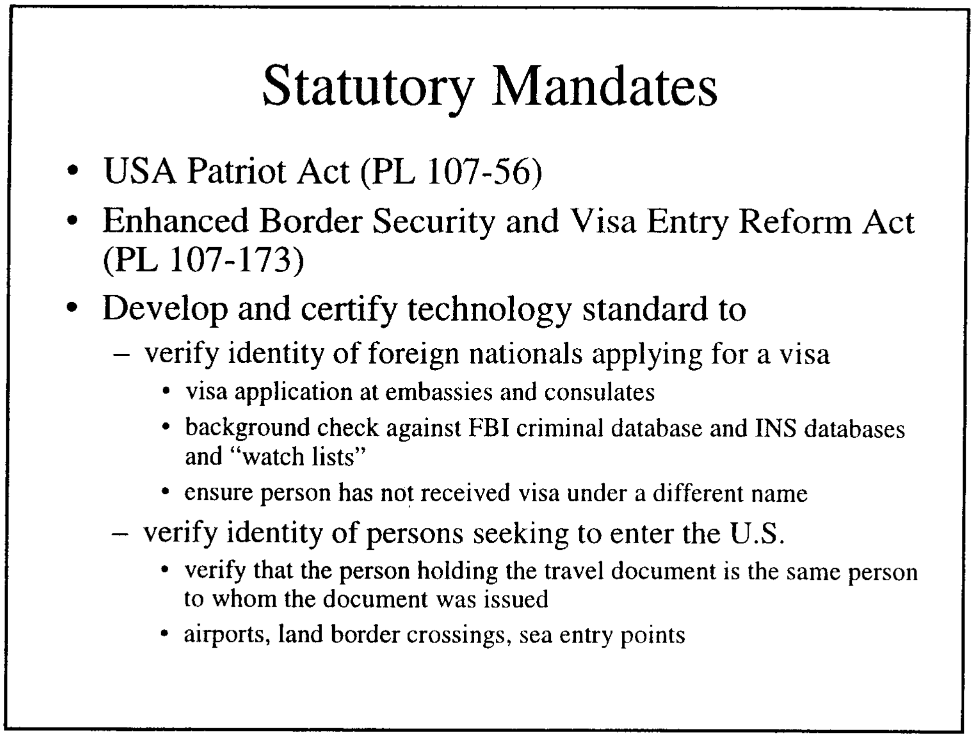
C. L. Wilson
Manager, Image Group

March 2003



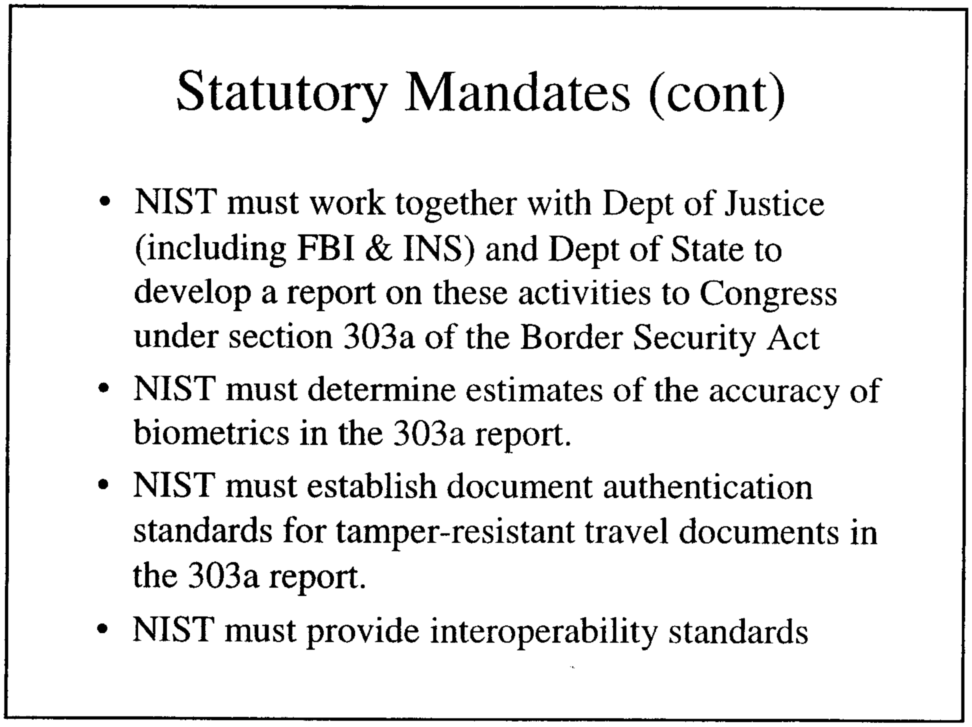
What are Biometrics?

- Biometrics are automated methods of recognizing a person based on a physical or behavioral characteristics
- Identification – Is this person in the database? “One-to-many matching”
- Verification – Is this person who (s)he claims to be? “One-to-one matching”



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 INS 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 must work together with Dept of Justice (including FBI & INS) 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.
- NIST must establish document authentication standards for tamper-resistant travel documents in the 303a report.
- NIST must provide interoperability standards

Status of NIST Patriot Act Biometric Standards

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

Status of NIST Patriot Act Biometric Standards (cont)

- Results show that fingerprints and face provide similar accuracy when image quality is well controlled. Uncontrolled face image quality results in a rapid accuracy decrease.
- Using realistic INS data, one index fingerprint can provide 90% probability of verification with a 1% probability of false acceptance for verification.
- 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 37% probability of verification.
- Previous work on fingerprint identity searches by Mitretek has shown that an acceptable identification can be obtained using four fingers in the FBI IAFIS. Further test with improved algorithms are being run at NIST.

BIOMERTIC TESTING DOES NOT SCALE

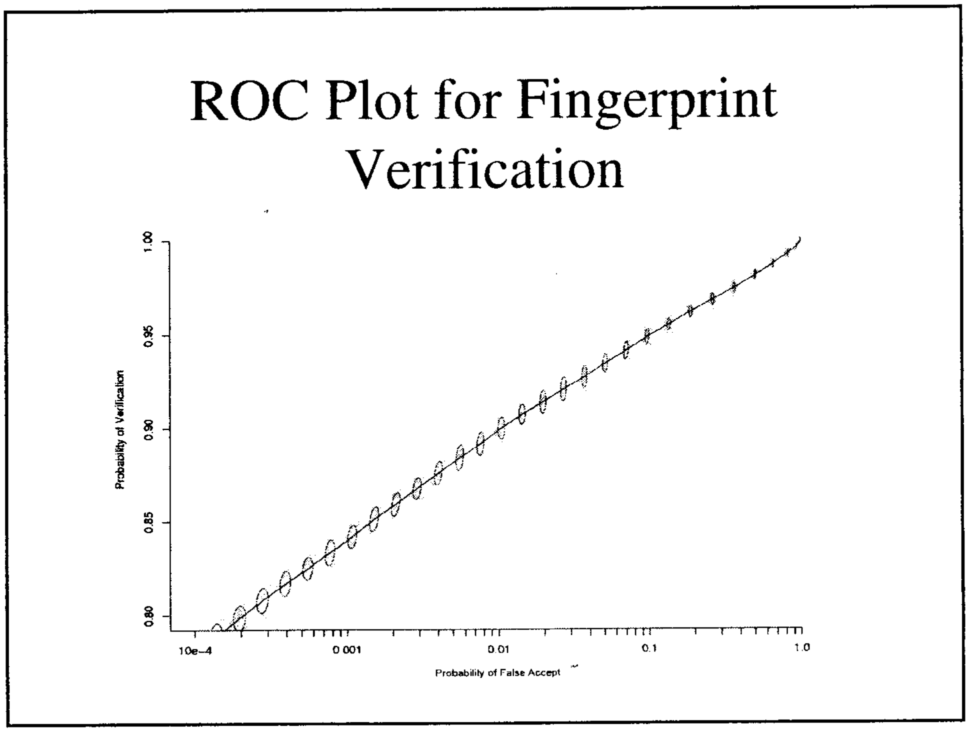
- SAMPLE SIZE 100-1,000
  Proves feasibility
- SAMPLE SIZE 1,000-10,000
  Measures subject variation
- SAMPLE SIZE 10,000-1,000,000
  Measures operational quality control

ONLY IMAGE BASED BIOMETRICS ARE INTEROPERABLE

- All fingerprint vendors claim significant accuracy loss using templates that are not their own unique proprietary templates.
- No common face template has been accepted.
- The only Iris template in use is proprietary.

FINGERPRINT VERIFICATION

- Used 60,000 operational quality fingerprints from the INS
- Achieved 90% probability of verification at 1% false accept rate
- Achieved 77% probability of verification at 0.01% false accept rate

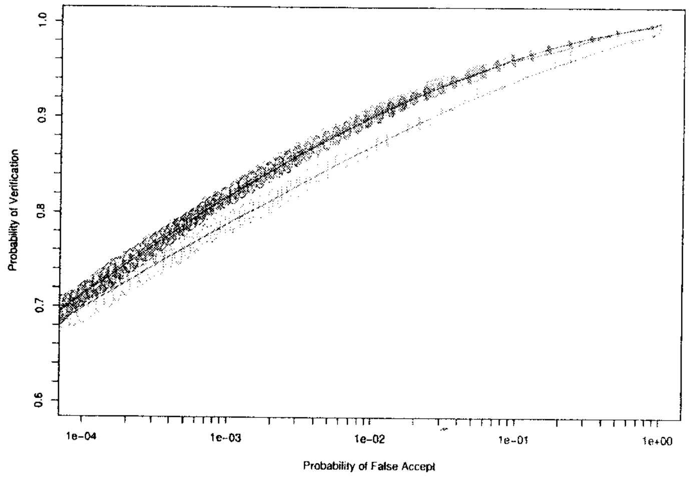


ROC Plot for Fingerprint Verification

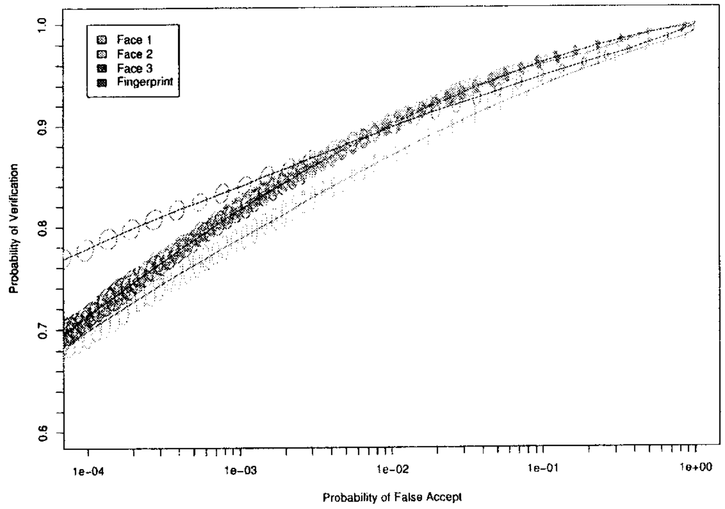
FACE VERIFICATION

- Used 4 copies of 37,000 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 37% probability of verification at 1% false accept rate

ROC plot for top 3 FRVT 2002 systems for face verification



ROC plot comparing face and fingerprints



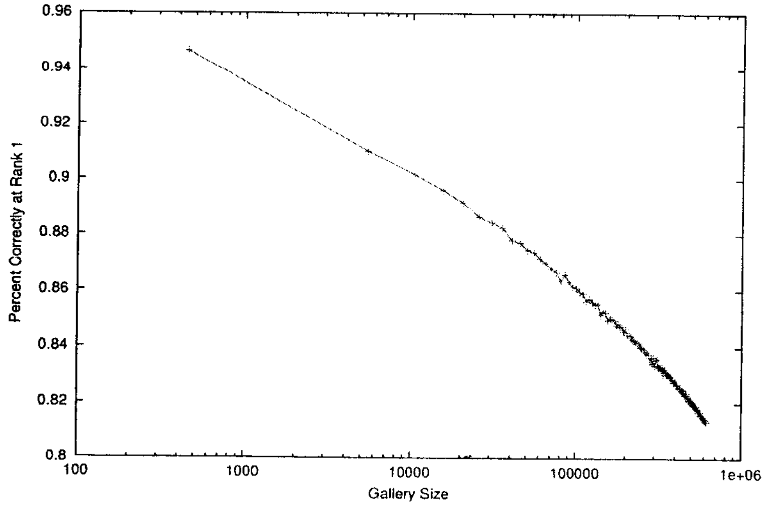
IDENTIFICATION

- This is a one-to-many match situation.
- Sample sizes need to be large enough to capture large scale image quality variations.
- Probability of detection with the highest score in a gallery of 10,000 fingerprints is 90% and for face it is 77% for the best tested face recognition system.
- Face consistently under-performs fingerprints on any gallery greater than 100.

FINGERPRINT IDENTIFICATION

- Used 620,000 operational quality fingerprint from the INS
- Achieved 96% probability of identification at rank one on a gallery size of 500.
- Achieved 90% probability of identification at rank one on a gallery size of 10,000.
- Achieved 86% probability of identification at rank one on a gallery size of 100,000.

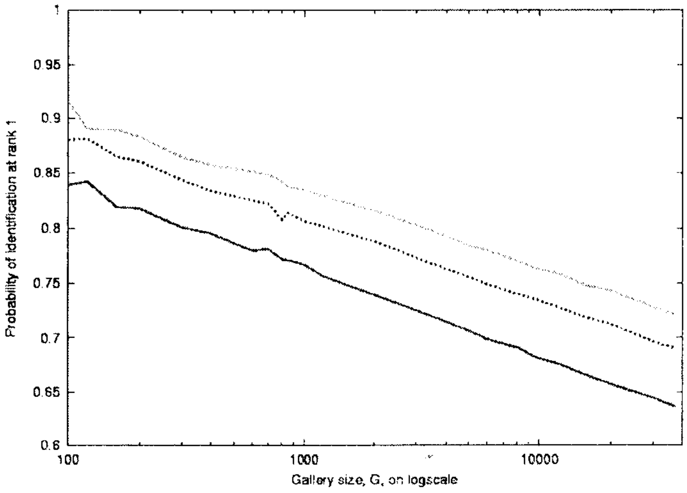
Probability of rank one detection for fingerprint vs gallery size.



IDENTIFICATION USING FACES

- Used 37,000 well controlled 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.

Probability of rank one detection for three best face systems vs gallery size



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 one or more fingerprint images and a face image is needed to meet existing system requirements.