Biometrics for Risk Based Screening

Jordan Cheney

10/17/18

Jordan.Cheney@noblis.org

noblis®

For the best of reasons

So What? Who Cares?

- Biometrics can be a powerful tool to enable TSA's Risk-Based Screening vision
- Performance is improving dramatically with advances in machine learning
- Biometric systems trade False Match Rate (FMR) and False Non-Match Rate (FNMR)
- TSA can design systems that adapt their FNMR / FMR operating points, recognizing that both are non-zero
- Performance differences persist between cooperative and non-cooperative biometrics
- TSA needs a continuous upgrade path to deploy future biometric performance gains
- Policy and use questions remain, but the public is warming to biometrics

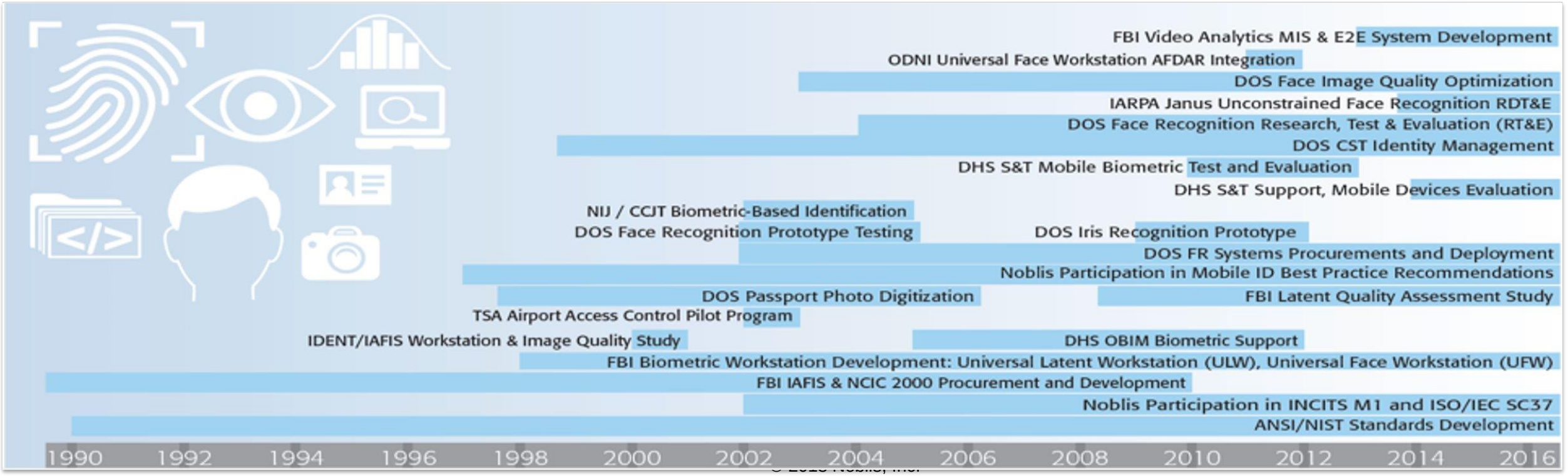
- Contact me: Jordan.Cheney@noblis.org, (703) 447-6291

noblis

Who is Noblis?

Noblis delivers creative, forward-thinking solutions that help our clients achieve their missions.

- Nonprofit, science, technology, and strategy company
- Work in the public interest
- Provide our clients with conflict-free solutions and have no ties to vendors or products
- Invest in research to build new capabilities

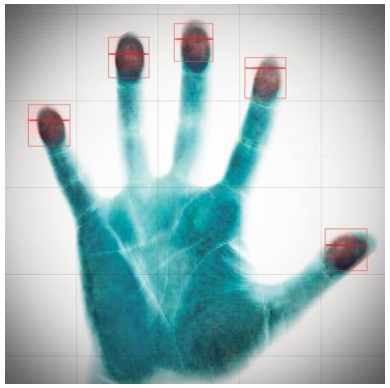


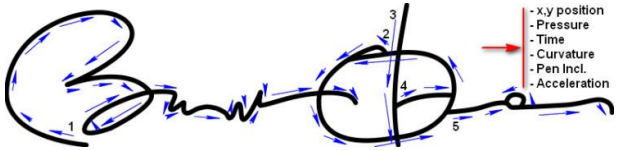
What is a Biometric?

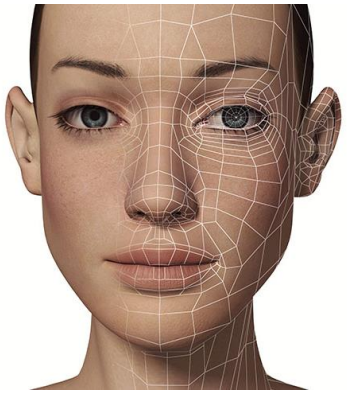
- Any anatomical or behavioral characteristic that is[1]:
  - **Universal:** Each person should have it
  - **Distinctive:** Any two persons are sufficiently different
  - **Permanent:** The characteristic should not vary (much) over time
  - **Collectable:** The characteristic can be measured quantitatively
- The viability of biometrics should be evaluated based on
  - **Performance:** Recognition accuracy and speed, in an operational environment
  - **Acceptability:** Are people are willing to accept an identifier's use?
  - **Circumvention:** Can the system be fooled using fraudulent methods?

1. A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Trans. on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, vol. 14, no. 1, pp. 4-20, January 2004

Type of Biometrics



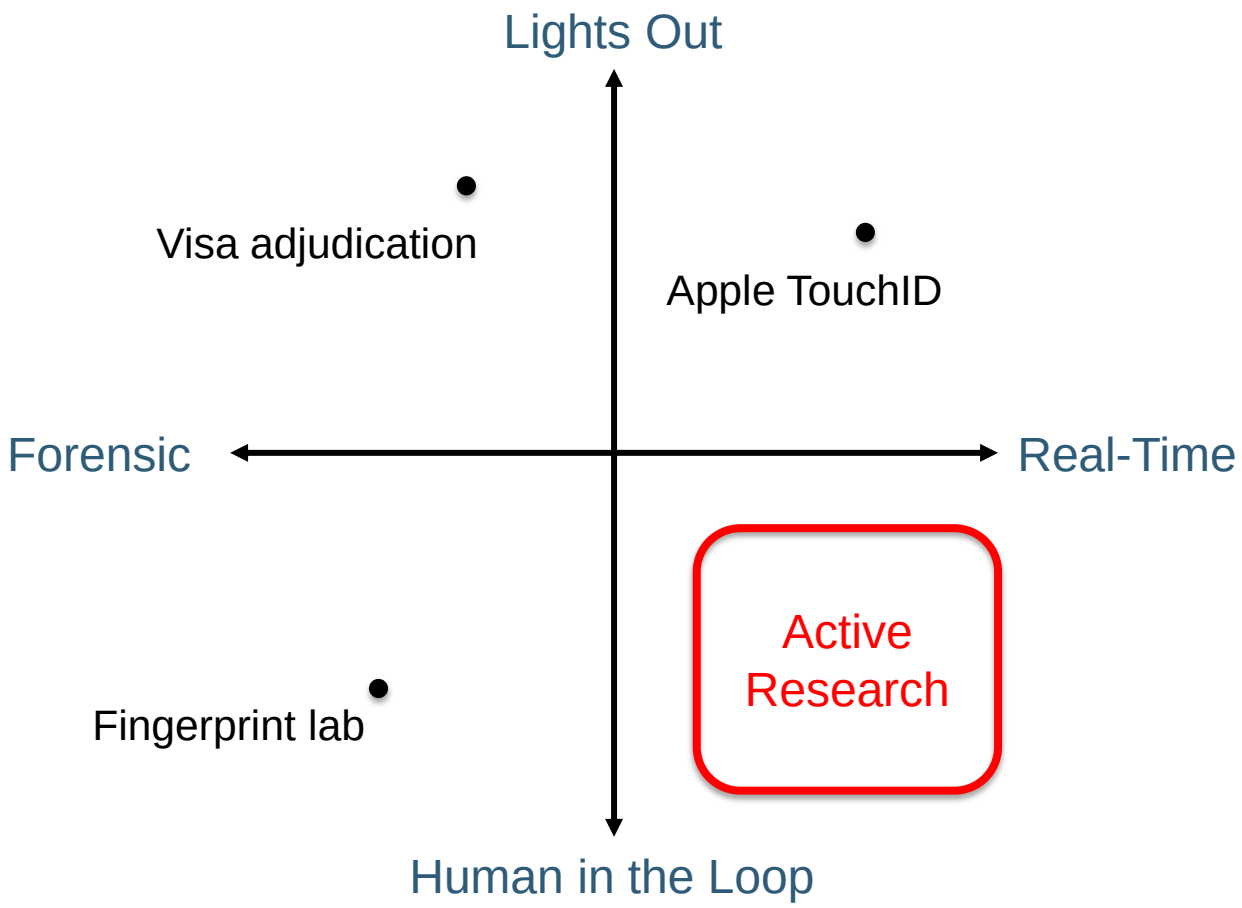




Passive

Cooperative

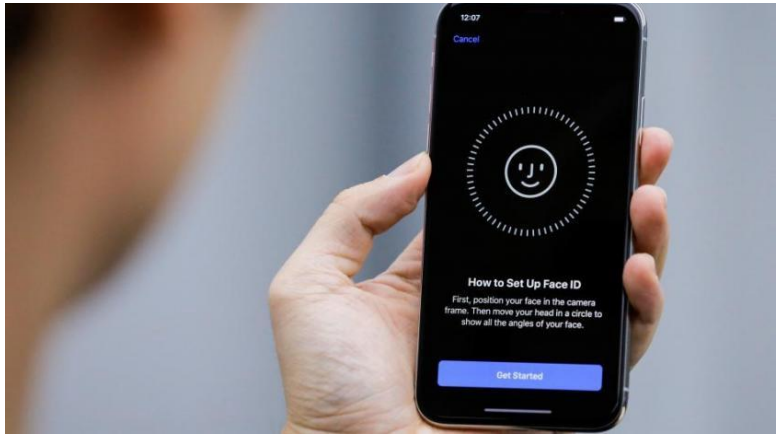
Biometric Scenarios



Social Considerations for Biometrics

- Biometrics can contain personal or health information that make people unwilling to share
  - Iris: Diabetes, hypertension
  - DNA: Contains almost everything
- Cooperative biometrics require willing participation
  - How will you scan children? The elderly? The disabled?
- Passive biometrics need a good capture opportunity
  - Face: Works best if the target looks at the camera

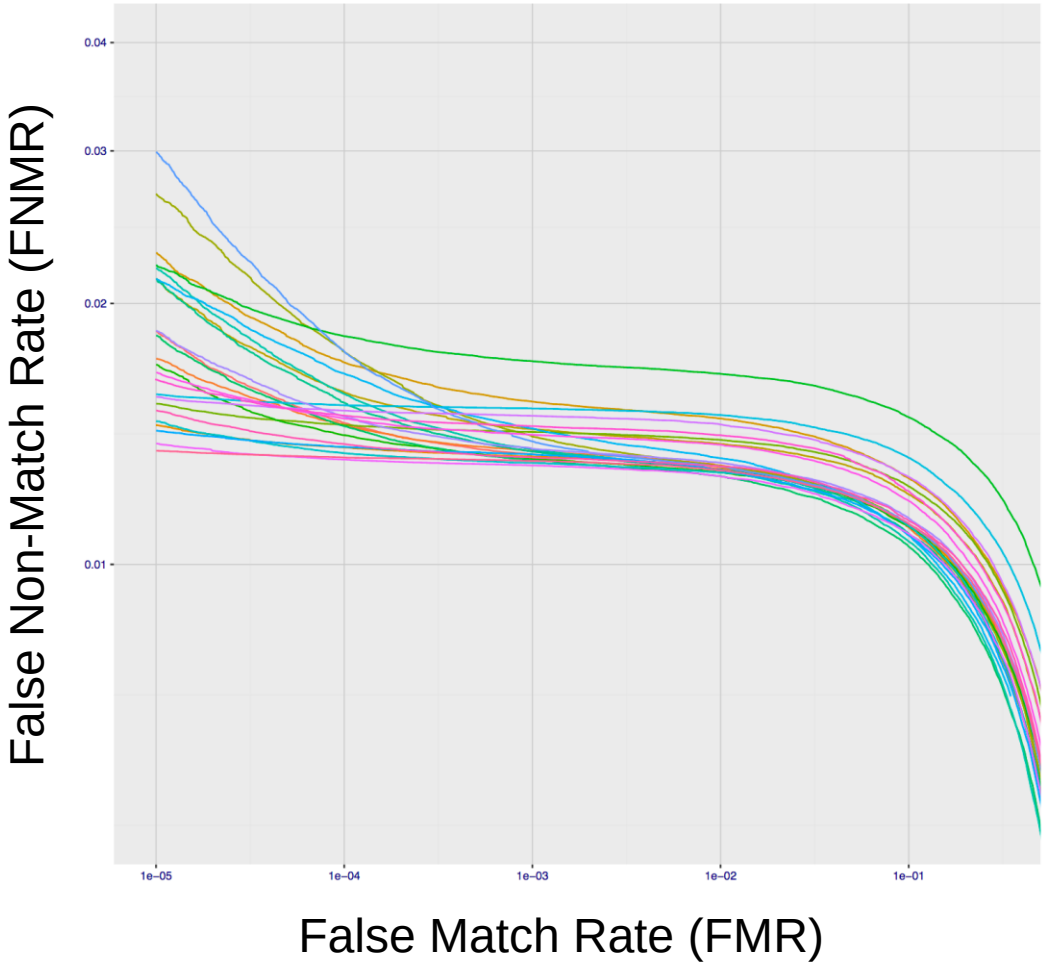
Iris Passport



noblis

State of the Art in Face Biometrics

- Face is universal, socially acceptable, difficult to circumvent and reasonably permanent (5-10 years for an adult)
  - Lots of companies are working to improve face biometrics
- NIST's Face Recognition Vendor Test[1] evaluates face recognition
  - 54 submissions from around the world
- 5/31/2017: FNMR: 0.05 @ FMR 0.001%
- 6/18/2018: FNMR: 0.01 @ FMR 0.001%
- 5X reduction in error rates in 1 year
- Improvements continue



1: https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

Conclusions

- Biometric performance is rapidly increasing thanks to machine learning
  - Face recognition error rates have dropped 5X since last year and continue to plummet
- TSA can actively trade FNMR and FMR to fit their requirements
- The public is becoming more accepting of biometric use in everyday life
- Policy questions remain about biometric signatures:
  - Capture (cooperative or non-cooperative)
  - Use(s)
  - Long-term storage
- Biometric identification is not perfect, but another layer in adaptable, risk-based security architectures

Backup

Questions

- What are the different modes (scenarios) that biometrics can be deployed?
- What are the metrics (P_D/P_{FA}) for detecting a known terrorist at the airport?
- How is passenger compliance with biometrics?
- How does biometrics apply to an adapting adversary?
- What limitations with the technology need to be improved?