Biometrics

Chapter 9

(Some images and slides are taken from Anil K. Jain)

Biometrics

- What is biometrics?
- Why Biometrics?
- Applications
- Traits
- Good Biometrics
  - Intra-class & Inter-class variability
- Challenges
- Conclusion

What is biometric?

- ★ Morris(1875): Derived from the Greek words **Bios**:life and **Metron**:a measure
- ★ Pollack(1981):“What makes each person unique?” Use of biometrics in the context of access control
- ★ Automated recognition of individuals based on their behavioral and biological characteristics [ISO/IECJTC12382-37:2012]

Taken from http://biometrics.cse.msu.edu/Presentations/AnilJain_Fed_Atlanta_2015.pdf

Identity Issues

- We rely our authentication systems on credentials (documents & secrets)

- Fake documents?
  - Fake id card (student card, national id card, driver license, etc)
- Identity Thefts

Fact

Back in 2006, a terrorist may has up to 10 (fake) passports

“An estimated 10,000 British passports were issued after fraudulent applications in the space of a year. Dhiren Barot, the most senior al-Qaida terrorist ever captured in Britain, had **7 passports in his true identity and 2 further passports in fraudulent identities**.”

290,000 passports issued by UK were lost/stolen in 2006

http://press.homeoffce.gov.uk/press-releases/passport-warning?version=1

Facts

Cards, Passwords, and PIN

The top 10 most common passwords were:

1. 123456
2. 123456789
3. qwerty
4. password
5. 111111
6. 12345678
7. abc123
8. 1234567
9. password1
10. 12345

https://edition.cnn.com/2019/04/22/uk/most-common-passwords-scli-gbr-intl/ind

Why biometrics?

- ★ Discourages fraud
- ★ Detects multiple enrollments
- ★ Cannot be transferred
- ★ Cannot be forgotten/lost
- ★ Eliminate **repudiation**
- ★ Convenience ?

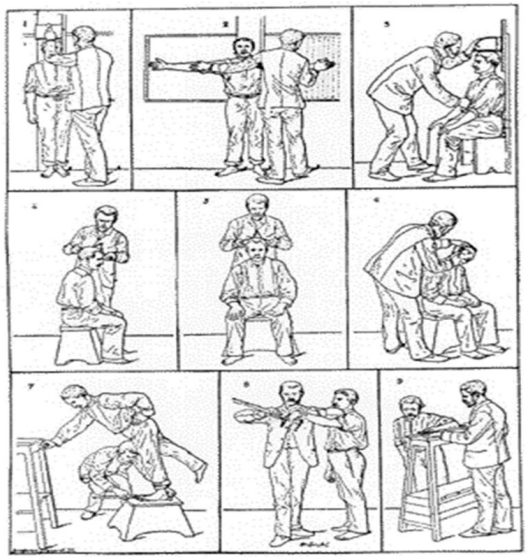
Applications

- ★ Forensics
- ★ Government
  - Fake Identity
  - Multiple enrollment
- ★ Commercial
  - Protect personal information
  - Eliminate Fraud

Biometrics in an early day

First Biometric System (1882)

Identify repeat offenders



H.T. F. Rhodes, Alphonse Bertillon: Father of Scientific Detection, Harrap, 1956

Taken from http://biometrics.cse.msu.edu/Presentations/AnilJain_Fed_Atlanta_2015.pdf

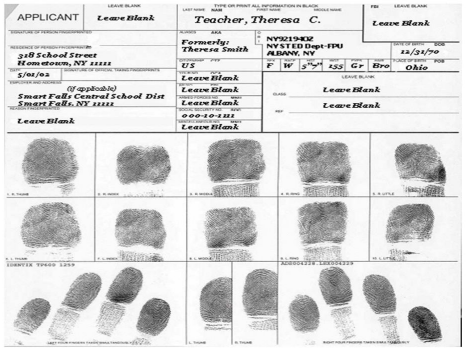
Biometrics in an early day

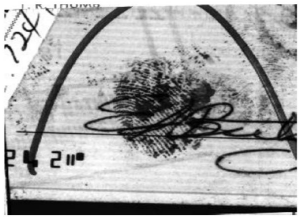
Friction Ridge Patterns

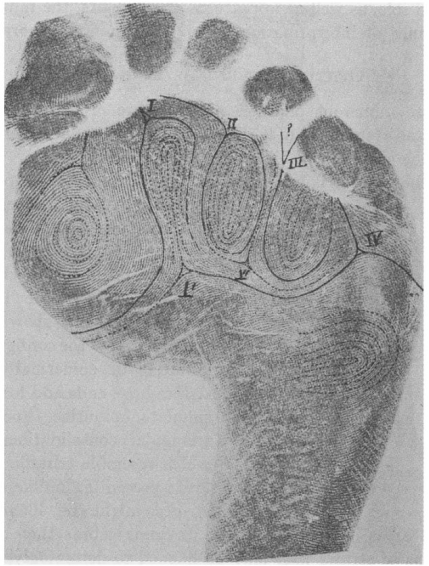
First Automatic Fingerprint identification system (AFIS): ~1980

Fingerprints in Law Enforcement

- Repeat Offenders: Compare rolled/slap tenprints
- Crime Scene evidence: Compare latents to tenprints



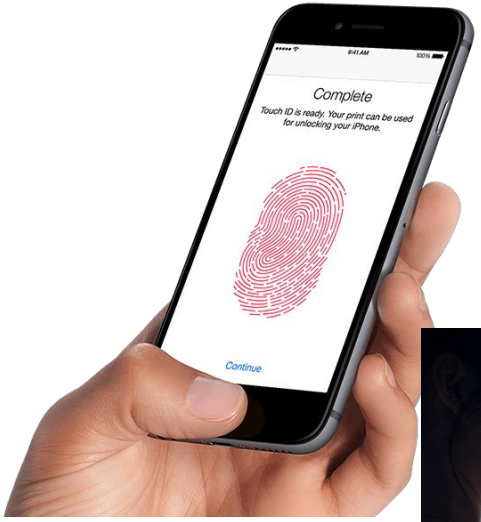


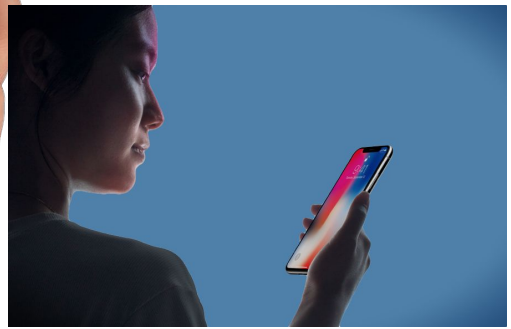


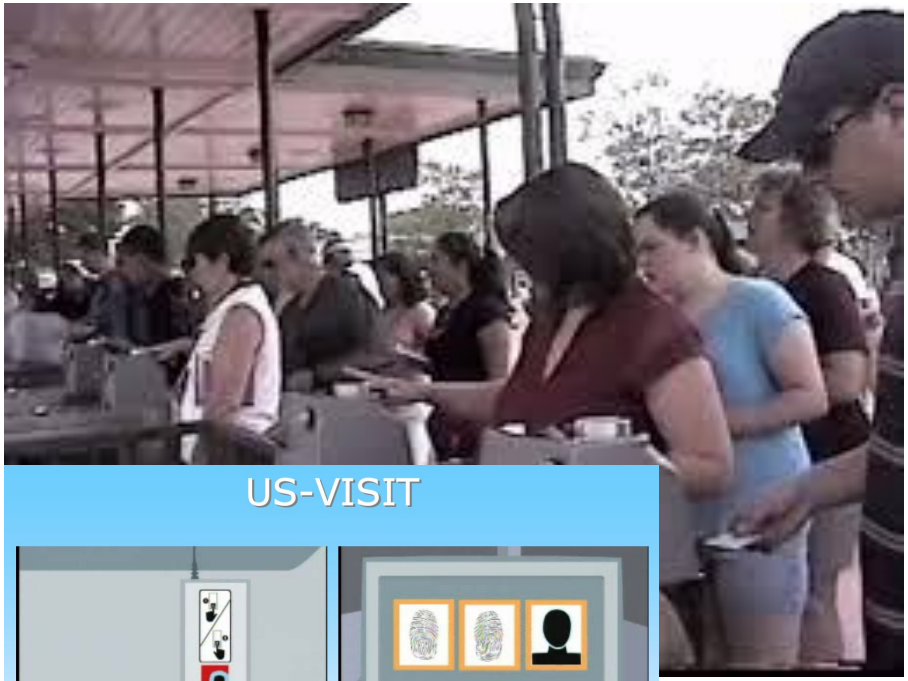
Cummins and Midlo, Finger Prints, Palms and Soles, Dover, 1961

Taken from http://biometrics.cse.msu.edu/Presentations/AnilJain_Fed_Atlanta_2015.pdf

Modern Day



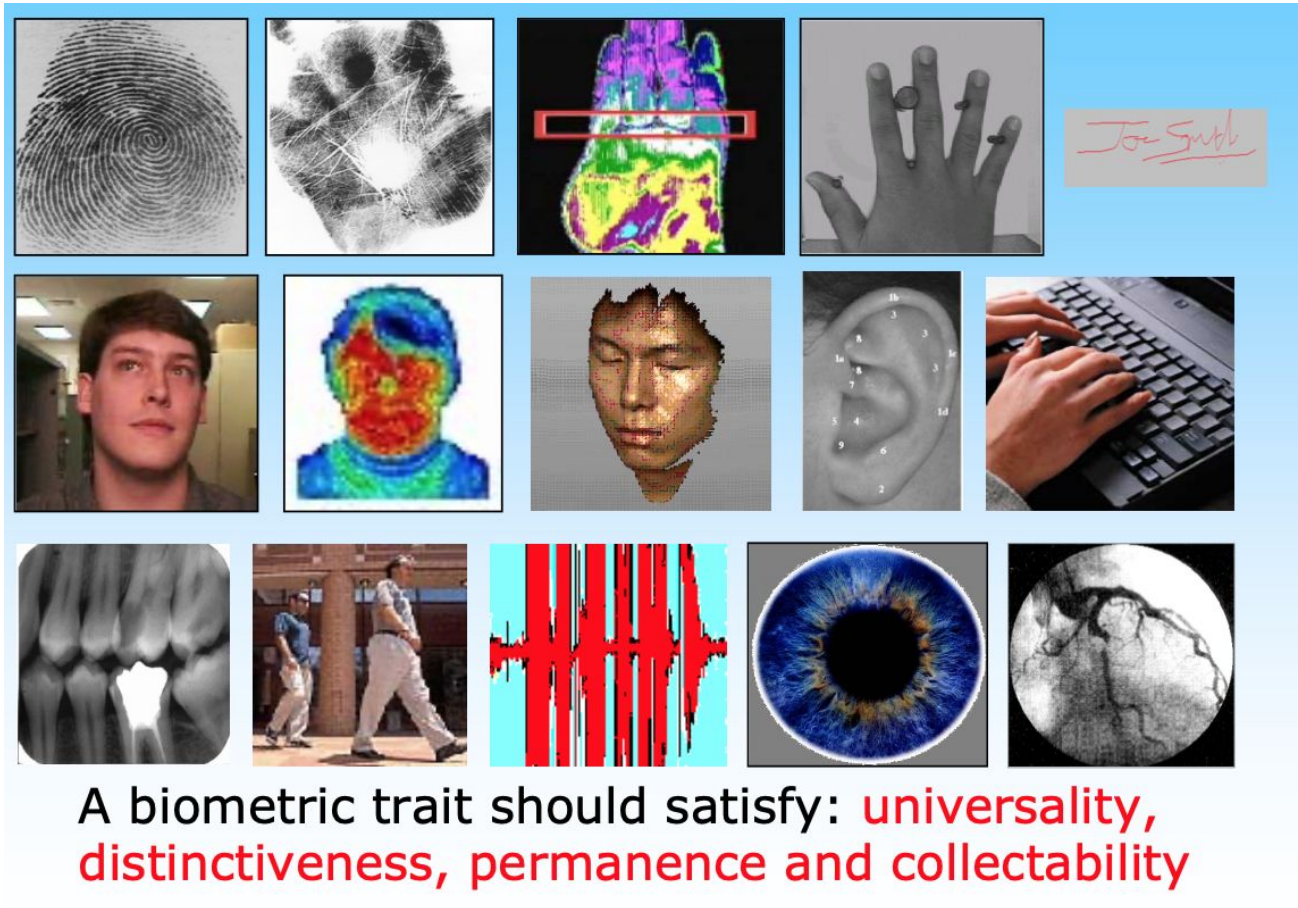




~ 70M visitors have been processed by US-VISIT; 1,100 criminals denied entry; watch list size ~4M

Traits

- ★ Should be:
- ★ unique
- ★ permanent



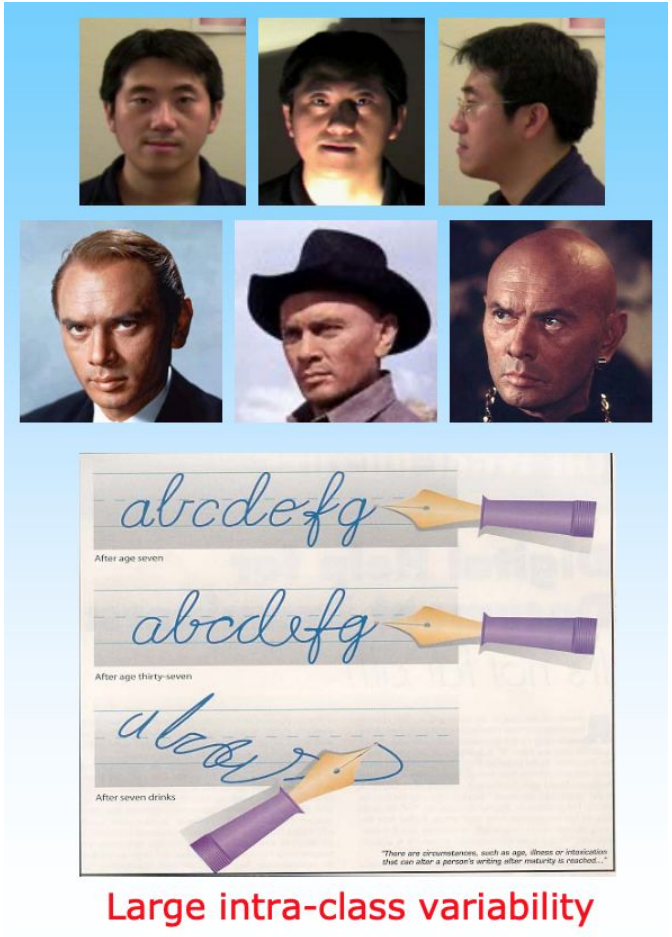
Good Biometrics

- ★ Large inter-class similarity
- ★ Twins have different fingerprints.

Large inter-class similarity

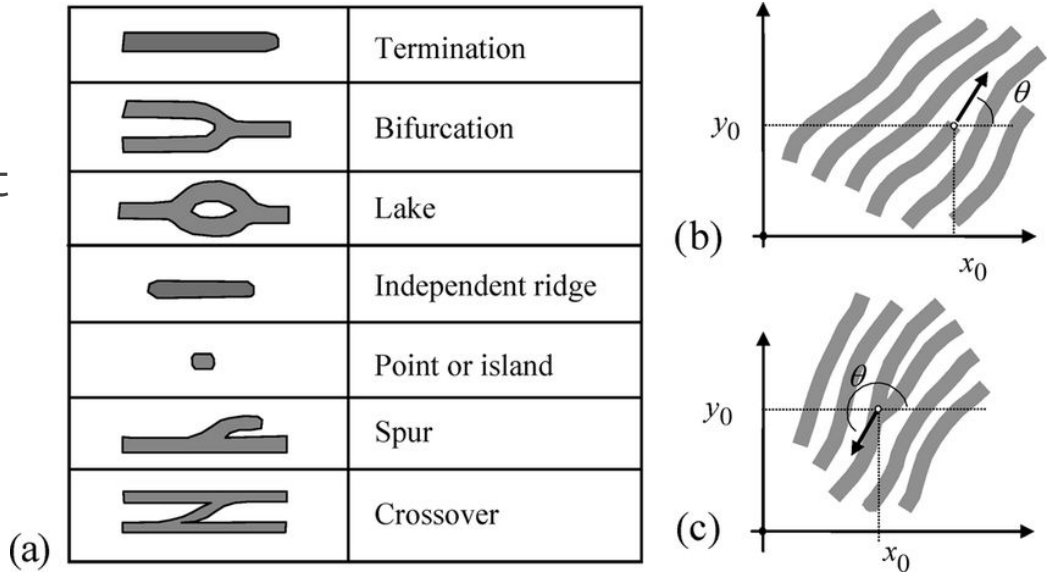
Good Biometrics (ctd.)

- ★ Small intra-class similarity



Quality of biometrics

- ★ Properties
  - Fingerprint minutiae
- ★ Image Quality/Alignment
- ★ Fake biometric



https://www.researchgate.net/profile/S_Pankanti/publication/3455239/figure/fig4/AS:669009137651715@1536515616365/Fingerprint-minutiae-a-The-common-fingerprint-minutiae-types-b-ridge-ending-x-y.ppm

Image Quality

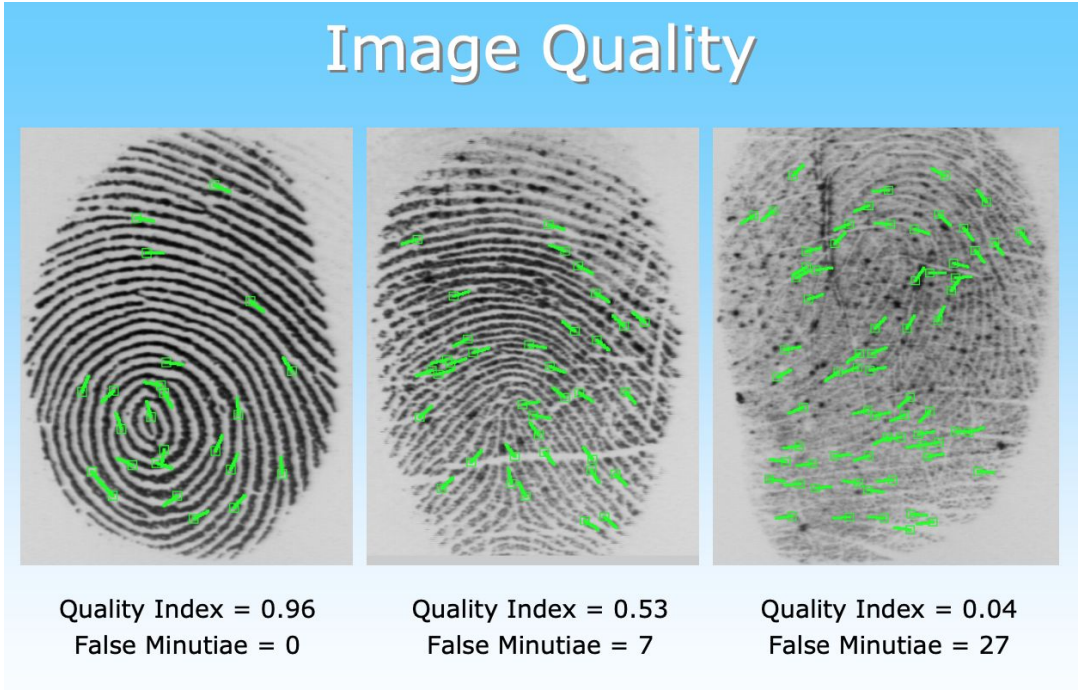
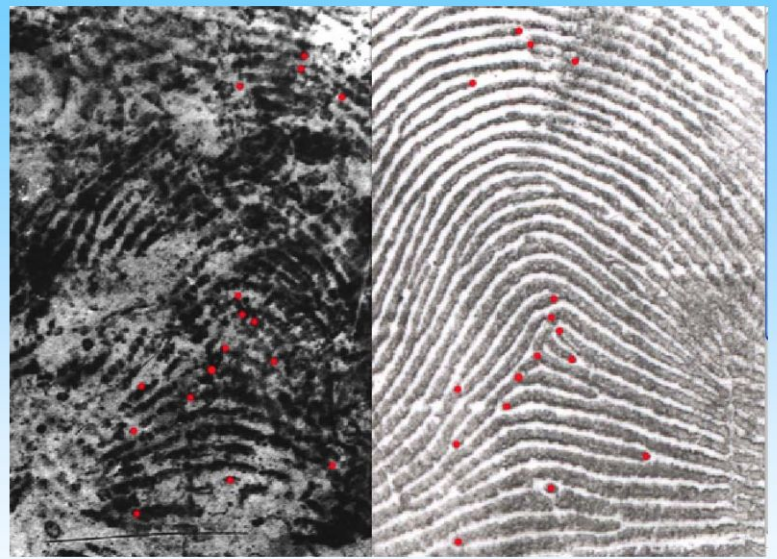


Image Quality

False Match

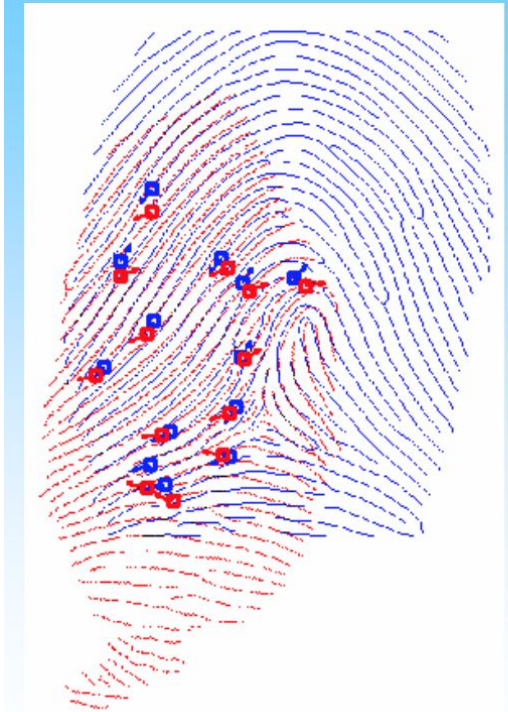


U.S. and Spanish authorities told reporters Mayfield's fingerprints matched those found on a bag discovered near the bombing site. Mayfield was later released after Spanish law enforcement officials said they matched fingerprints on the plastic bag to an Algerian man

Image Alignment

Human skin is an elastic surface.

Alignment

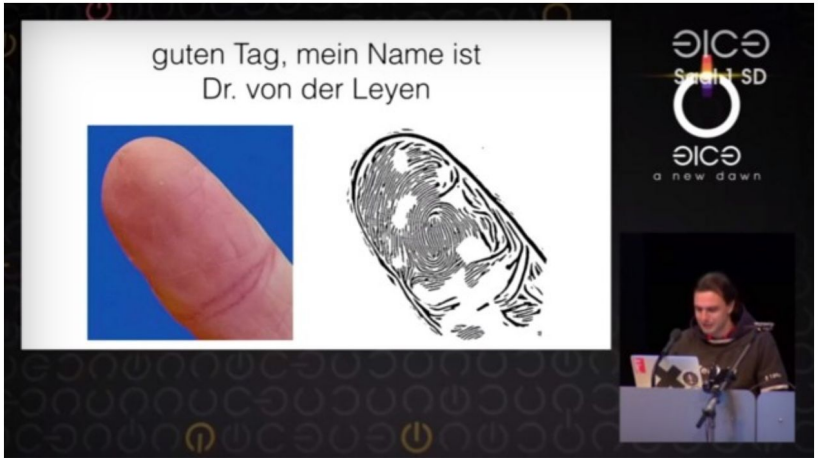


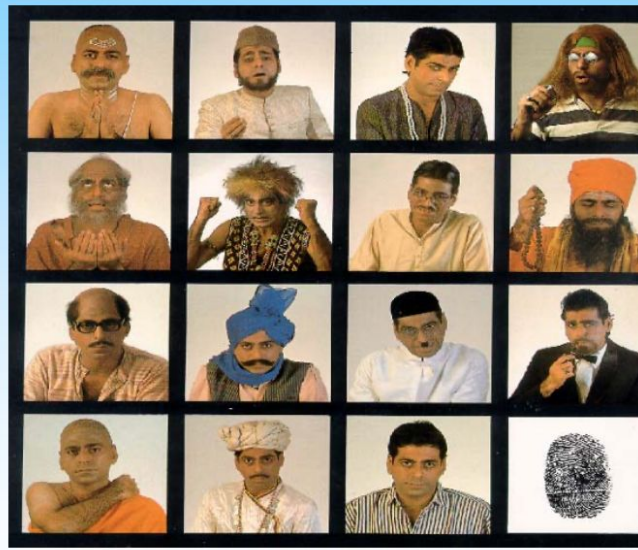
Non-linear surface distortion due to expression change

Fake biometrics

Hacker clones a politician's fingerprint using normal, long-distance public photos

By Sebastian Anthony on December 29, 2014 at 1:18 pm | 1 Comment





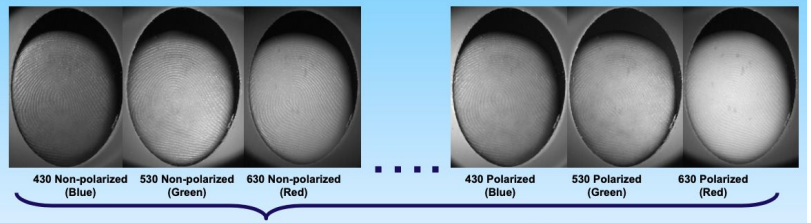
https://www.extremetech.com/extreme/196503-hacker-clones-a-politicians-fingerprint-using-normal-long-distance-public-photos

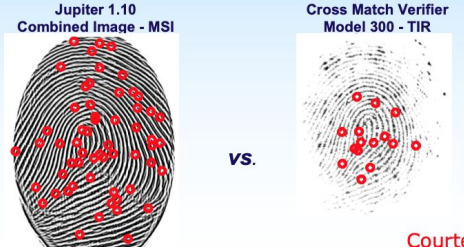
Against Fake biometrics

★ High Quality Sensor

Countering Spoof Attacks

Multiple wavelengths capture fingerprint features at different depths (surface and subsurface) of tissue

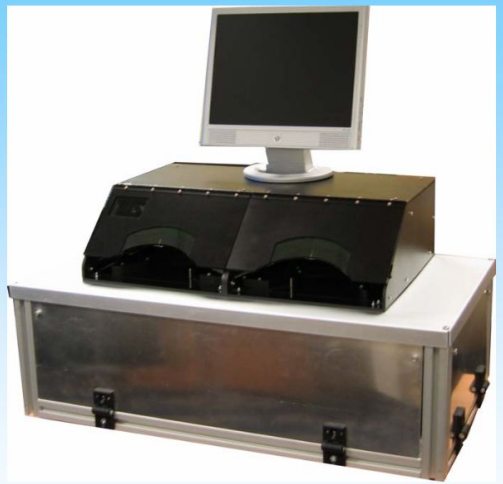




Courtesy, Lumidigm

Touchless Fingerprint Sensor

Surround Imager



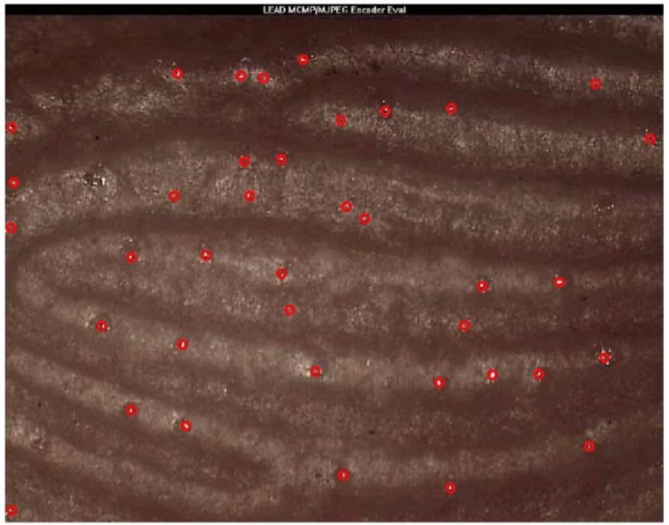
Ten print capture device

NIJ fast fingerprint capture technology initiative; US-VISIT will start capturing 10 fingers as opposed to current 2 fingers (Courtesy TBS, NA)

Against Fake biometrics

★ High resolution sensors can detect pores, dots.

High Resolution Sensors



Provide Level 3 features (pores, dots,..) in addition to commonly used minutiae

Template?

- ★ Template should be stored as minutiaes.
- ★ An image can be used to construct Fake biometrics.

Template Protection

Myth: "A true biometric image cannot be created from master template.."

Template security is critical because it is not easy to revoke templates like passwords

A. Ross, J. Shah and A. K. Jain, "From Templates to Images: Reconstructing Fingerprints from Minutiae Points", *IEEE Trans. on PAMI*, Vol. 29, No. 4, pp. 544-560, April 2007

Facts

Fingerprint template in national database (of Thailand?).

★ Can you construct a fake biometric from these images?

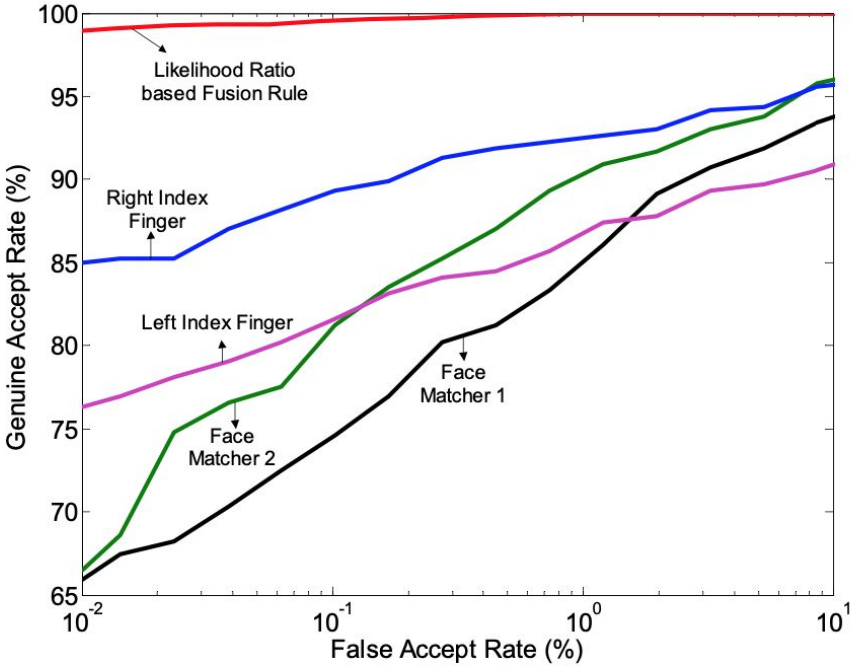
If an image of your fingerprint is stolen, what should you do?

Error Rates

	Test	Test Parameter	False Reject Rate	False Accept Rate
Fingerprint	FVC [2006]	Heterogeneous population incl. manual workers and elderly people	2.2%	2.2%
	FpVTE [2003]	US govt. operational data	0.1%	1%
Face	FRVT [2006]	Controlled illumination, high resolution	0.8%-1.6%	0.1%
Iris	ICE [2006]	Controlled illumination, broad quality range	1.1%-1.4%	0.1%
Voice	NIST [2004]	Text independent, multi-lingual	5-10%	2-5%

85M passengers at Atlanta airport in 2006; what is the acceptable error?

Fusing Face and Fingerprints



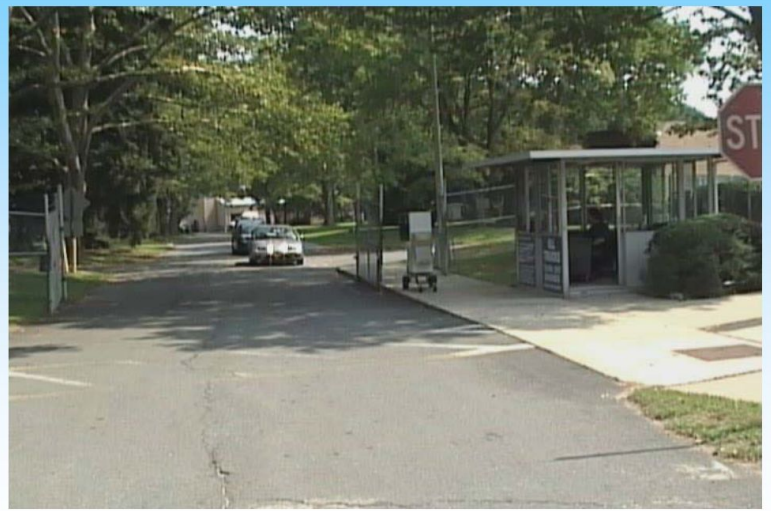
K. Nandakumar, Y. Chen, S. Dass, A.K. Jain, IEEE Trans. PAMI, 2007 (to appear)

Challenges

- ★ New Traits
- ★ Sensors
- ★ Algorithms/Accuracy
- ★ Multibiometrics (fusion)?
- ★ Biometrics from distance (from space?)
- ★ System Security

Iris at a Distance

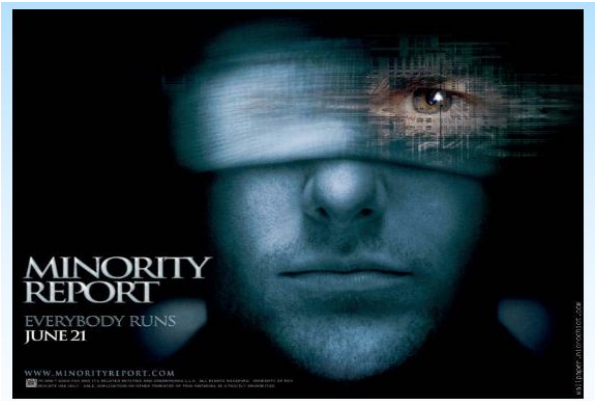
- Current systems require proximity to sensor

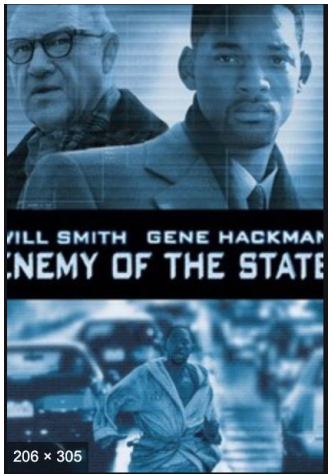


Courtesy: Jim Matey, Sarnoff

Privacy

- ★ Will biometric be used to track people?
- ★ Will biometric be used only for the intended purpose?
- ★ Will the databases be “linked”? (Function creep)





Conclusion

- ★ Reliable recognition is critical to several applications
- ★ No single biometric system is perfect
- ★ Trade off/Cost-benefit analysis
- ★ Will you use it for you system?

References

★ Public presentations on biometrics by Anil K. Jain, Biometrics research group, Michigan State University (http://biometrics.cse.msu.edu/index.html)

End of Chapter 9