Biometric Recognition: A New Paradigm for Security

Anil K. Jain

Dept. of Computer Science and Engineering

Michigan State University

http://biometrics.cse.msu.edu

Identity Questions

- Should John be granted a visa?
- Does Alice already have a driver license?
- Is Cathy authorized to enter the facility?
- Can Steve access the website?
- Is Mary the owner of the bank account?
- Does Charlie have a criminal record?

We rely on credentials: documents & secrets

Al-Qaida Gets Fake Papers

James Sturcke & Agencies
Tuesday March 20, 2007
Guardian Unlimited

"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

Cards, Passwords and PIN

- Ten most common passwords: password, 123456, Qwerty, abc123, letmein, monkey, myspace1, password1, link182, (your first name)
  http://www.pcmag.com/article2/0,1895,2113976,00.asp
- ~40% of user-chosen passwords are readily guessable by programs
  http://portal.acm.org/citation.cfm?id=359168.359172
- Personal data is routinely lost & stolen
  http://www.privacyrights.org/ar/ChronDataBreaches.htm
- A complete identity (govt. issued ID, US bank account and new DOB) can be bought for $14 *The Straits Times, Singapore, March 20, 2007*

Phishing

Credit card fraud amounted to ~$56B in losses in 2005 for millions of customers

Challenge

We now live in a global society of increasingly desperate and dangerous people who can not be trusted based on identification documents

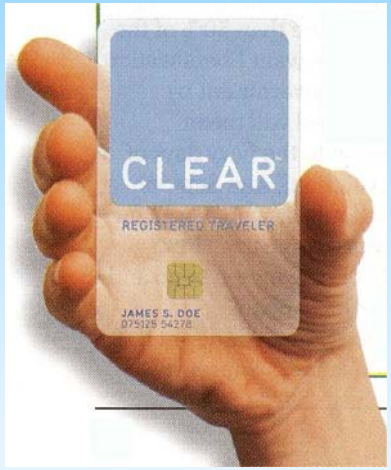
- Are the credentials genuine?
- Are they in the possession of the authorized person?

Homeland/Enterprise/Personal security

Biometric Recognition

Automatic recognition based on "who you are" as opposed to "what you know" (PIN) or "what you have" (ID card)


Stephen J. Boitano, AP



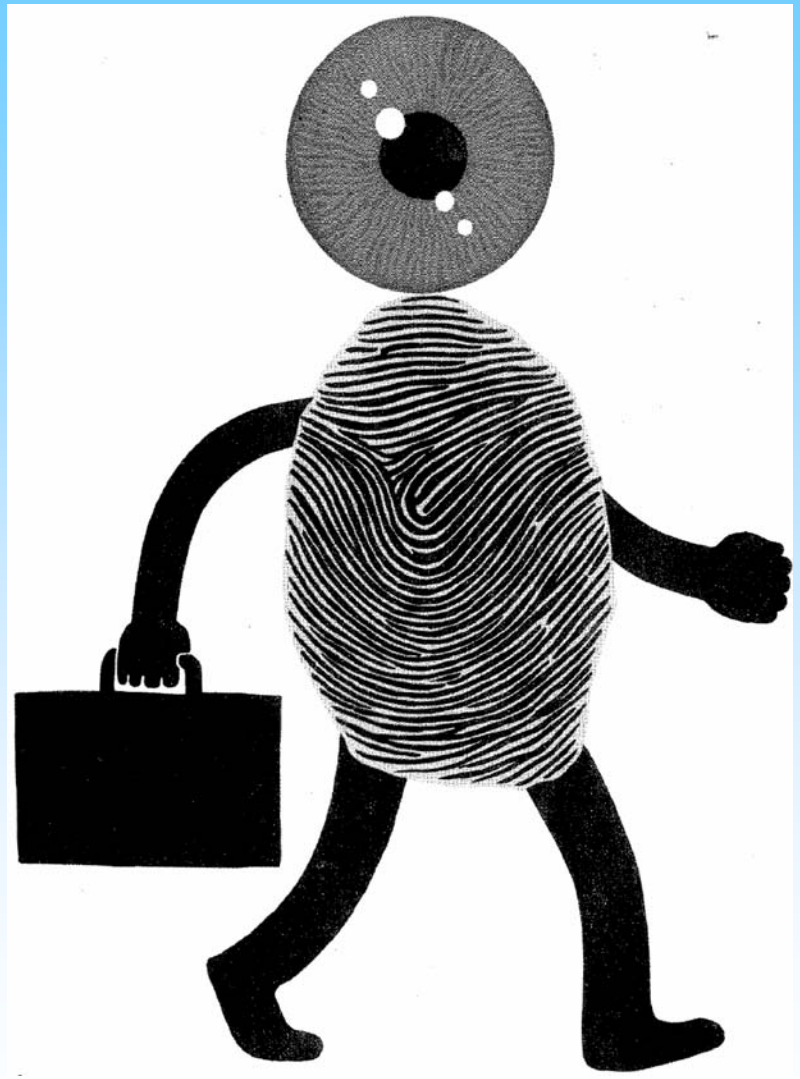
Recognition of a person by his body & then linking that body to an externally established identity, forms a very powerful tool for identity management

Why Biometric Recognition?

- Discourages fraud & enhances security
- Detects multiple enrollments
- Cannot be transferred/forgotten/lost/copied
- Eliminates repudiation claims
- User convenience

Multifactor authentication (card, PIN and biometric): PIV card, Trusted traveler

The Winning Card



"Basic Pilot Program (DHS) should include tamperproof ID for job-seekers, incorporating biometrics. Only then would it be possible to establish not only that job applicants are authorized to work but also that they are who they say they are"

Doris Meissner and James Ziglar, New York Times OP-ED, April 16, 2007

Fundamental Premise

Biometric traits are unique & permanent

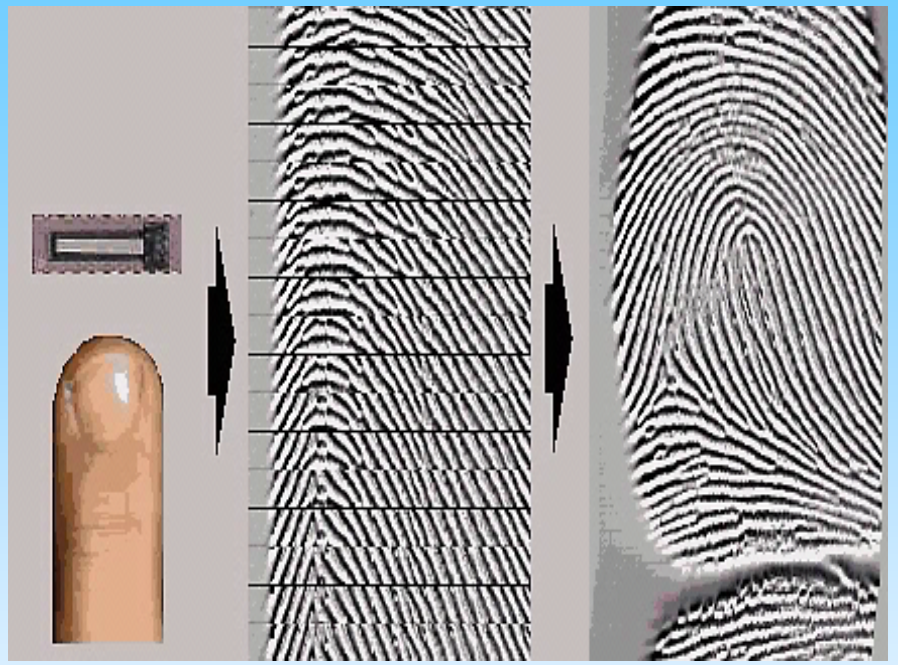
- Very small intra-class variability
- Very large inter-class variability

Biometrics is Not New!

- Habitual Criminal Act, U.K. (1858)
- Bertillon system (1882) took a subject's photograph, and recorded height, length of foot, arm and index finger
- Galton/Henry system of fingerprint matching adopted by Scotland Yard in 1900
- FBI set up a fingerprint identification division in 1924
- AFIS installed in 1965 with a database of 800K fingerprints
- Goldstein (1971) published first face recognition paper
- Daugman (~1990) developed iris recognition technology
- FBI installed IAFIS in 2000 with a database of 80 million 10 prints; ~80,000 searches per day; ~20% of searches are in lights out mode; ~2 hour response time

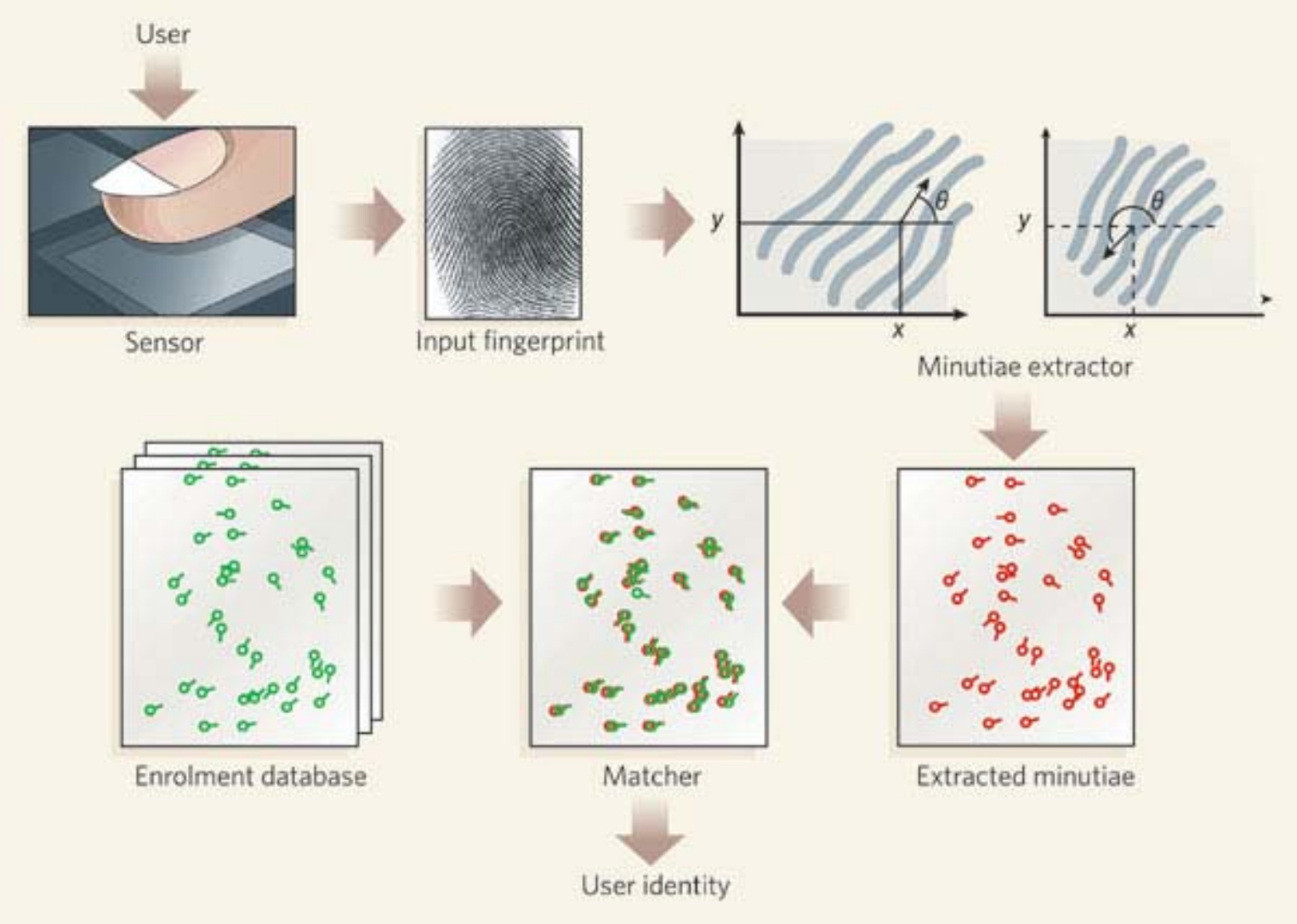
Biometrics: New Era

- Border security
- Multiple enrollments
- Financial fraud
- User convenience



- Cheap & compact sensors
- A practical system must meet speed, accuracy and resource requirements

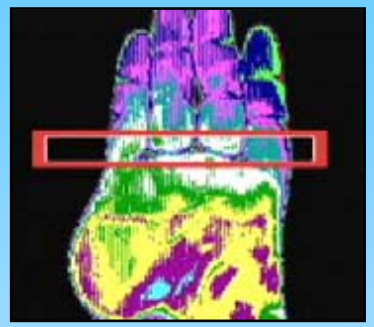
Automatic Biometric Recognition

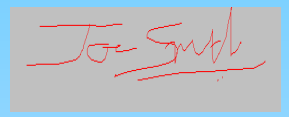
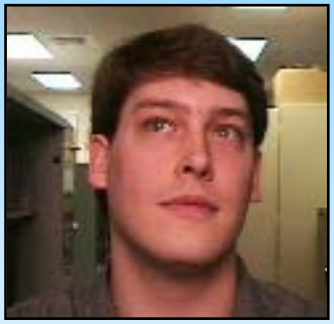
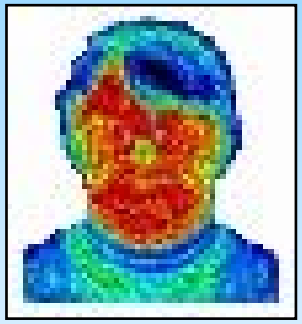
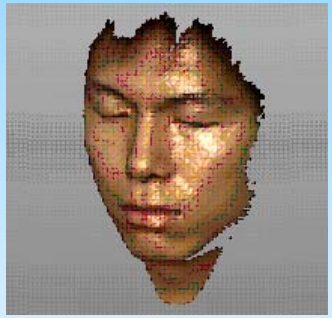
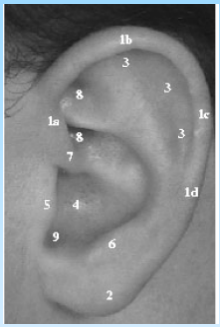


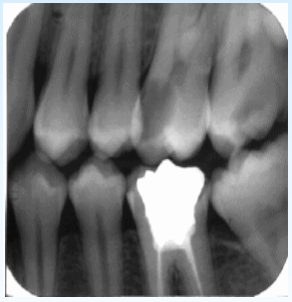
Threshold on the match score determines tradeoff between Far and FRR

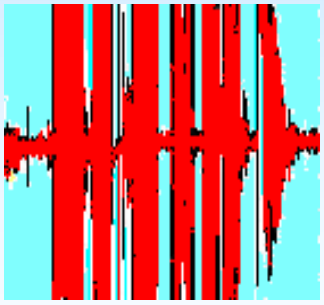
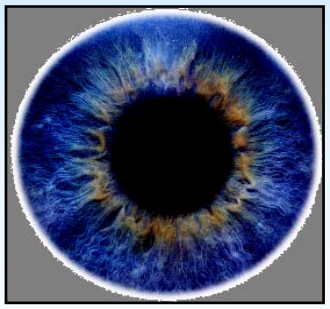
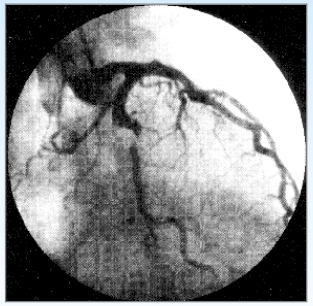
Biometric Traits





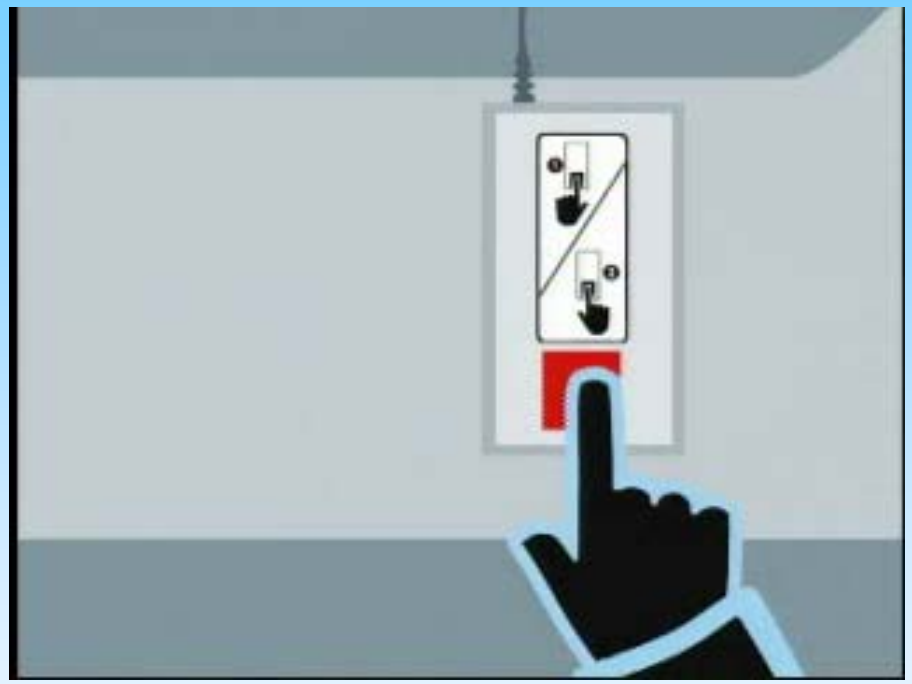






A biometric trait should satisfy: universality, distinctiveness, permanence and collectability

US-VISIT



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

Border Crossing System in UAE

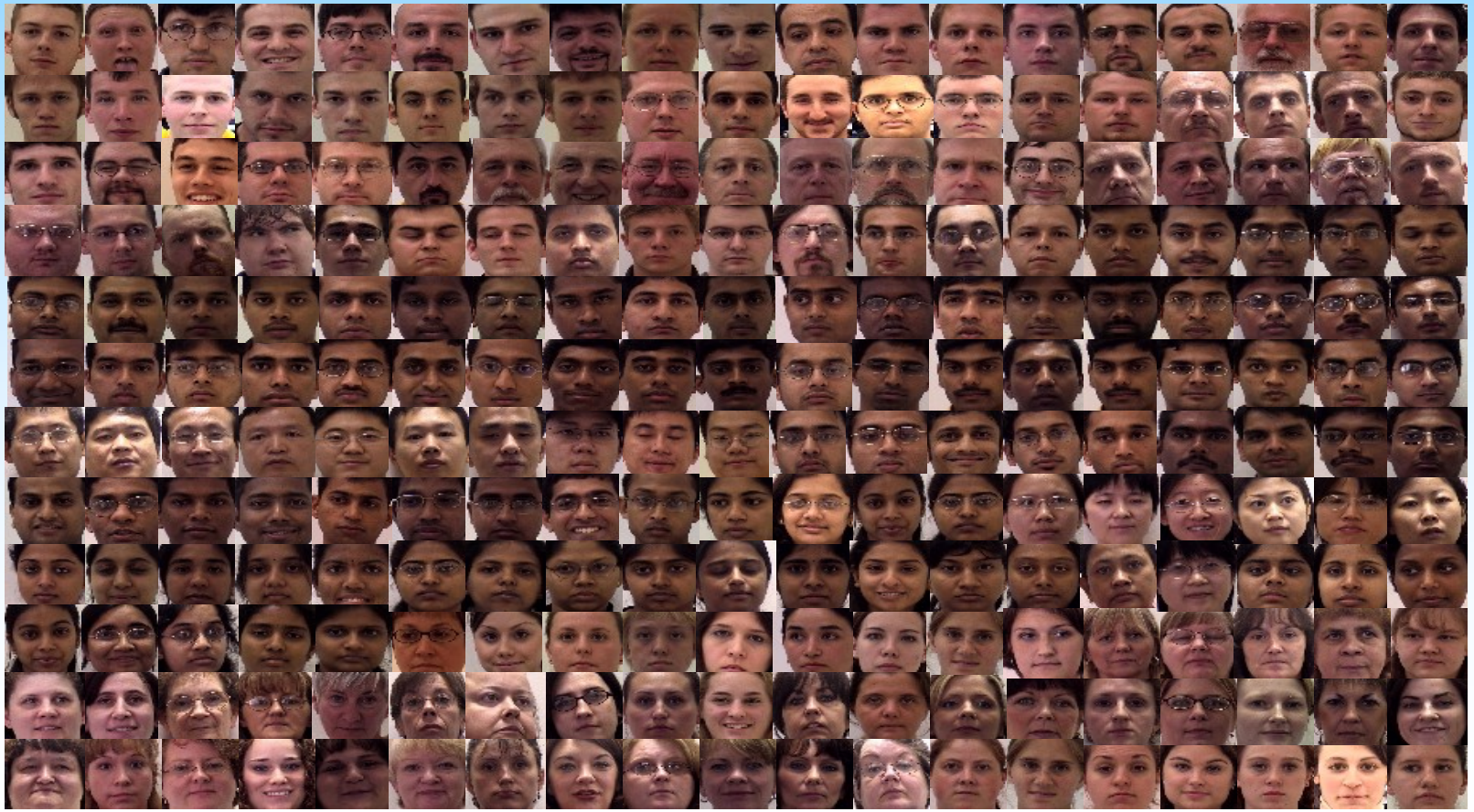
Many people expelled from the UAE make repeated efforts to re-enter with new identities using forged travel documents

Hong Kong Smart ID Card

- Security: Prevent misuse of stolen cards
- Convenience: e-Certificate
- Service: electronic government services
- Travel: Passenger Clearance System

Multiple Enrollments

- Large legacy databases (passports, driver licenses)
- Florida DMV “scrubbed” its database and found ~5,000 duplicates by matching 700K face images against a database of 51M faces (Courtesy, Merkatum)



Disney World, Orlando

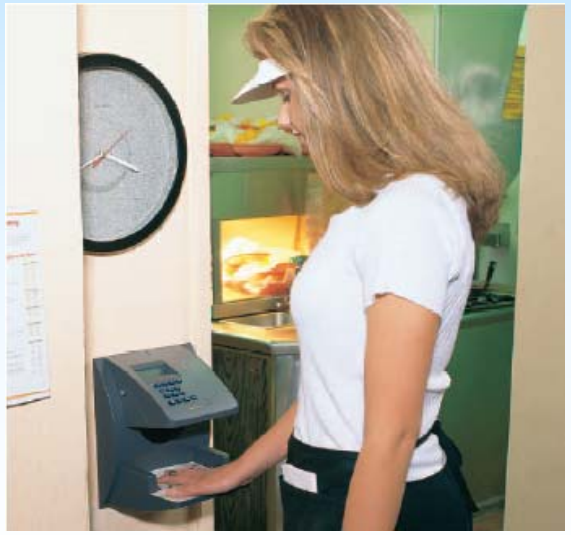
Throughput: 100K/day, 365 days/ year; provides access to paying customers & denies access to non-paying customers

Commercial Applications

Meijer supermarket, Okemos

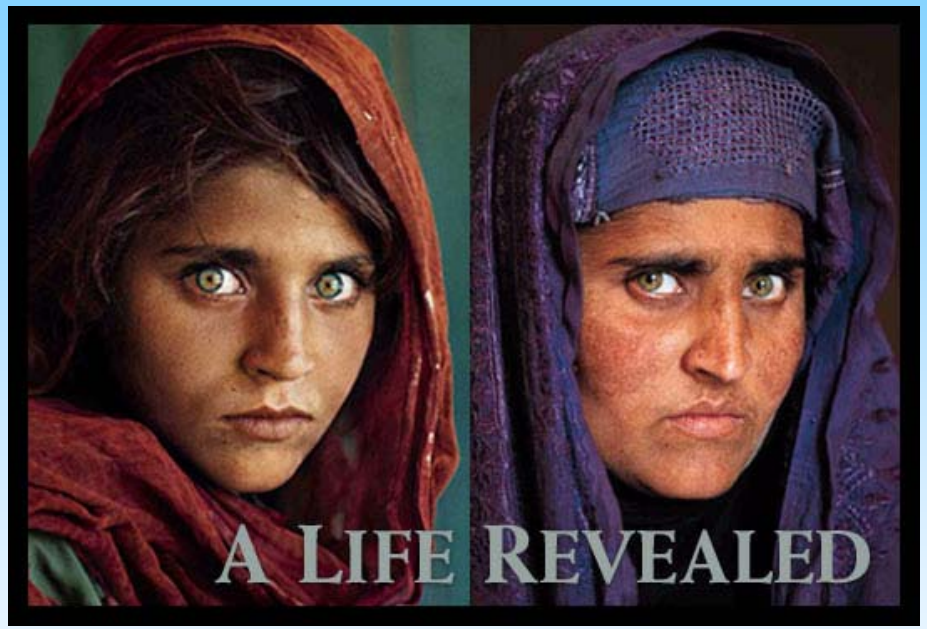
MSU Federal Credit Union, East Lansing

Citibank, Singapore: pay by fingerprints

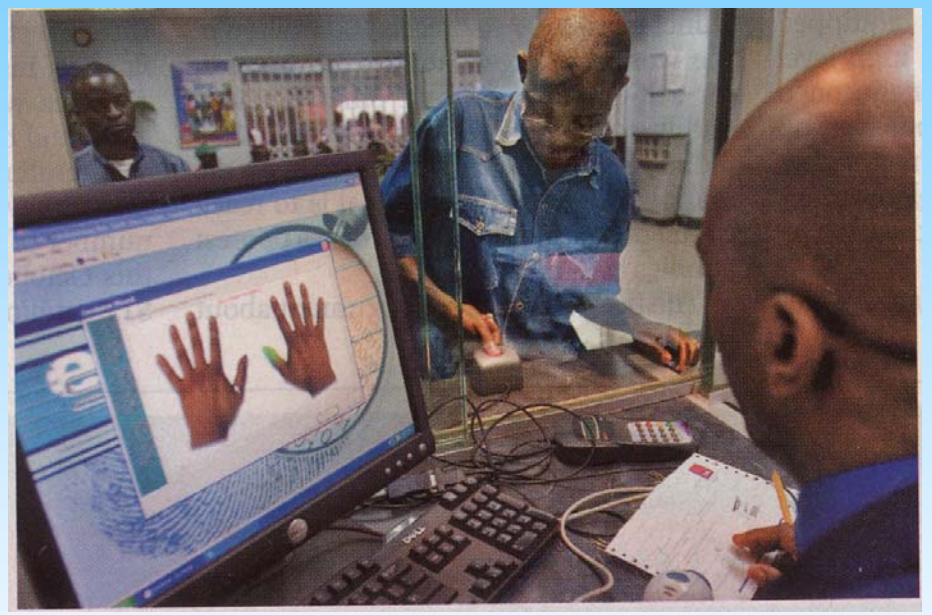


Time & Attendance; Hilton Waterfront Beach Resort

Societal Benefits



Sharbat Gula in 1985, 2002 (Steve McCurry, National Geographic)



Bank in Malawi uses fingerprint smart cards for micro-loans

Biometric Systems: Limitations

- Intrinsic failure
  - Lack of uniqueness in biometric trait (large intra-class variability, large inter-user similarity)
  - Recognition error (False accept, false reject, failure to enroll)
- Adversary attack
  - Administrative/insider attack (integrity of enrollment, collusion, coercion)
  - Non-secure infrastructure (template security, channel security, software integrity)
  - Biometric overtness (spoof attack)

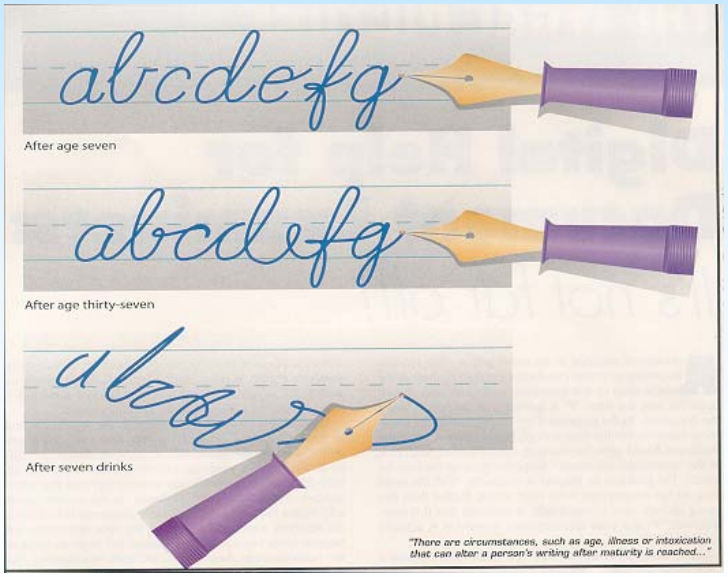
Most fake bombs missed by screeners: 75% not detected at LAX; 60% at O'Hare (USA Today, Oct 18, 2007)

"State-of-the-art" Error Rates

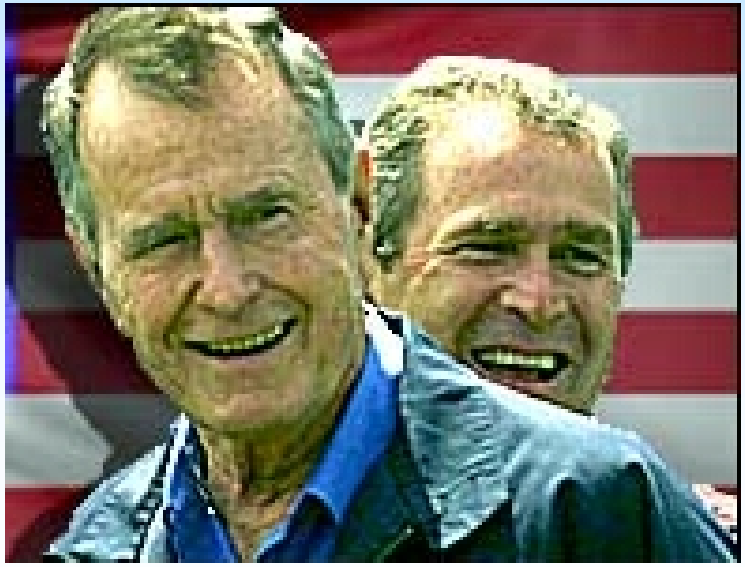
	Test	Test Parameter	False Reject Rate	False Accept Rate
Fingerprint	FVC [2006]	Heterogeneous population incl. manual workers and elderly people	2.2%	2.2%
	FpVTE [2003]	US govt. operational data	0.1%	1%
Face	FRVT [2006]	Controlled illumination, high resolution	0.8%-1.6%	0.1%
Iris	ICE [2006]	Controlled 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?

Intra-Class & Inter-Class Variations



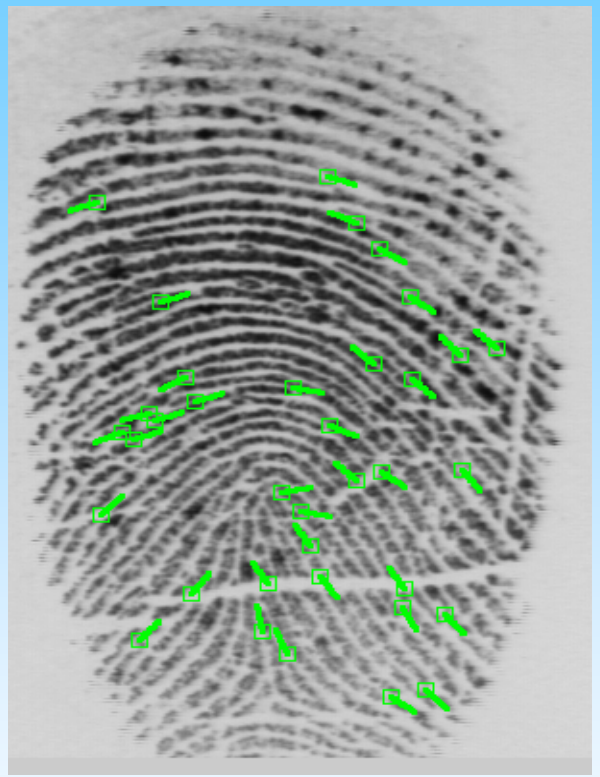
Large intra-class variability



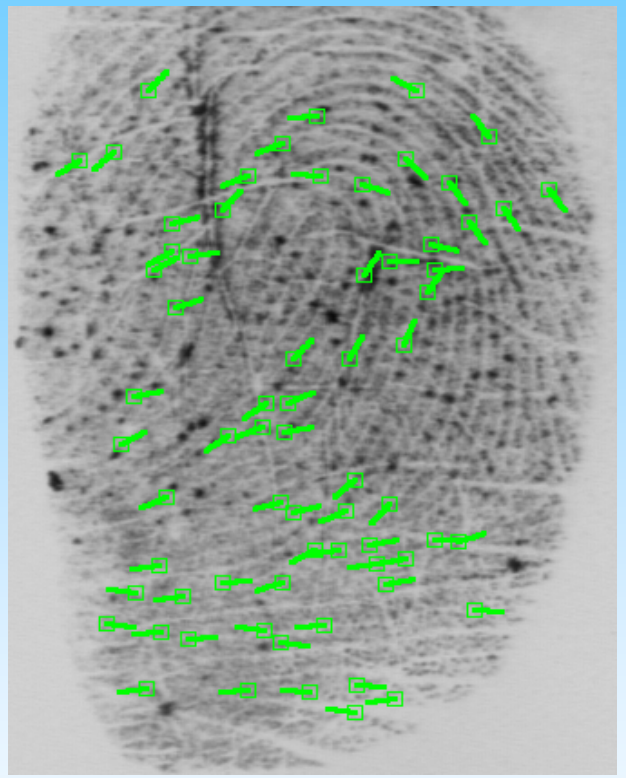
Large inter-class similarity

Image Quality

Quality Index = 0.96
False Minutiae = 0

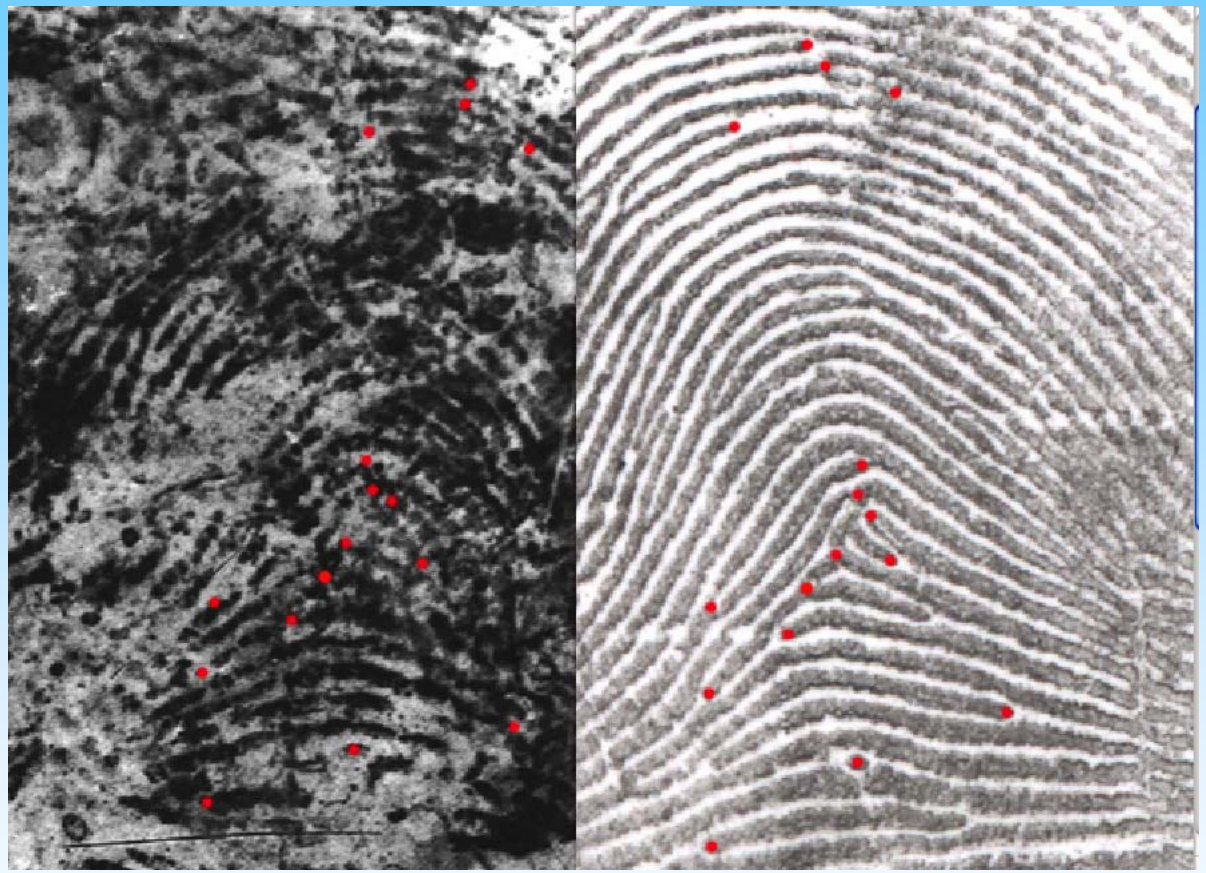


Quality Index = 0.53
False Minutiae = 7



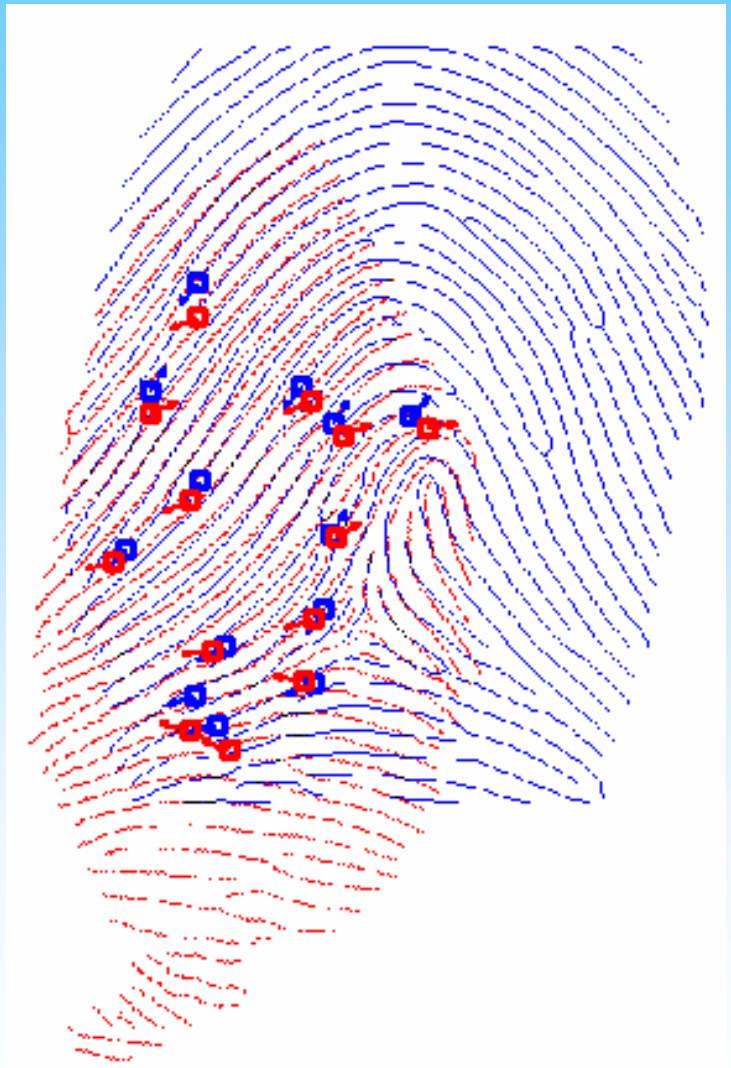
Quality Index = 0.04
False Minutiae = 27

False Match



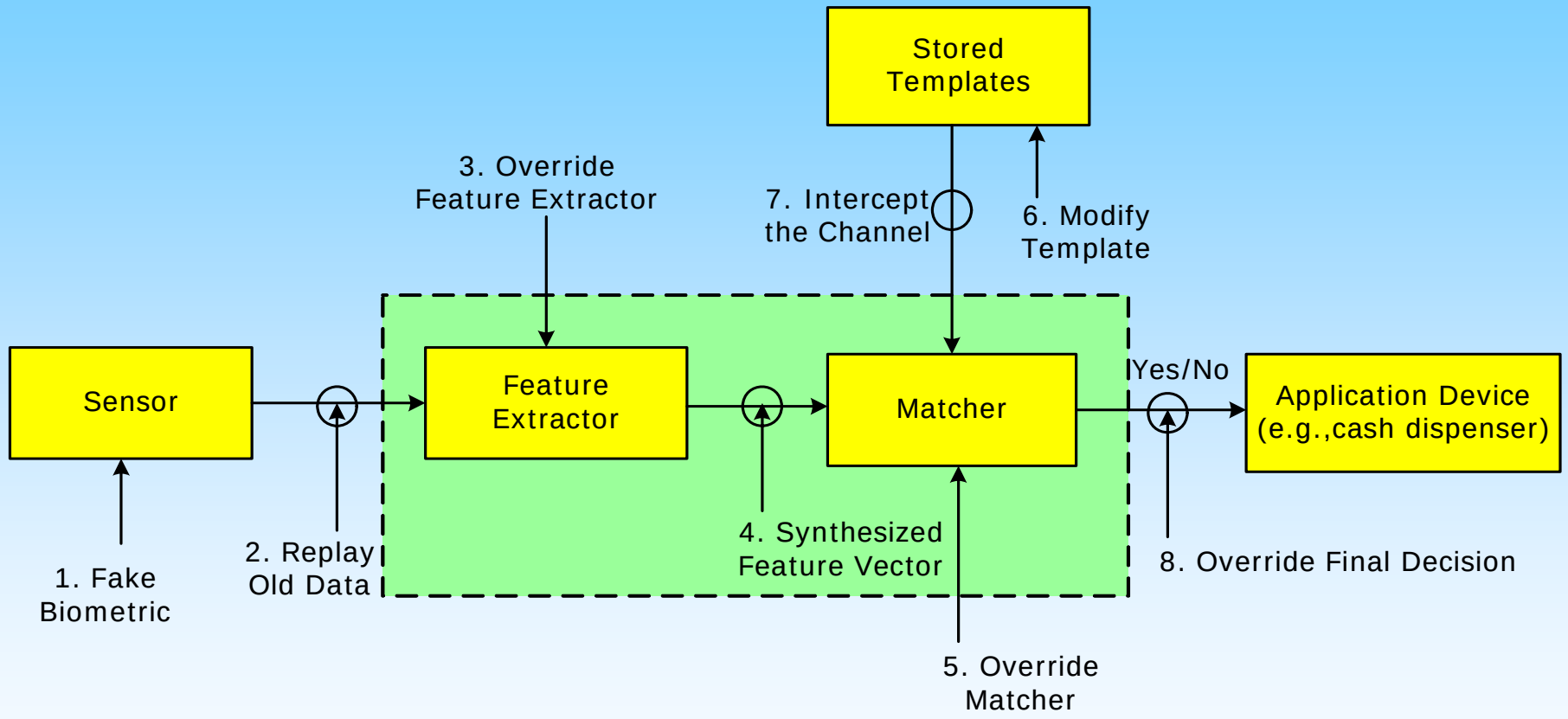
U.S. and Spanish authorities told reporters Mayfield's fingerprints matched those found on a bag discovered near the bombing site. Mayfield was later released after Spanish law enforcement officials said they matched fingerprints on the plastic bag to an Algerian man

Alignment

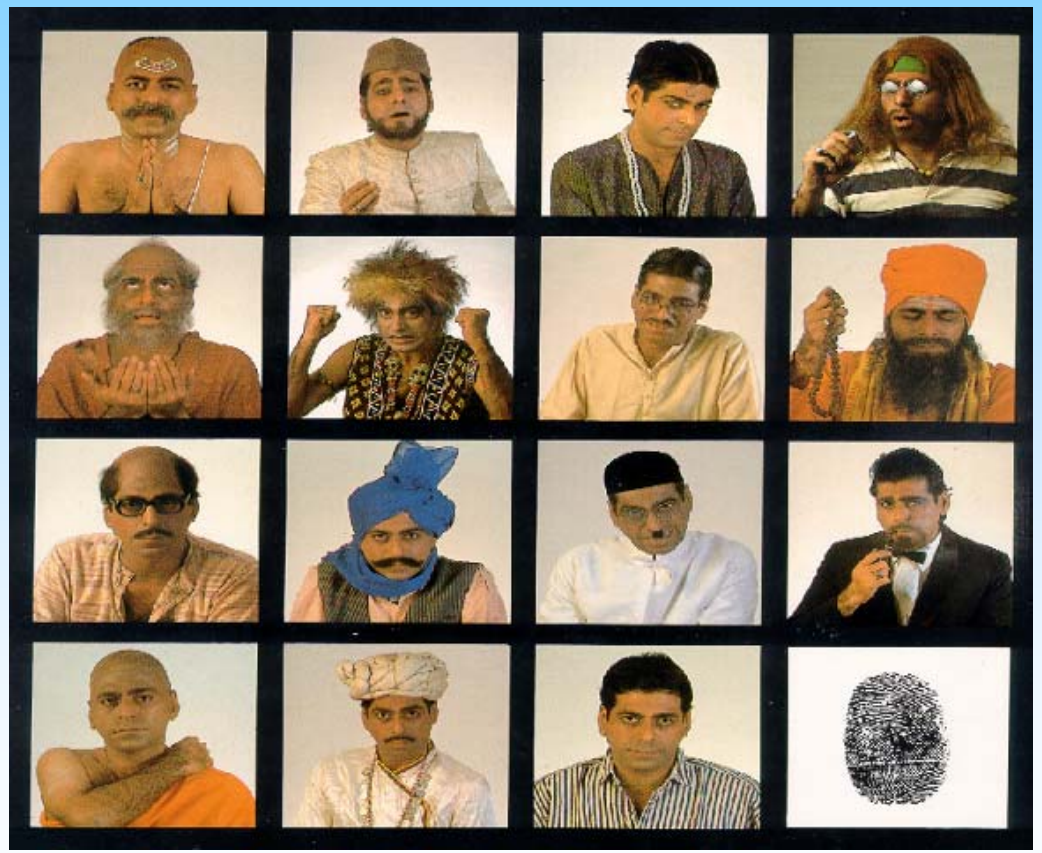


Non-linear surface distortion due to expression change

Adversary Attacks



Fake Biometrics



No Fault of Biometric Technology!

- "Many well-meaning students, teachers, and parents—once their irises had been scanned and the computer had unlocked the door for them—held the door open for another person entering the building behind them (Tail gaiting)"

- "Teachers, staff members, and others who went outside the school on their lunch break or between classes to eat, smoke, or talk to their colleagues often propped open a door behind them.... School officials even found a brick placed by one door, used to prop it open"

"Keeping an Eye on School Security: The Iris Recognition Project in New Jersey Schools", NIJ Journal, No. 254, July 2006

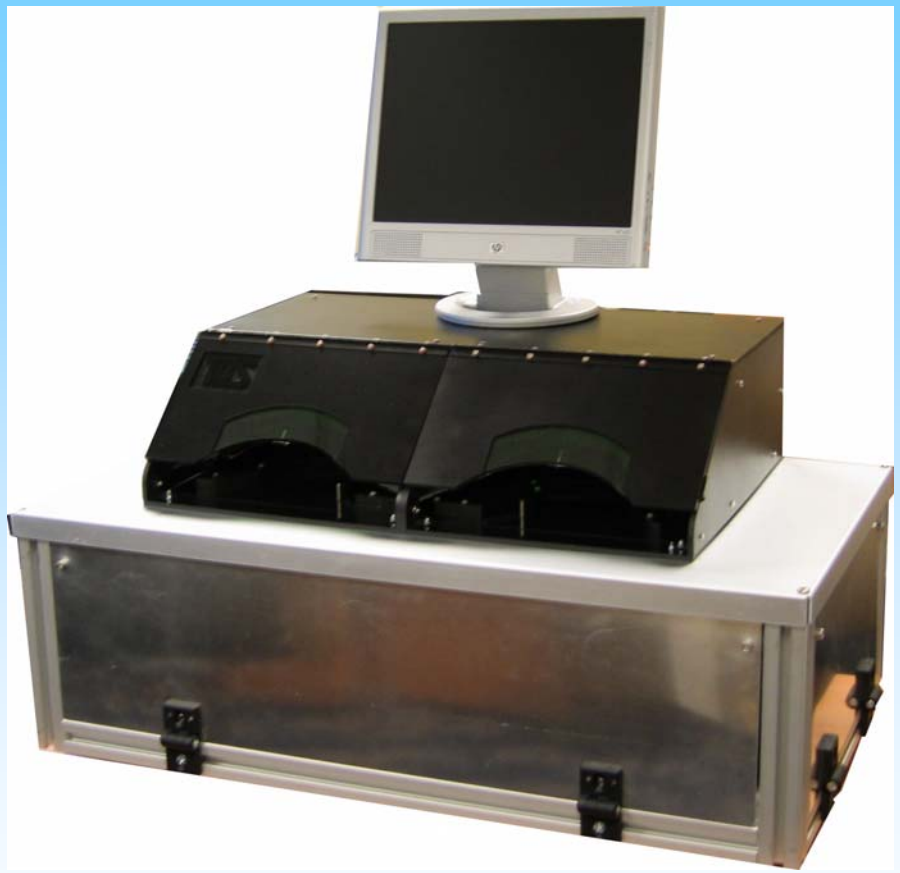
Research Directions

Biometric Recognition is not a fully solved problem

- New traits
- New sensors
- Salient representation
- Robust matching
- Multibiometric systems
- Soft biometrics
- System security
- Recognition at a distance
- Uniqueness of biometrics traits

Touchless Fingerprint Sensor

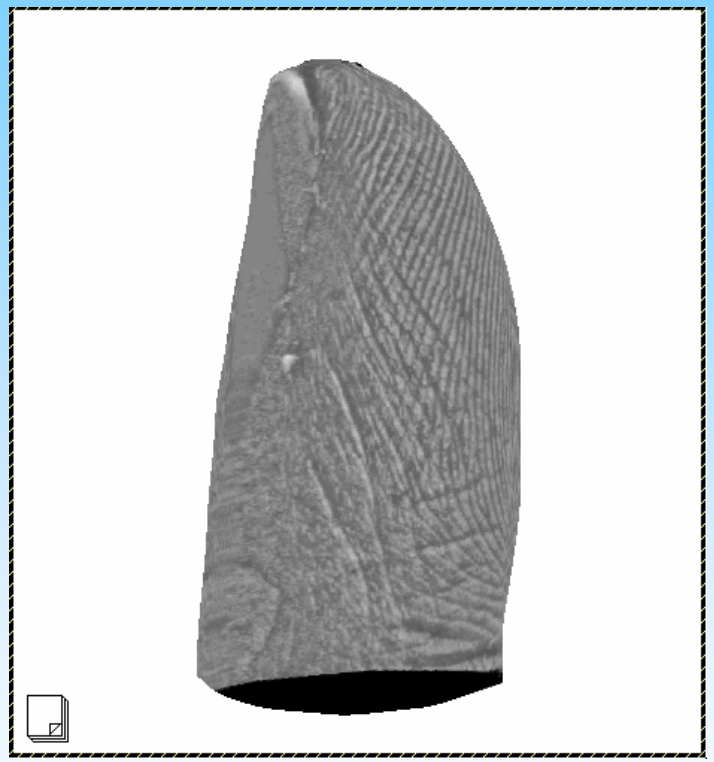
Surround Imager



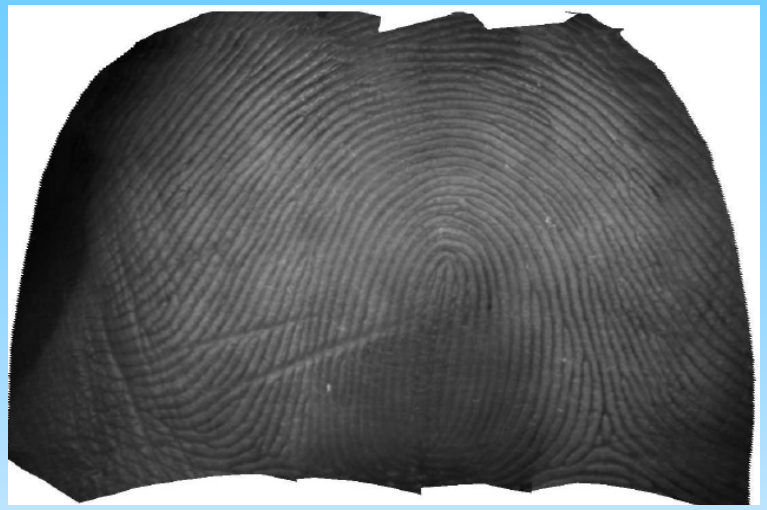
Ten print capture device

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

Interoperability



Touchless 3D image



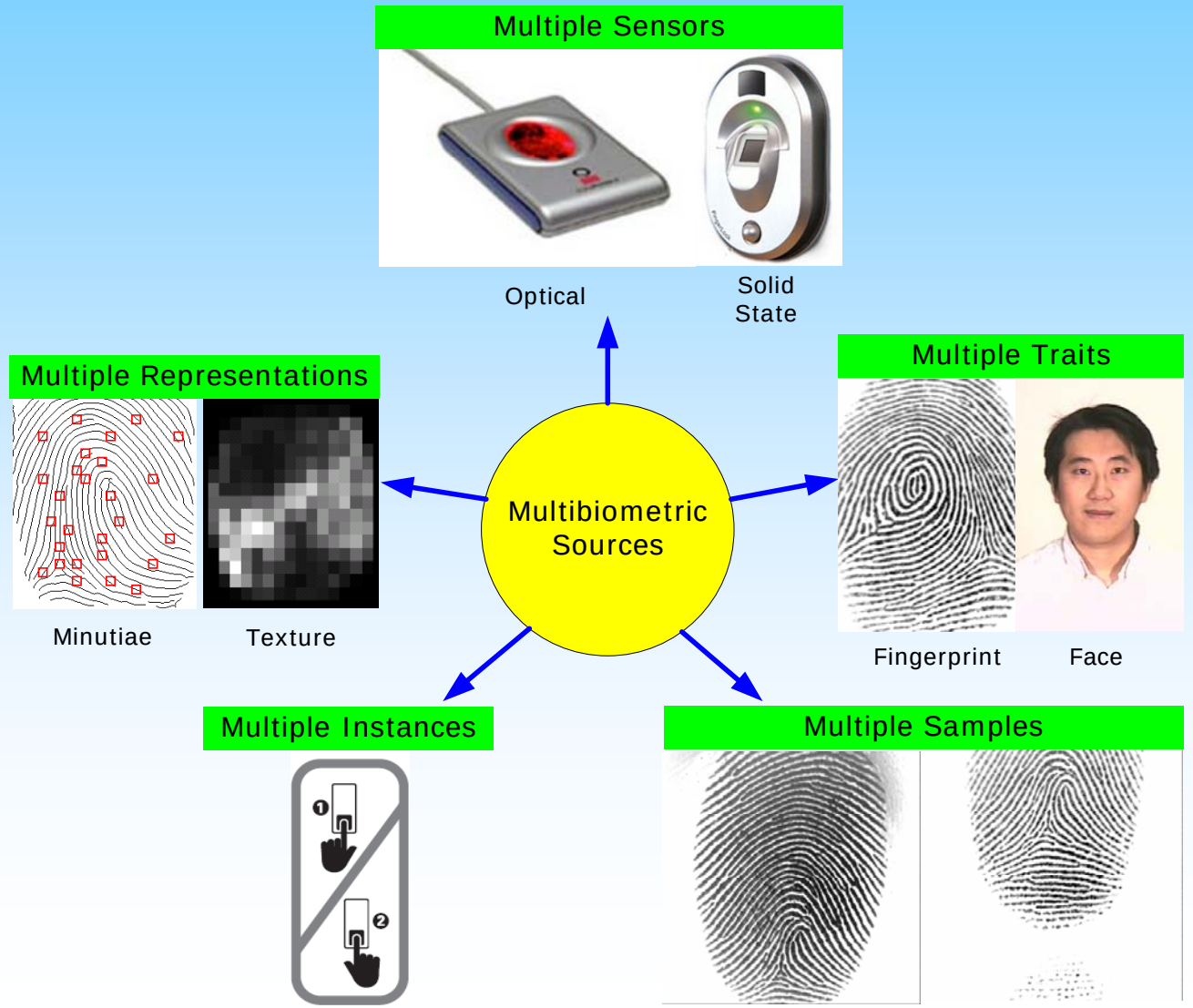
Virtual “rolled” image

Ink on paper

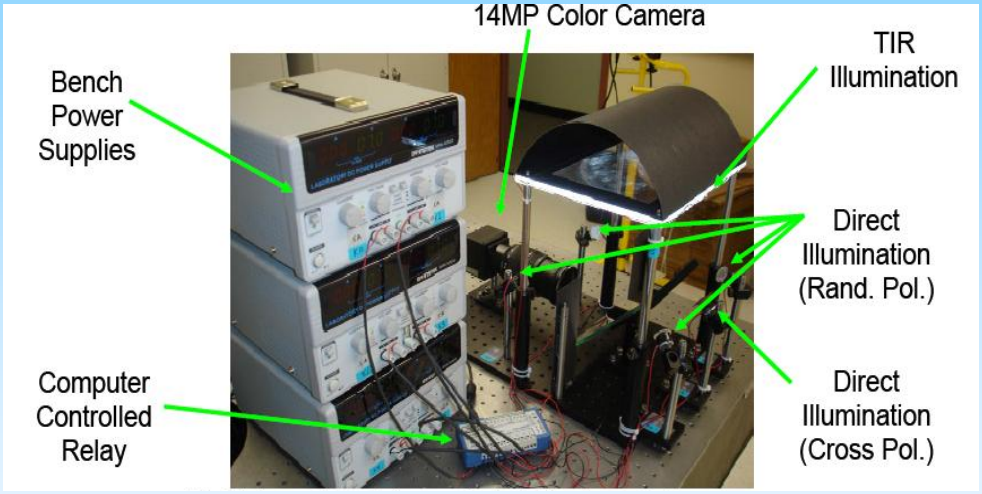
Courtesy TBS, NA

Multibiometrics

Decreases failure to enroll, spoof attacks, error rate

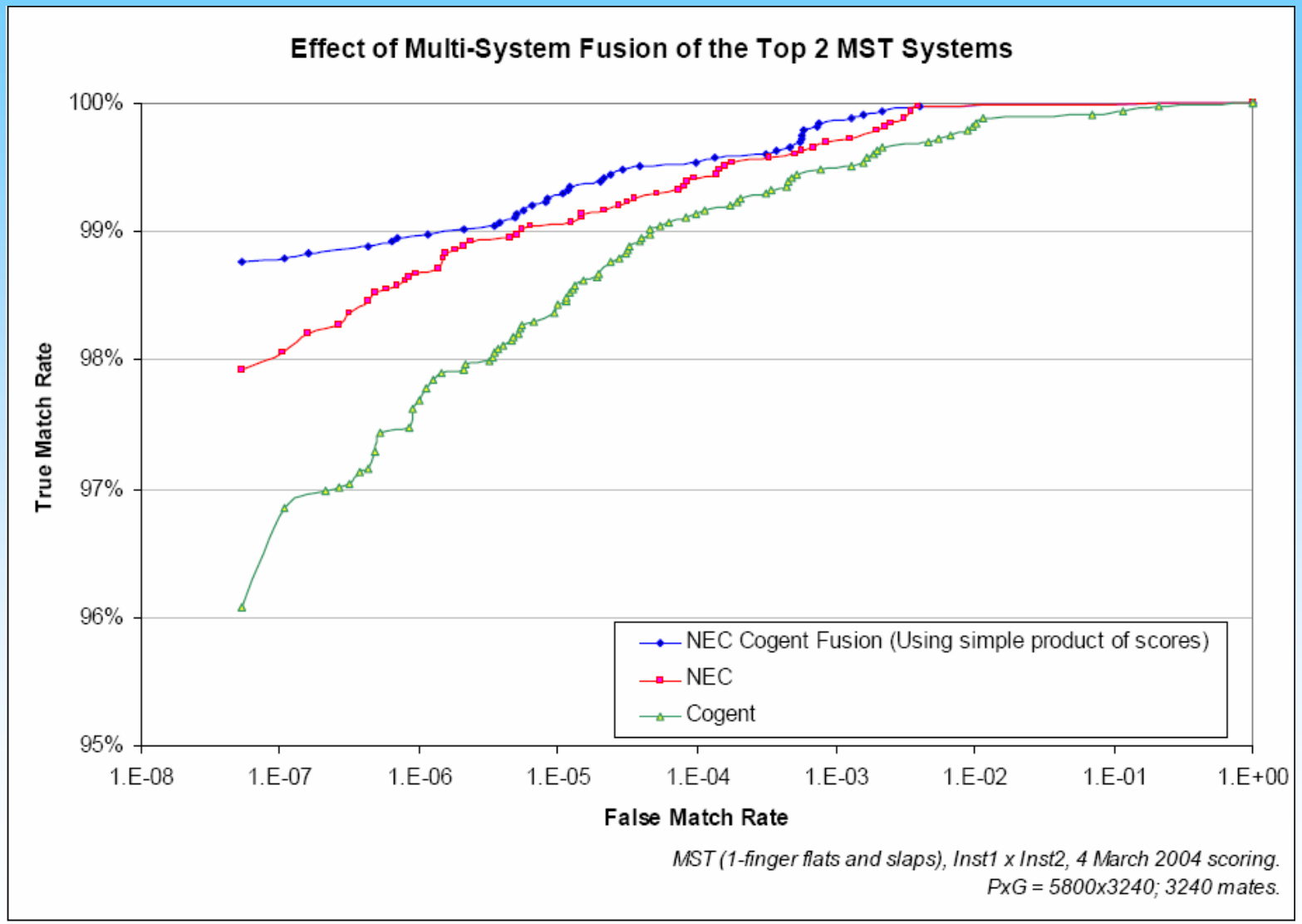


Sensing Multibiometric Traits



Courtesy, Lumidigm

Fusion of Matchers



Likelihood Ratio Based Fusion

- Neyman-Pearson theorem: For a given FAR, likelihood ratio (LR) test gives maximum GAR
- Let $\boldsymbol{S} = (S_1, S_2, \ldots, S_K)$ be the match score vector for K modalities. LR test decides "genuine" if

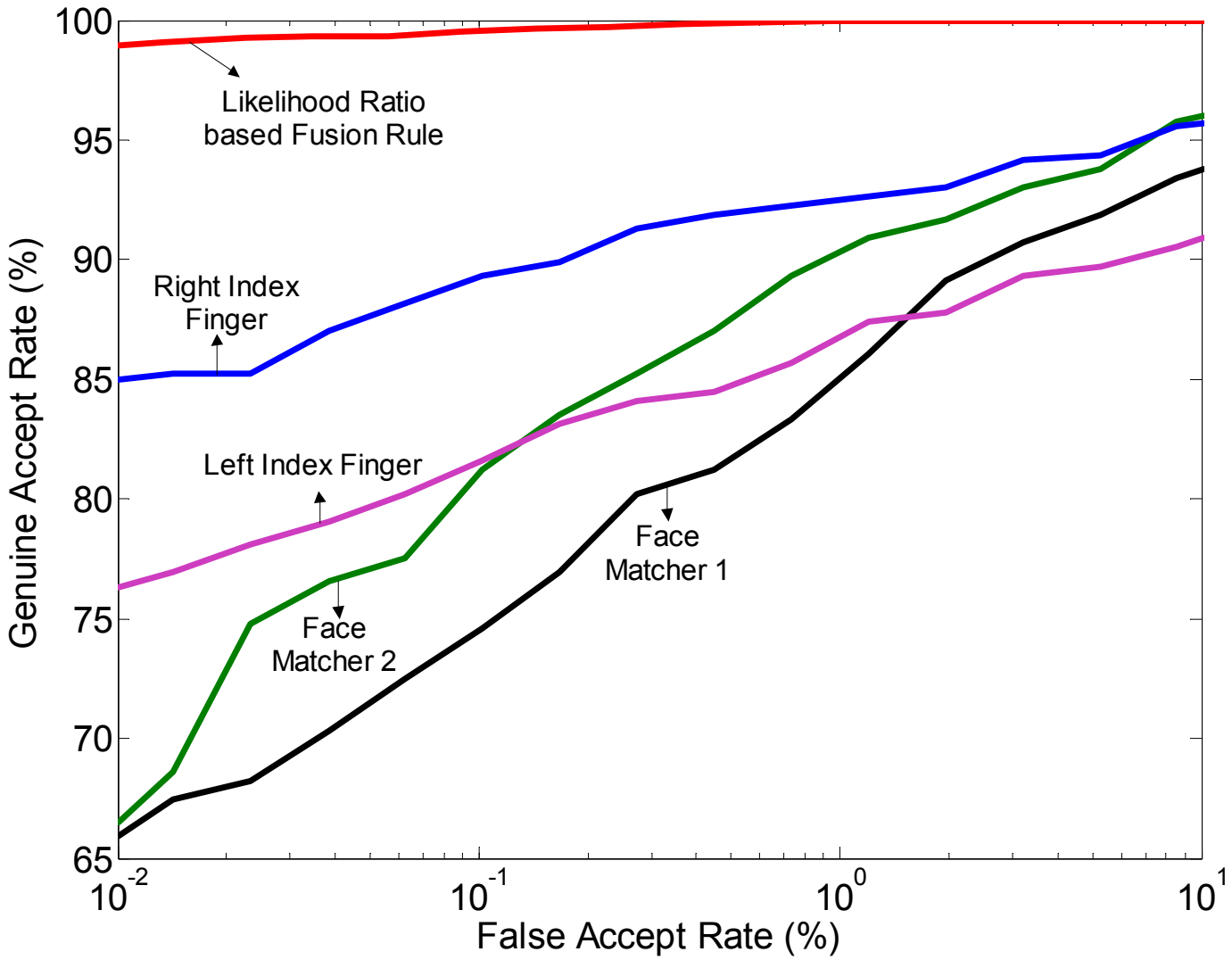
$$FS(\boldsymbol{S}) = \frac{P(\boldsymbol{S} \mid genuine)}{P(\boldsymbol{S} \mid impostor)} \geq \eta$$

where η is determined by the given FAR

- Let $\boldsymbol{Q} = (Q_1, Q_2, \ldots, Q_K)$ be the quality vector; quality-based fusion (QLR) rule decides "genuine" if

$$QFS(\boldsymbol{S},\boldsymbol{Q}) = \frac{P(\boldsymbol{S},\boldsymbol{Q} \mid genuine)}{P(\boldsymbol{S},\boldsymbol{Q} \mid impostor)} \geq \eta$$

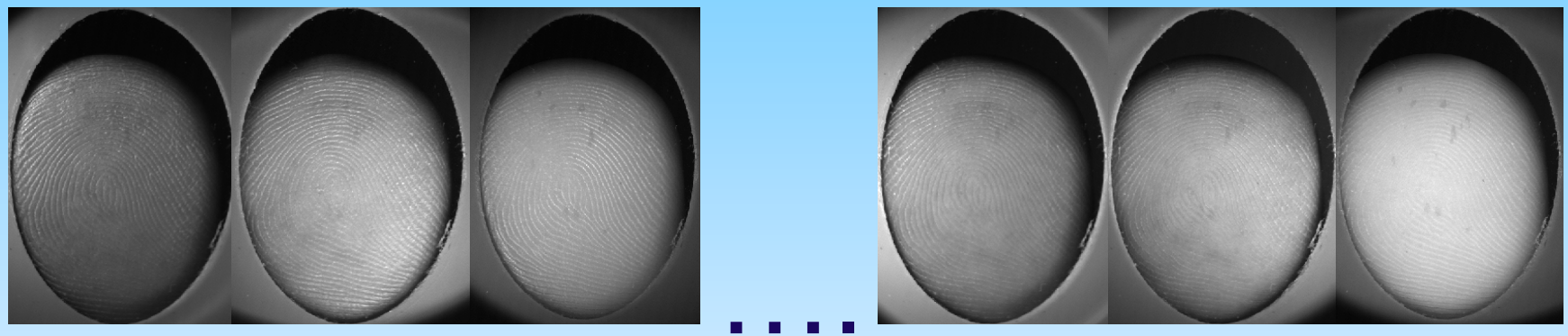
Fusing Face and Fingerprints



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

Countering Spoof Attacks

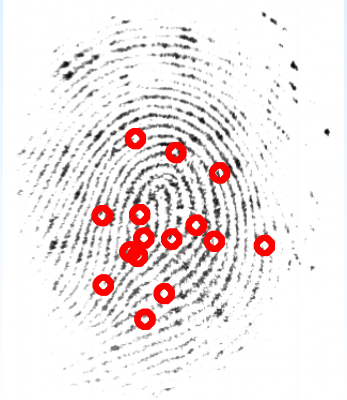
Multiple wavelengths capture fingerprint features at different depths (surface and subsurface) of tissue



Jupiter 1.10
Combined Image - MSI

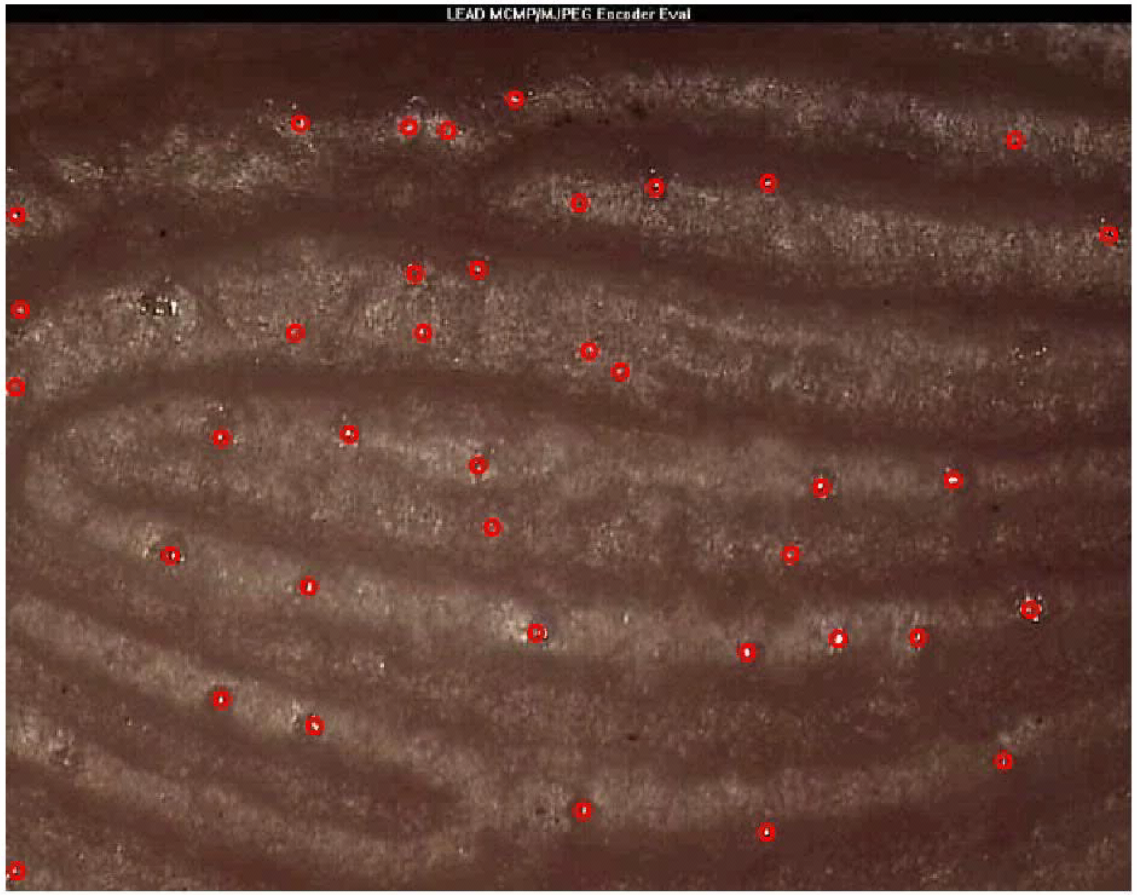
VS.

Cross Match Verifier
Model 300 - TIR



Courtesy, Lumidigm

High Resolution Sensors



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

Courtesy, TBS NA

Template Protection

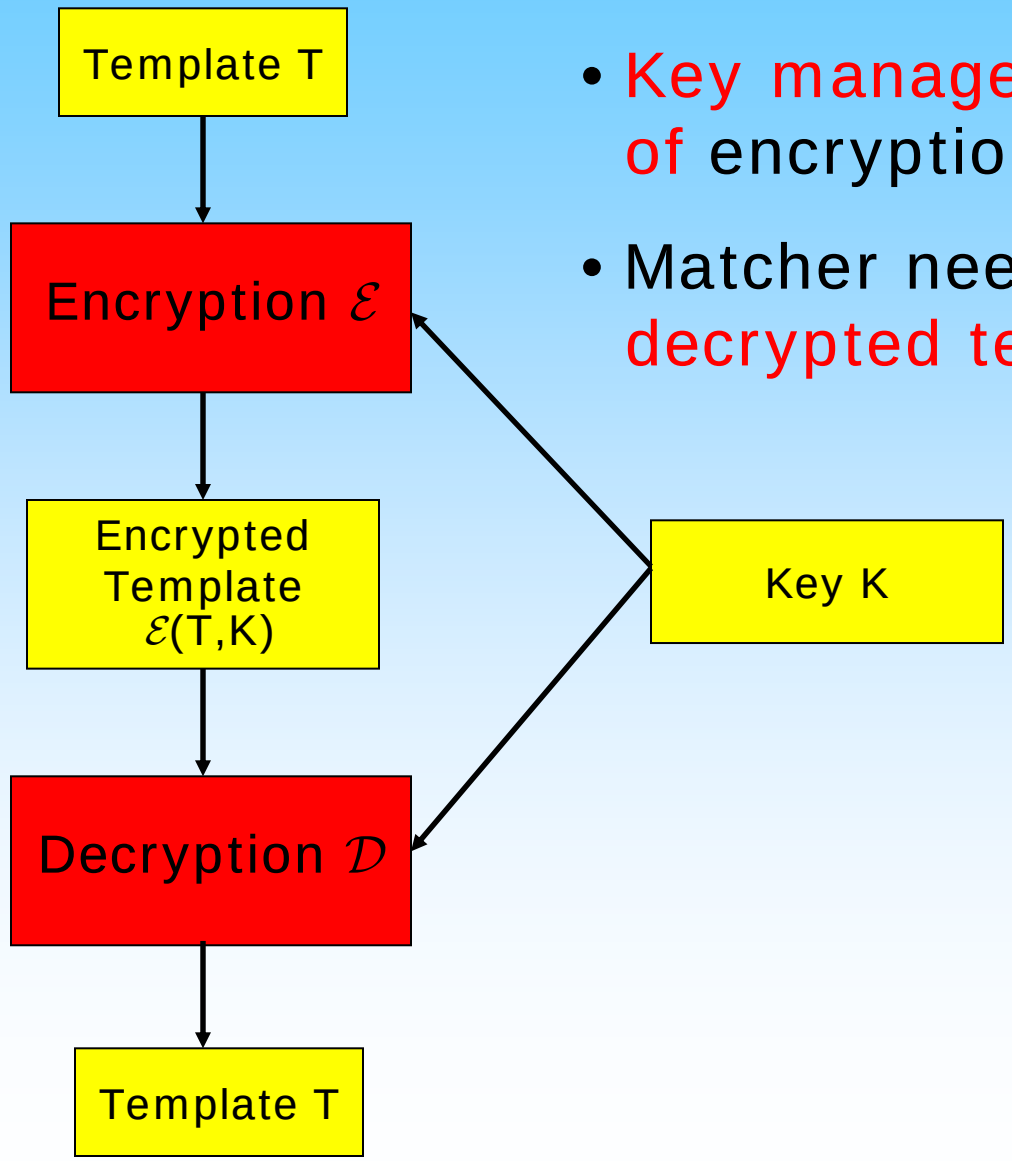
- Myth: “A true biometric image cannot be created from master template..”
- Template security is critical because it is not easy to revoke templates like passwords

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

Template Protection Goals

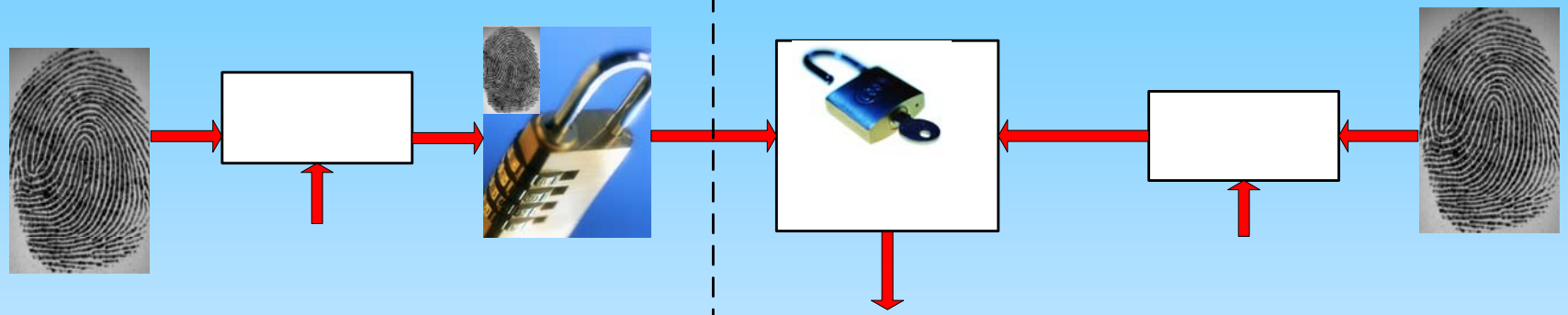
- Revocability
  - revoke compromised templates and reissue new ones based on the same biometric data
- Security
  - must be computationally hard to reverse engineer the original biometric template
- Performance
  - should not adversely affect matching error
- Privacy
  - prevent cross-matching across databases

Template Encryption

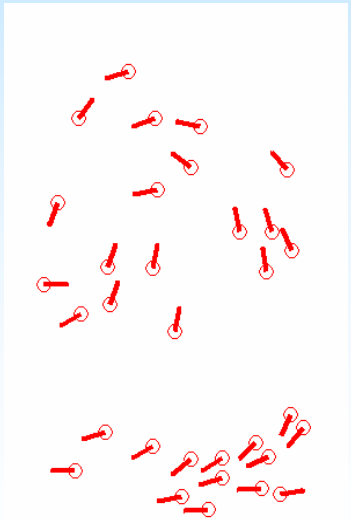


- Key management problem: security of encryption/decryption key
- Matcher needs original template; decrypted templates are vulnerable

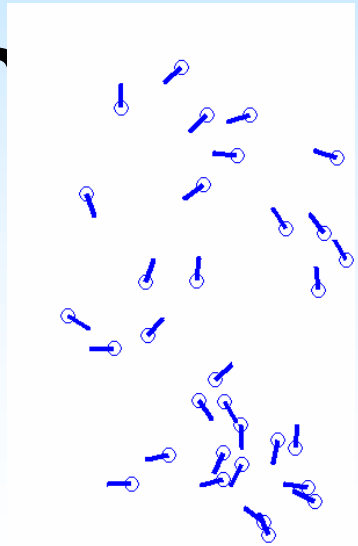
Non-invertible Transform



- Template is revoked by changing key/transform
- Matching in transformed domain; transformation is non-invertible, so security of key is not critical

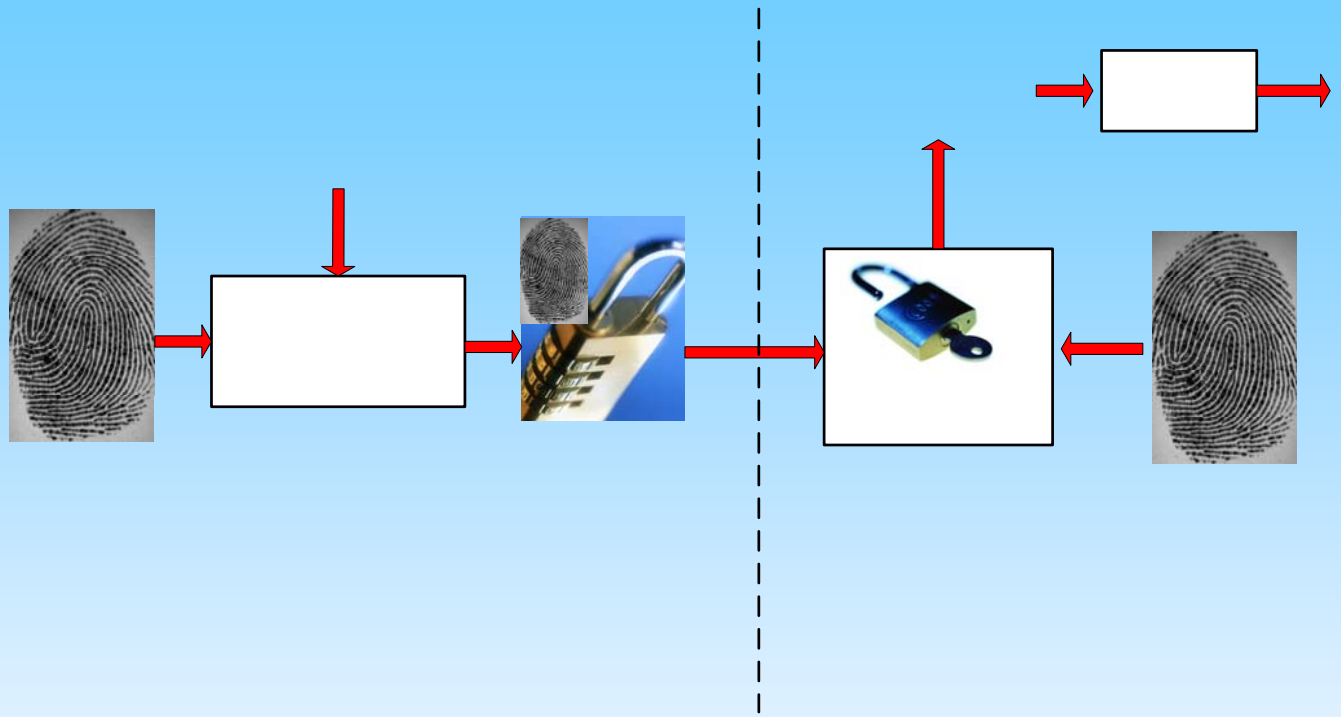


Original minutiae



Transformed minutiae

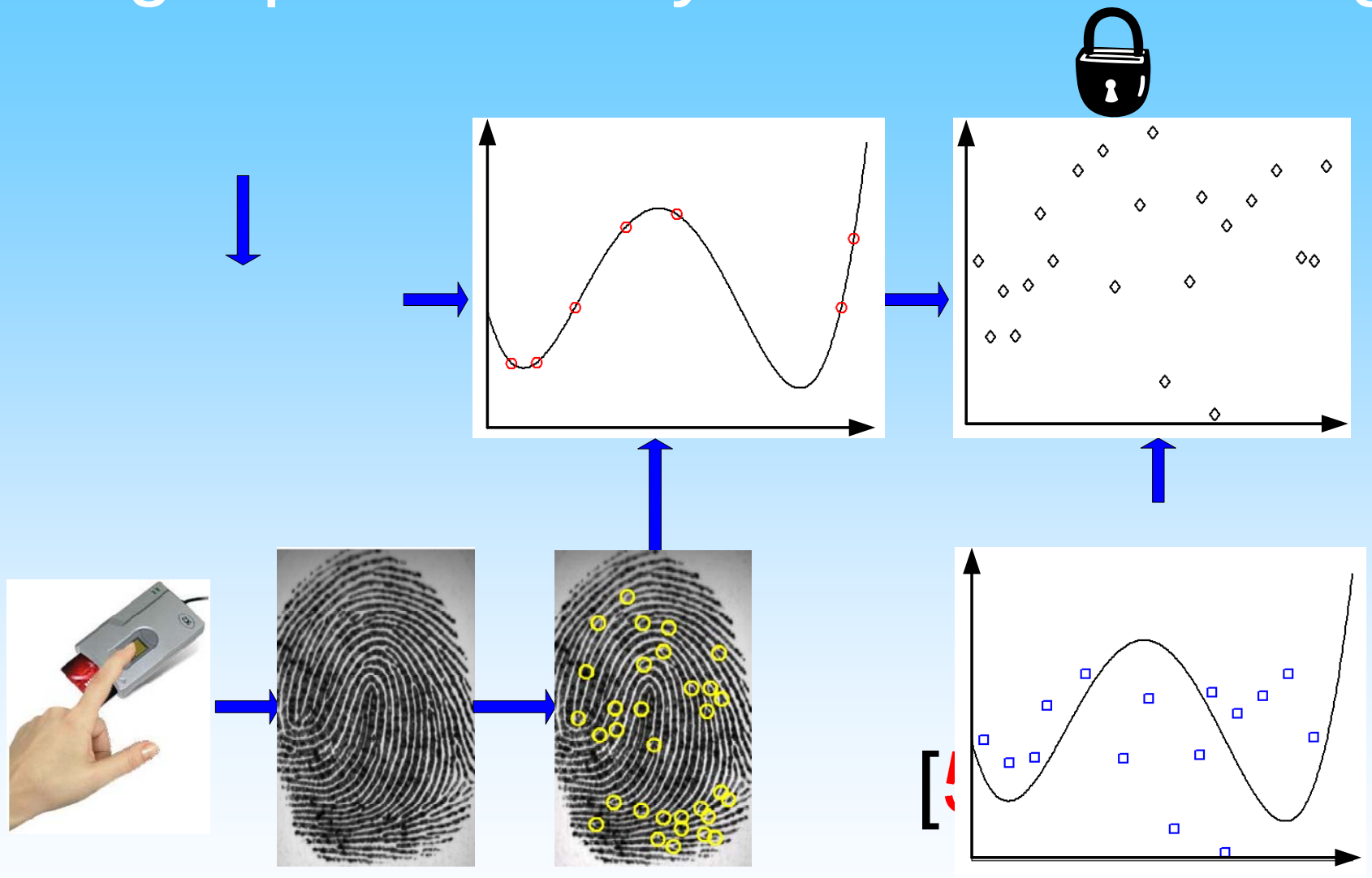
Biometric Cryptosystems



- A valid key can be generated from helper data only when the query is sufficiently close to the original template (Fuzzy Vault, Juels and Sudan 2002)
- Error correction capability of Recovery procedure allows limited intra-user variations in biometric data

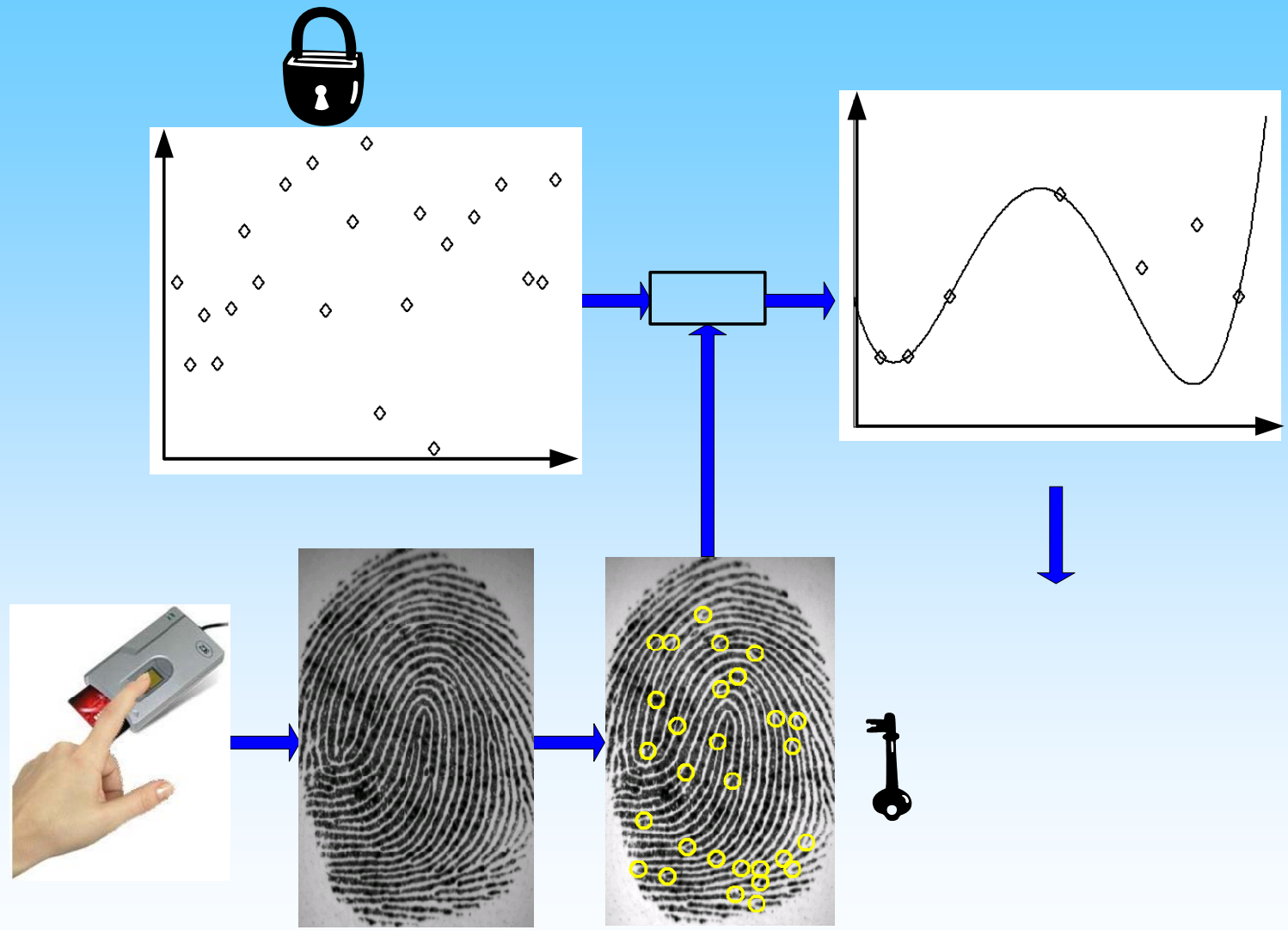
Key (K

Fingerprint Fuzzy Vault: Encoding



K. Nandakumar, A. K. Jain and S. Pankanti, "Fingerprint-based Fuzzy Vault: Implementation and Performance", *IEEE Trans. on Info. Forensics & Security*, 2007 (To appear)

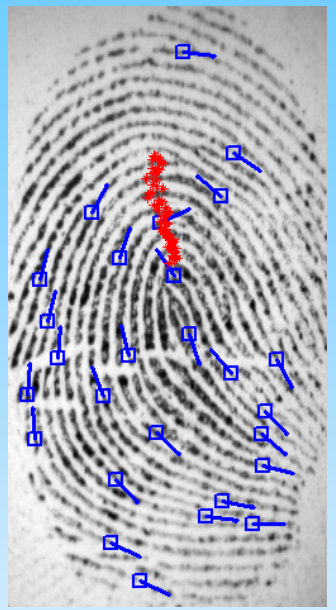
Fingerprint Fuzzy Vault: Decoding



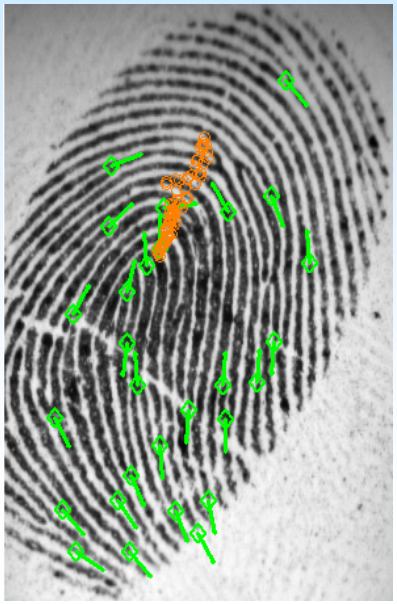
Recovery of a valid key indicates successful match

Fingerprint Vault Performance

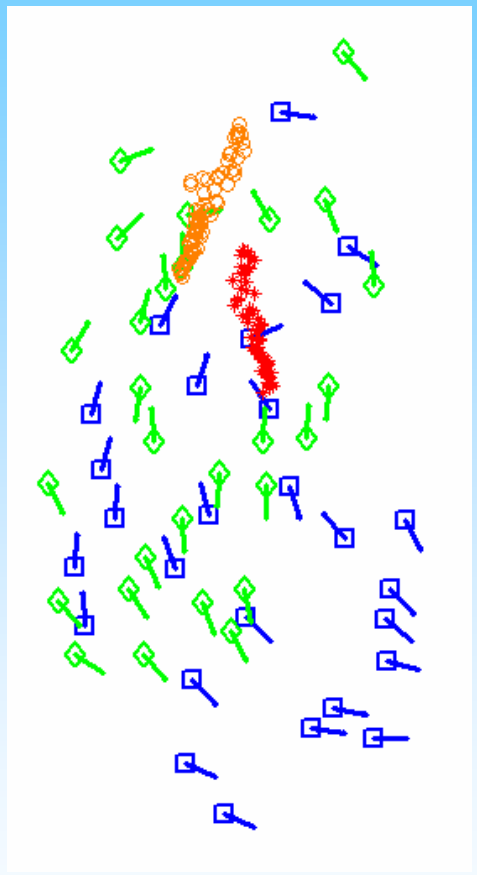
Template



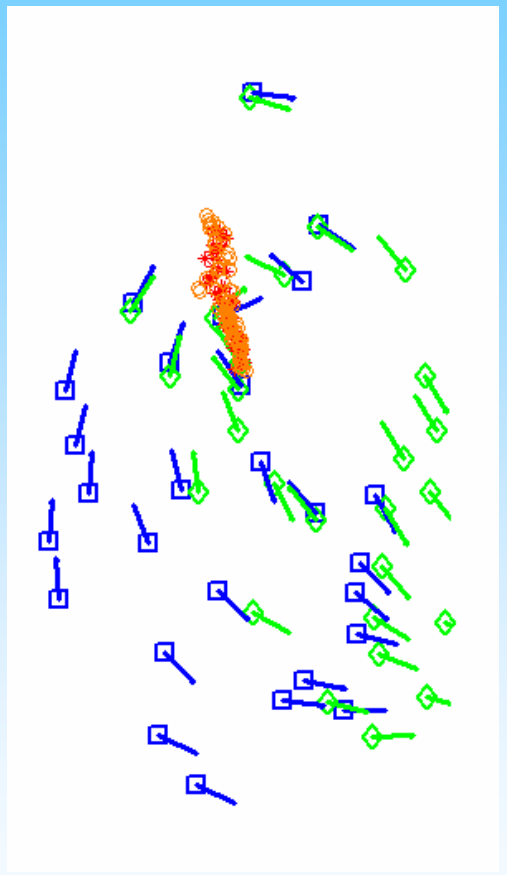
Query



Before alignment

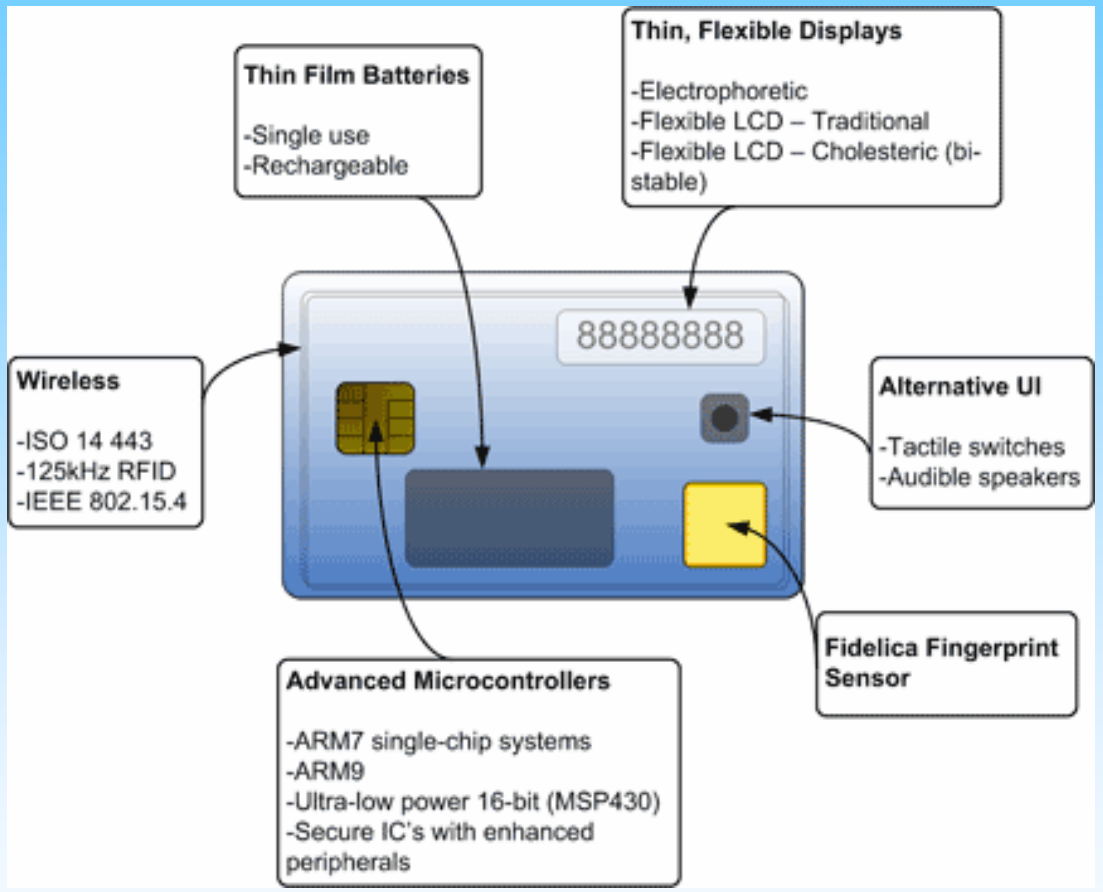


After ICP alignment



- High curvature points do not reveal template
- GAR of 91% at a FAR of 0.01% on FVC 2002 database; slight loss in performance due to small no. of minutiae and alignment error

Biometric System on Secure Chip



Privaris plusID

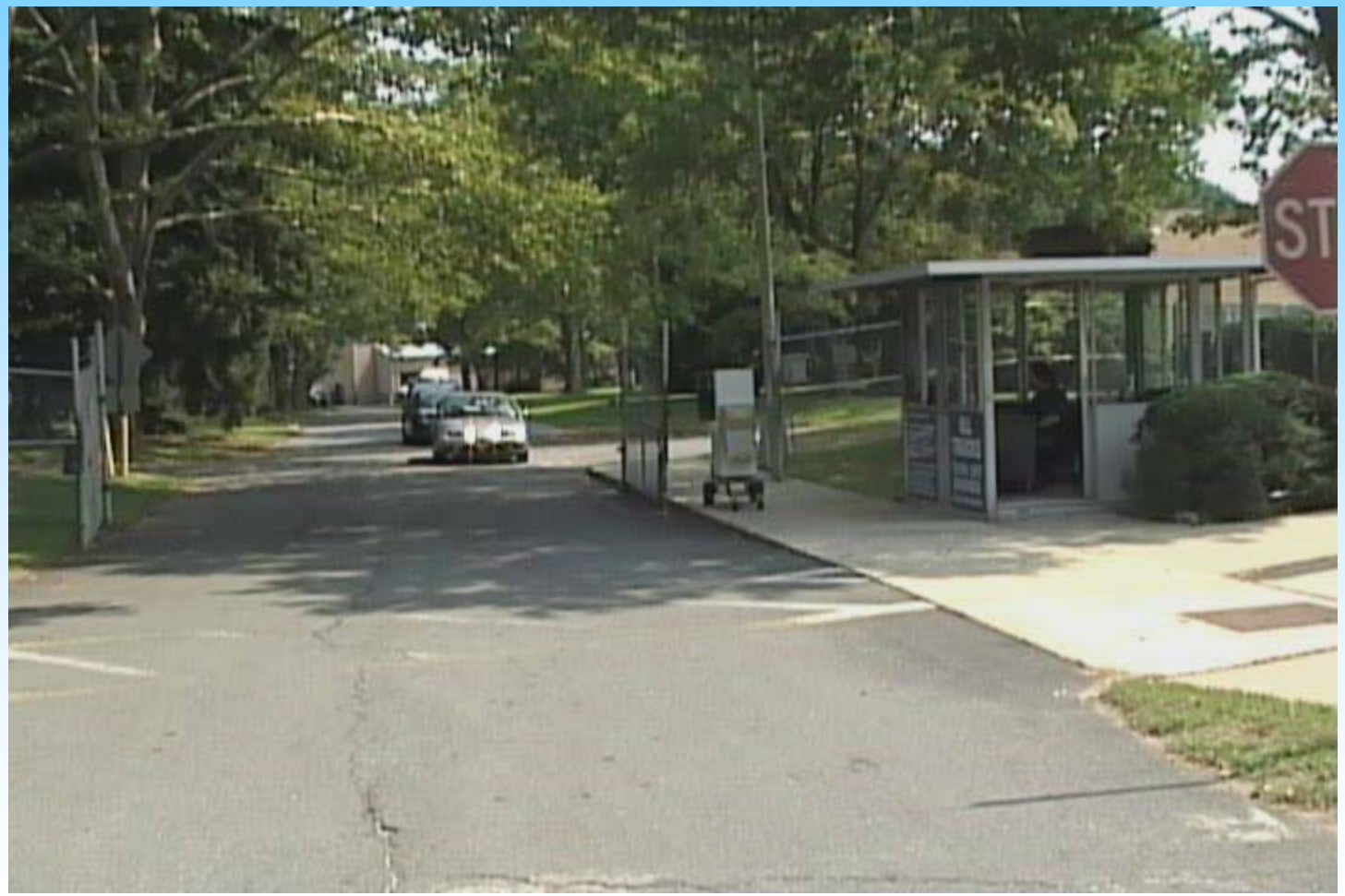
Pros: Biometric sample is secure; template is secure; feature extraction is trusted; matching is trusted

Cons: Requires very small reader; less accurate

http://www.fidelica.com/solutions/index.php

Iris at a Distance

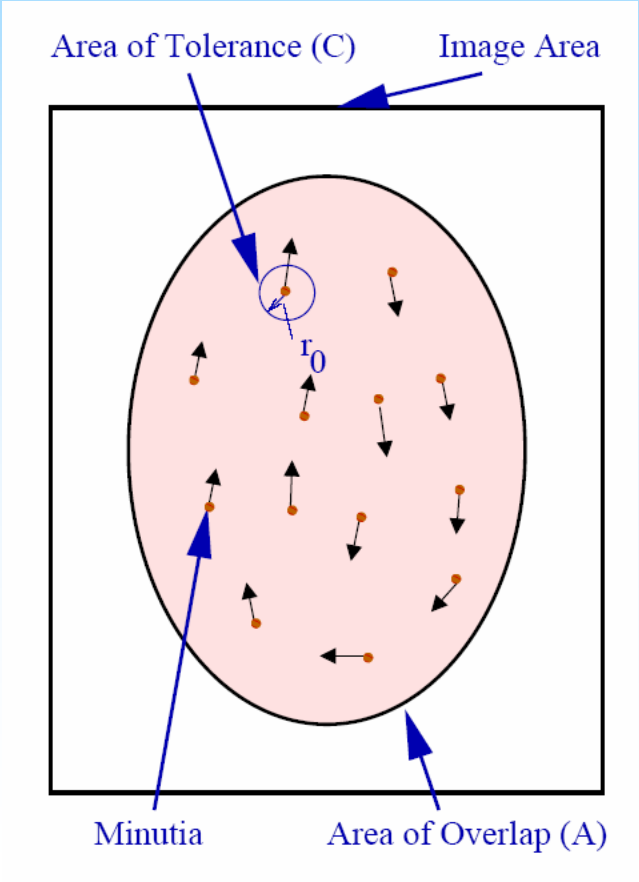
- Current systems require proximity to sensor



Courtesy: Jim Matey, Sarnoff

Uniqueness of Biometric Traits

- "Two Like Fingerprints Would be Found Only Once Every 10^{48} Years" *Scientific American, 1911*
- Given two fingerprints with m & *n* minutiae, what is the probability they will share *q* minutiae? USA v Daubert (1993), USA v Byron Mitchell (1999)



1. m=n=52, q=12
   PRC = 4.4×10^{-3}
   (Observed value = 3.5×10^{-3})

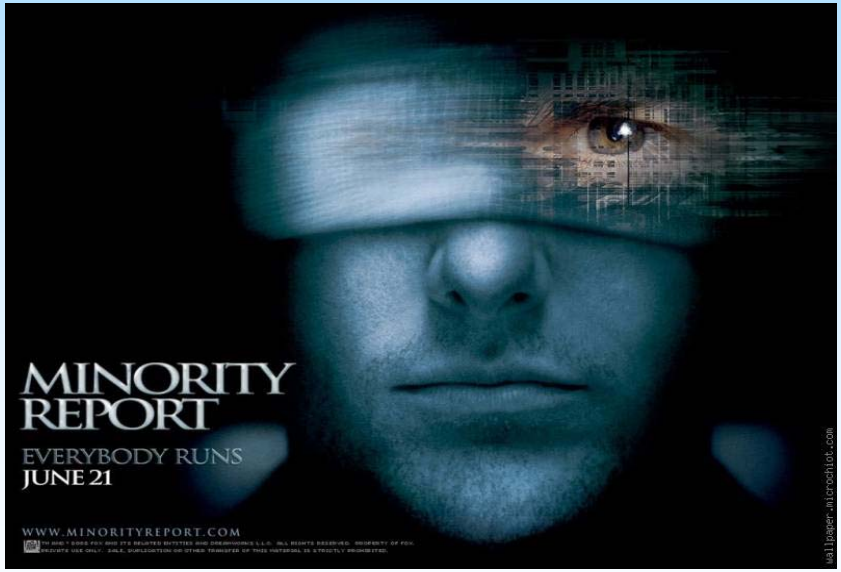
2. m=n=52, q=26
   PRC = 3.4×10^{-14}

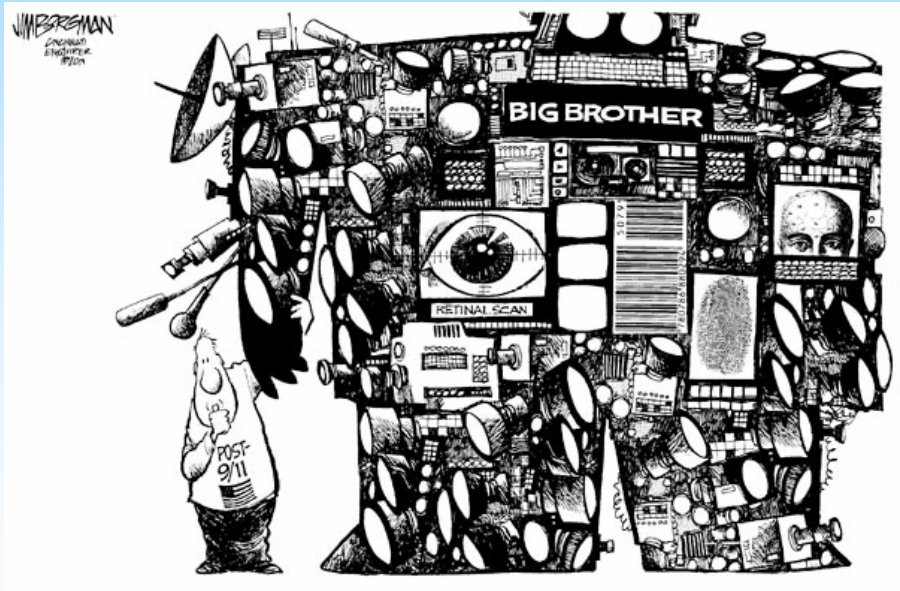
M = A/C=413 (NIST-4 database)

Y. Zhu, S.C. Dass and A.K. Jain, "Statistical Models for Assessing the Individuality of Fingerprints", IEEE TIFS, Vol. 2, No. 3, pp. 391-401, September 2007

Privacy Concerns

- Will biometric be used to track people?
- Will biometric be used only for the intended purpose? Will the databases be “linked”? (Function creep)
- How do we alleviate these concerns?





Summary

- Reliable personal recognition is critical to many business processes; a sound recognition system must incorporate biometric component
- Accuracy of current biometric systems is not perfect; will foolproof systems ever exist?
- Security requirements depend on the threat model and cost-benefit analysis; biometric systems are effective deterrents to perpetrators
- A tradeoff between security & privacy might be necessary; responsible use of biometrics can in fact protect individual privacy

Identification at a Distance

"Would you like to see the top on Google Earth?"