Biometrics: A Grand Challenge

Anil K. Jain, Sharath Pankanti, Salil Prabhakar,
Lin Hong, Arun Ross, and James L. Wayman

Michigan State University, IBM T. J. Watson Research Center, DigitalPersona Inc.,
Siemens Corporate Research, West Virginia University, San Jose State University

http://biometrics.cse.msu.edu

Person Identification

- Identifying fellow human beings has been crucial to the fabric of human society

- In the early days of civilization, people lived in small communities and everyone knew each other

- With the population growth and increase in mobility, we started relying on documents and secrets to establish identity

- Person identification is now an integral part of the infrastructure needed for diverse business sectors such as banking, border control, law enforcement..

Identification Problems

Security Threats:

We now live in a global society of increasingly desperate and dangerous people whom we can no longer trust based on identification documents which may have been compromised

Senator? Terrorist? A Watch List Stops Kennedy at Airport: Senator Edward M. Kennedy, Democrat of Mass., discussed the problems faced by ordinary citizens mistakenly placed on terrorist watch lists. Between March 1 and April 6, airline agents tried to block Mr. Kennedy from boarding airplanes on five occasions because his name resembled an alias used by a suspected terrorist who had been barred from flying on airlines in the United States. RACHEL L. SWARNS,NY Times,Aug 20, 2004

Identification Problems

Identity Theft: Identity thieves steal PIN (e.g., date of birth) to open credit card accounts, withdraw money from accounts and take out loans

3.3 million identity thefts in U.S. in 2002; 6.7 million victims of credit card fraud

Surrogate representations of identity such as passwords and ID cards no longer suffice

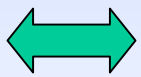
Too Many Passwords to Remember!

• Heavy web users have an **average of 21 passwords**; 81% of users select a common password and 30% write their passwords down or store them in a file. *(2002 NTA Monitor Password Survey)*

Biometrics

utomatic recognition of people based on their distinctive anatomical (e.g., face, fingerprint, iris, retina, hand geometry) and behavioral (e.g., signature, gait) characteristics

ecognition of a person by their body, then linking that body to an exte l "identity", forms a very powerful tool



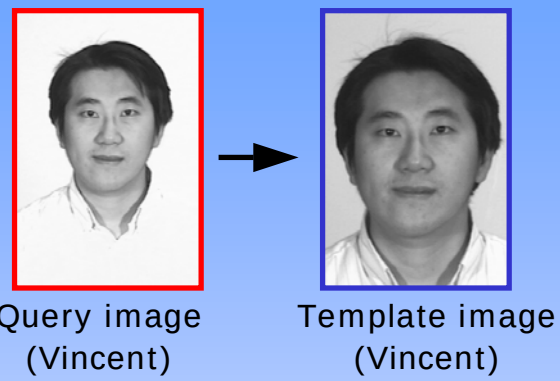
John Smith

Biometric Functionalities

- Positive Identification

  Is this person truly known to the system?

  Provide log-in access to a valid user



- Large Scale Identification

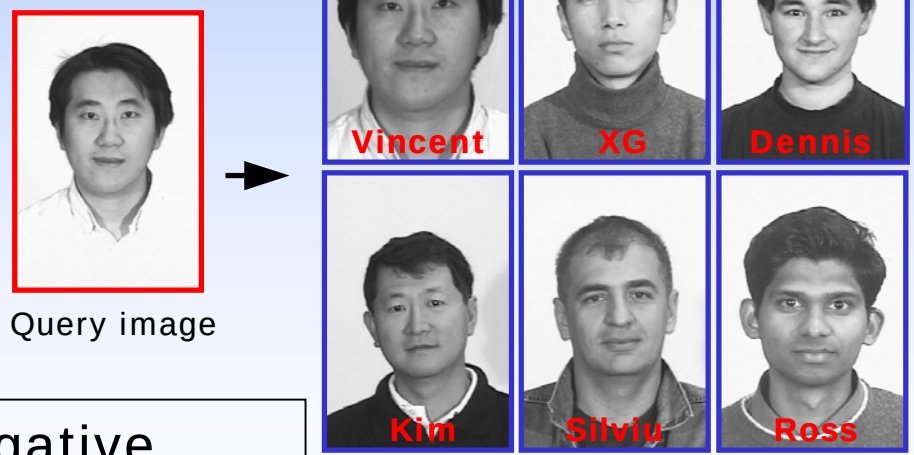
  Is this person in the database?

  Prevent issuing multiple driver licenses to the same person

- Screening

  Is this a wanted person?

  Airport watch-list



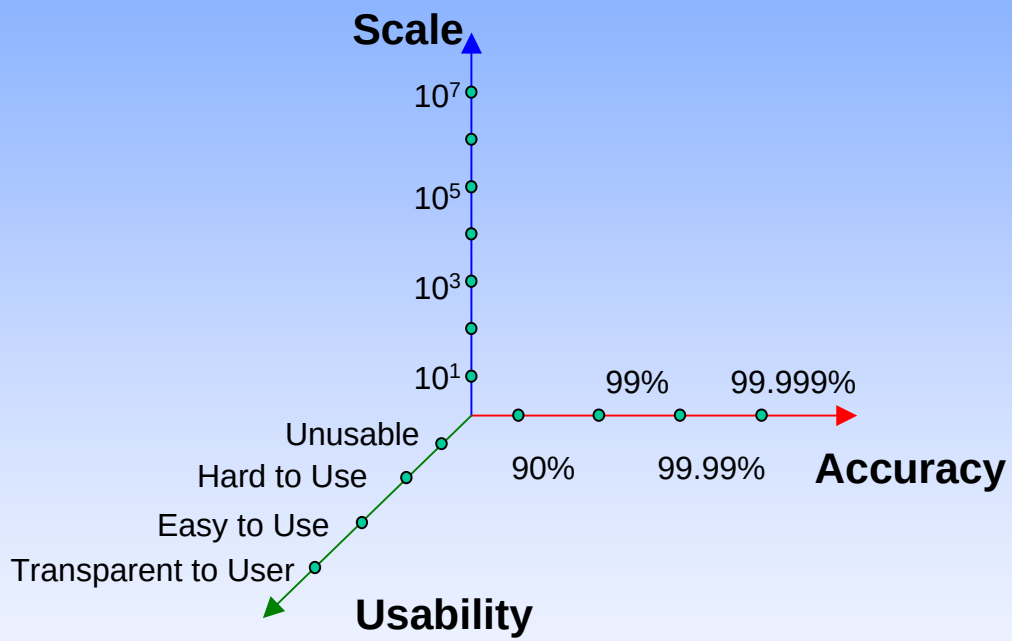
Only biometrics can provide negative identification (i.e., I am not he) capability

Biometrics: A Killer P.R. Application

- A Challenging Pattern Recognition Problem
- Enabling Technology to make our society safer, reduce fraud and offer user convenience (user-friendly man-machine interface)
- Policy-makers worldwide concede this is one of the crucial components of reliable person identification
- Given its *unique* capability of identifying persons based on their *intrinsic* characteristics, it will emerge as a pervasive tool for personal identification

Biometrics: A Grand Challenge

"A fundamental problem in science and engineering with broad economic and scientific Impact"



The grand challenge is to design a biometric system that would operate on the extremes of all these three axes simultaneously

US-VISIT
www.dhs.gov/us-visit

Homeland Security

As part of the enhanced procedures, most visitors traveling on visas will have two fingerprints scanned by an inkless device and a digital photograph taken. All of the data and information is then used to assist the border inspector in determining whether or not to admit the traveler. These enhanced procedures will add only seconds to the visitor's overall processing time. (*DHS US-VISIT web-site*)

The electronic fingerprint scanner will allow inspectors to check identities of visitors against those on terrorist watch lists. (Stephen J. Boitano, AP)

There are ~500 million border crossings/year (each way) in the U.S.

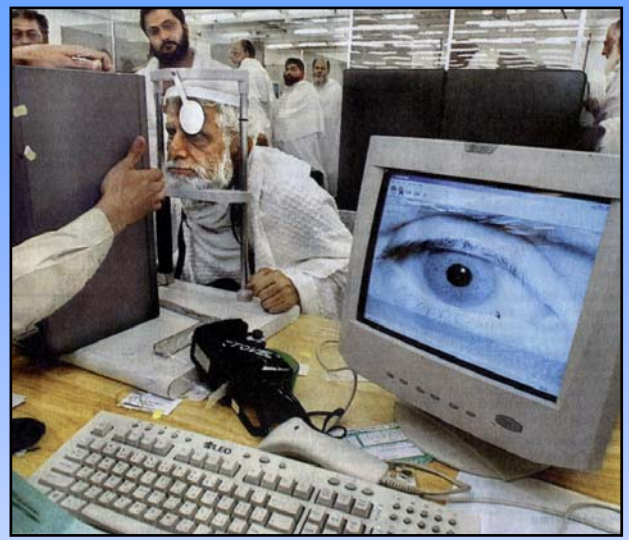
Want to Charge It?

Beepcard, a company in California, has designed a credit card that works only when it recognizes the voice of its rightful owner

Enclosed in the card is a tiny microphone, a loudspeaker and a speech recognition chip that compares the spoken password with a recorded sample.

Total credit card fraud amounts to billions of dollars every year

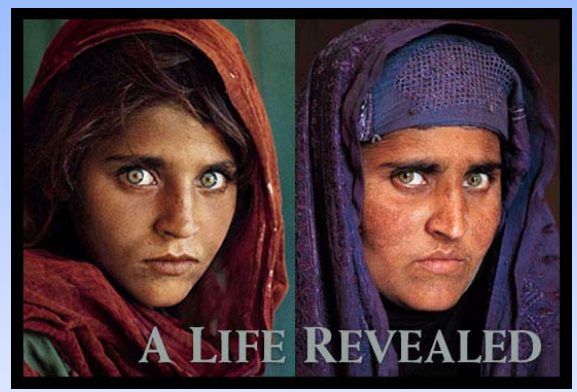
Biometric Applications



Haj pilgrims in Saudi Arabia

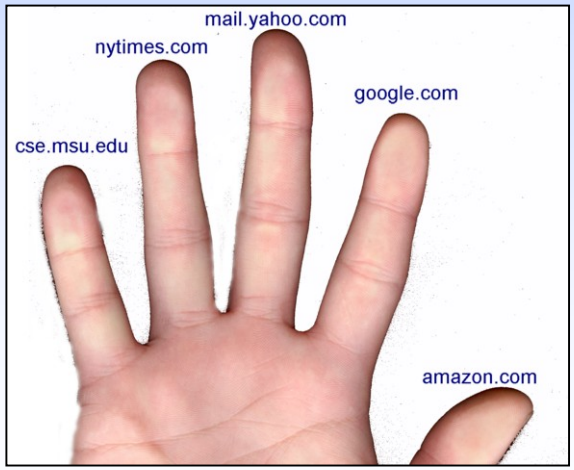
Point of sale

Disney World



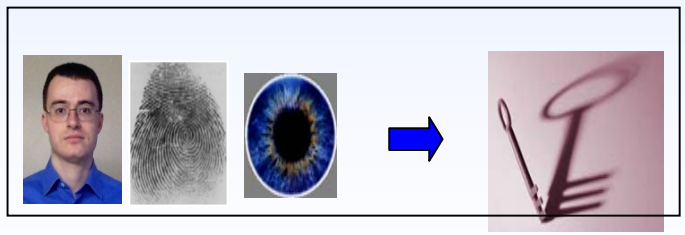
Sharbat Gula in 1985, 1992

Iris-based ATM



URL at your fingertip

Mobile phone



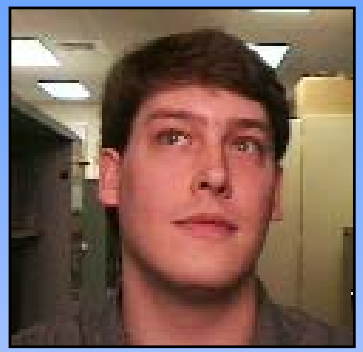
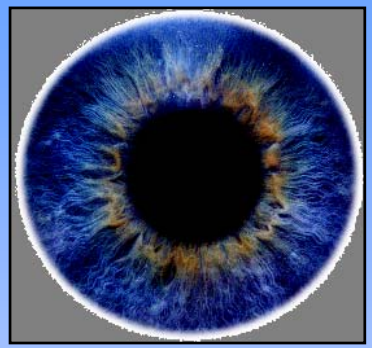
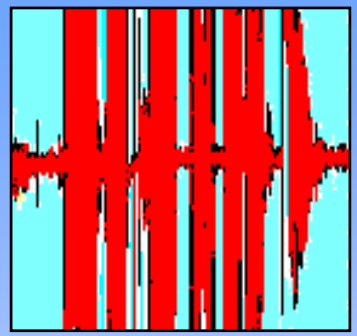
Secure multimedia

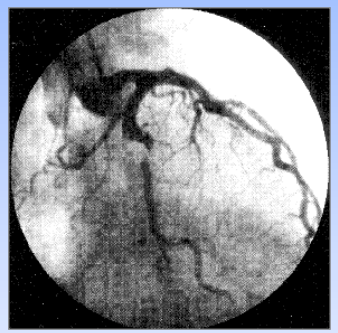
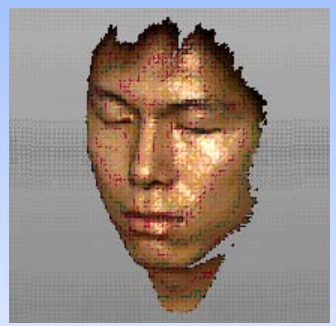
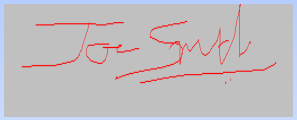
Biometrics is Not New!

- Bertillon system (1882) took subject's photograph, and recorded height, the length of one foot, an arm and index finger
- Galton/Henry system of fingerprint classification adopted by Scotland Yard in 1900
- FBI set up a fingerprint identification division in 1924
- AFIS installed in 1965 with a database of 810,000 fingerprints
- First face recognition paper published in 1971 (Goldstein et al.)
- FBI installed IAFIS in ~2000 with a database of 47 million 10 prints; average of 50,000 searches per day; ~15% of searches are in lights out mode. 2 hour response time for criminal search

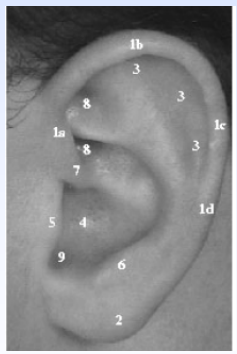
Emphasis now is to automatically perform reliable person identification in unattended mode, often remotely (or at a distance)

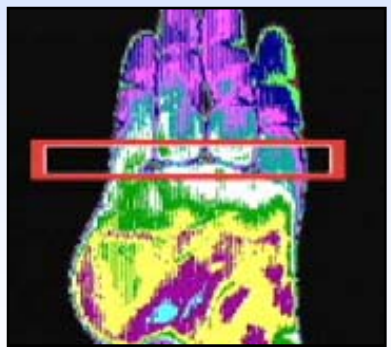
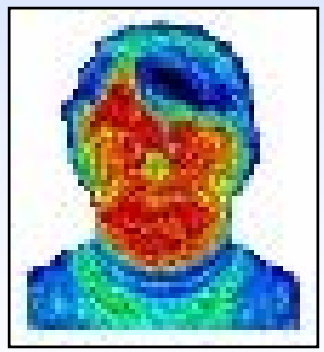
Biometric Characteristics

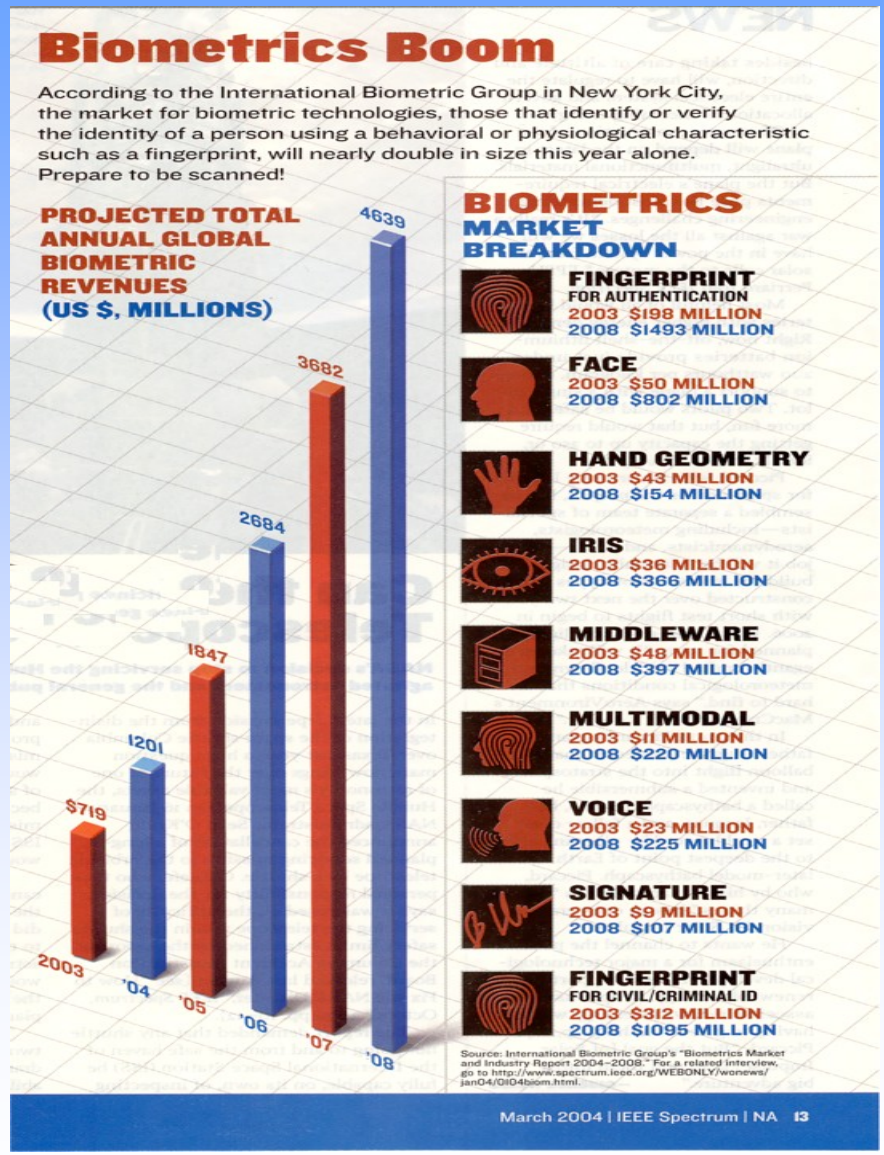









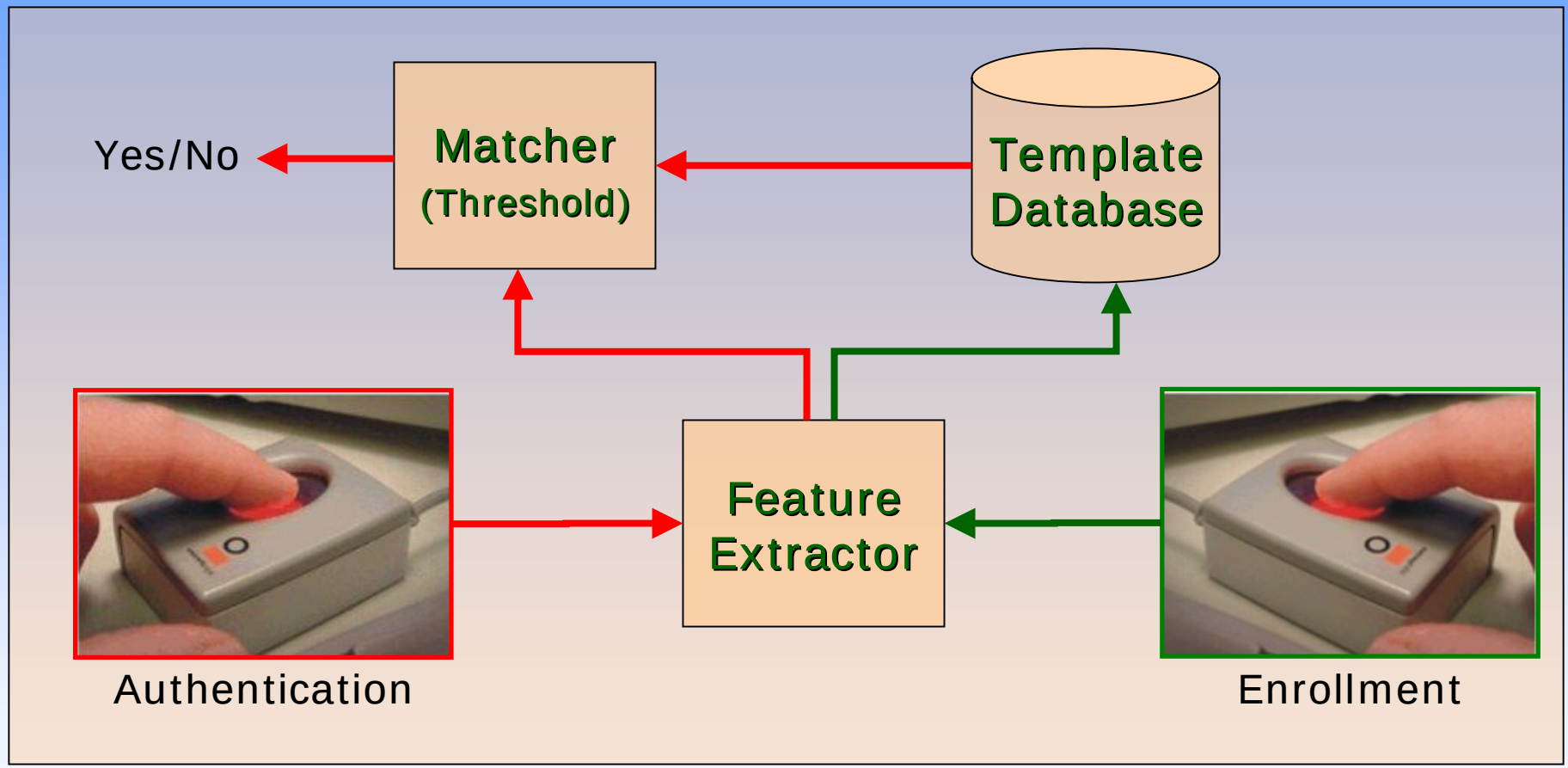



Biometric Market Growth



International Biometric Group

Biometrics: A Pattern Recognition System



- False accept rate (FAR): Proportion of imposters accepted
- False reject rate (FRR): Proportion of genuine users rejected

Why is Biometrics so Difficult?

- Intra-class variability and inter-class similarity
- Segmentation
- Noisy input & population coverage
- System performance (error rate, speed, cost)
- Individuality of biometric characteristics
- Fusion of multiple biometric attributes
- Scalability
- Attacks on the biometric system
- Privacy Issues

Intra-class and Inter-class Variations

Variability observed in the face image of a single person due to change in pose, expression, lighting and eye glasses

Faces that look similar

R.-L. Hsu, "Face Detection and Modeling for Recognition", Ph.D. Thesis, 2002

Recognizing the Smile

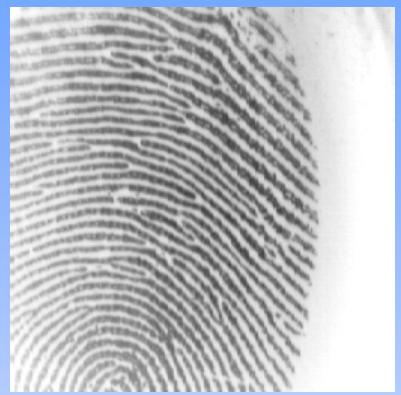
Home Office prohibits happy biometric passports

- The Home Office says all new passport photographs must be of an unsmiling face with its gob firmly shut because open mouths can confuse facial recognition systems.
- The new guidelines state that photographs must have a strong definition between the face and background; be of the full face facing straight at the camera; show no shadows, and that subjects must have "a neutral expression, with your mouth closed".
- A Sun report confidently tells its readers that "immigration Service officials will run the passport through scanners which will cross-check them against worldwide crime memory banks" and that "the 'biometric' tests ensure that people cannot use stolen or fake documents".

- Lucy Sherriff, *The Register*, Aug. 6, 2004

Temporal Variations





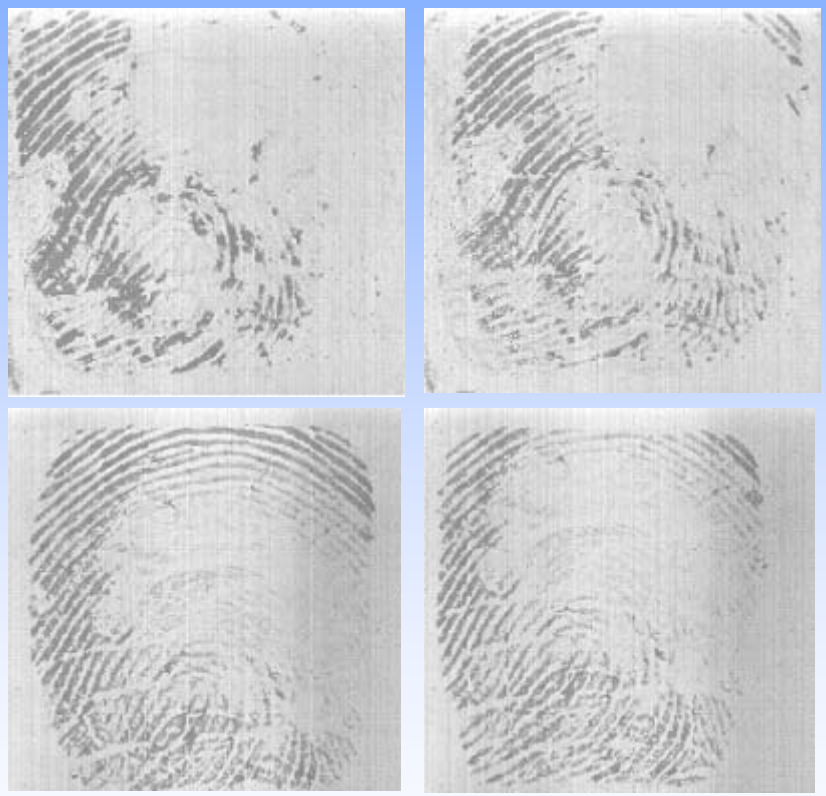



Sensor Interoperability

- Sensors used during enrollment and verification may be different

Noisy Images

- ~ 3% of the population has poor quality fingerprint images



Four impressions of a user's fingerprint

Jan 2, 2004

Faded fingerprints cost former welder a job

ASSOCIATED PRESS

DECATUR — The years Chuck Strickler spent as a welder provided him with the experience he needed as a welding inspector at power plants across the nation.

But the welding also has left Strickler, 60, of Decatur, lacking a full set of intact fingerprints required under new, stepped-up security regulations at nuclear plants. Since the U.S. Department of Homeland Security issued the new rules in the wake of Sept. 11, the reams of documents Strickler has attesting to his identity no longer are sufficient.

"I first ran into a problem with it three or four years ago," Strickler said. "They said my fingerprints weren't valid. But at the time they accepted a picture ID as proof of identity."

Earlier this year, when he tried to get a job inspecting the D.C. Cook Nuclear Power Station near Bridgman, where he had worked before, his application was turned down because of the worn-down ridges on his fingertips.

"I passed everything except for the fingerprints," Strickler said adding that the application process included a comprehensive psychological examination and criminal background check.

Strickler

"The plant sent the fingerprints to the FBI, and they said it's outside the realm of the Homeland Security's guidelines (for what is needed). It was a little frustrating."

A person has about 100 identification marks on his or her fingerprints, and most adults have about 80 that can be used to identify them.

But because of his welding work, Strickler has only about 30 of the identification points.

Strickler is free to work at non-nuclear plants. But he says he prefers to have the option of working for the nuclear facilities.

"This cuts my income in half," he said.

Segmentation: Face Detection

*Theo Pavlidis, http://home.att.net/~t.pavlidis/comphumans/comphuman.htm

“State-of-the-art” Error Rates

	Test	Test Parameter	False Reject Rate	False Accept Rate
Fingerprint	FVC [2004]	20 years (average age)	2%	2%
Face	FRVT [2002]	Varied lighting, outdoor/indoor	10%	1%
Voice	NIST [2000]	Text Independent	10-20%	2-5%

At NY airports, an average of ~ 200,000 passengers pass through daily. If all of these used biometric-authenticated smart cards for identification, there would be 4000 falsely rejected (and inconvenienced) passengers per day for fingerprints, 20,000 for face and 30,000 for voice. Similar numbers can be computed for false accepts

FVC 2004 Results

Algoritm	EER (%)	Avg Enroll Time (sec)	Avg Match Time (sec)	Avg Model Size (KB)
Bioscrypt Inc.	2.07	0.08	1.48	24
Sonda Ltd	2.10	2.07	2.07	1.3
Chinese Academy of Sciences	2.30	0.35	0.67	16.4
Gevarius	2.45	0.69	0.71	2.0
Jan Lunter	2.90	1.01	1.19	3.1

- Database:
  - DB1: optical sensor "V300" by CrossMatch
  - DB2: optical sensor "U.are.U 4000" by Digital Persona
  - DB3: thermal sweeping sensor "FingerChip FCD4B14CB" by Atmel
  - DB4: synthetic fingerprints

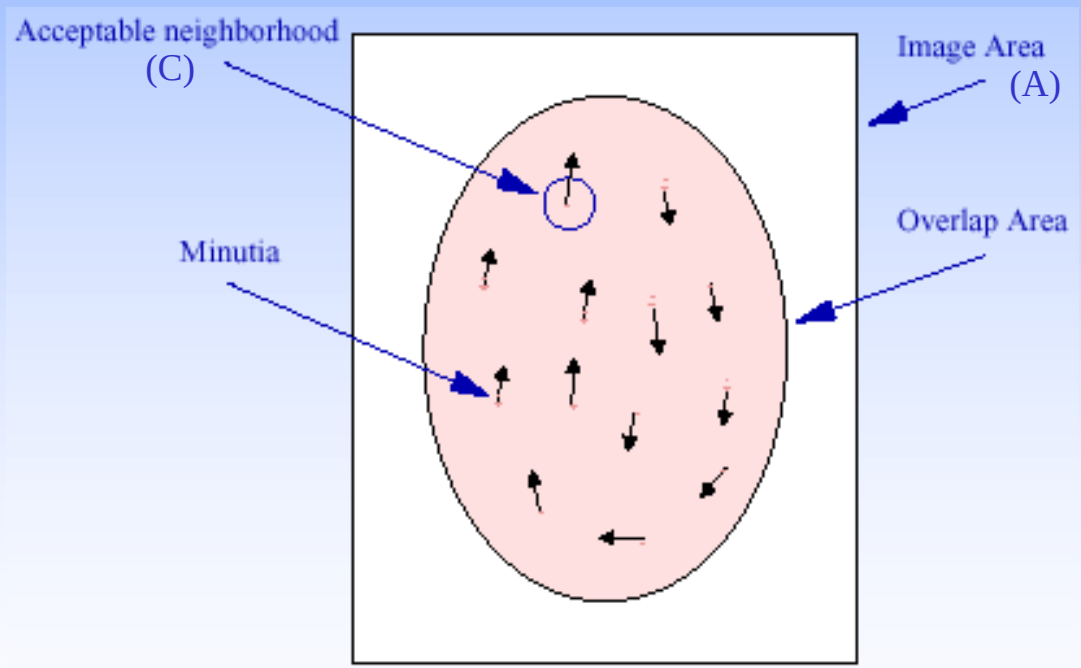
Typical Intrinsic Matcher (1:1) Performance Requirements

Functionality	FNMR %	FMR %
Authentication	0.1	0.1
Large Scale Identification	10.0	0.0001
Screening	1.0	0.0001

It is assumed that large-scale identification consists of 1 million identities and screening involves 500 identities. FTA and FTE are assumed to be zero. These numbers are based on what the authors believe to be the order of magnitude estimate of the performance needed for viability of a typical application.

Individuality of Fingerprints

- Given an input fingerprint with *n* minutiae, compute the probability that it will share *q* minutiae with any other template fingerprint containing *m* minutiae, p(M, m, n, q). The corresponding minutiae should “match” in location and orientation.



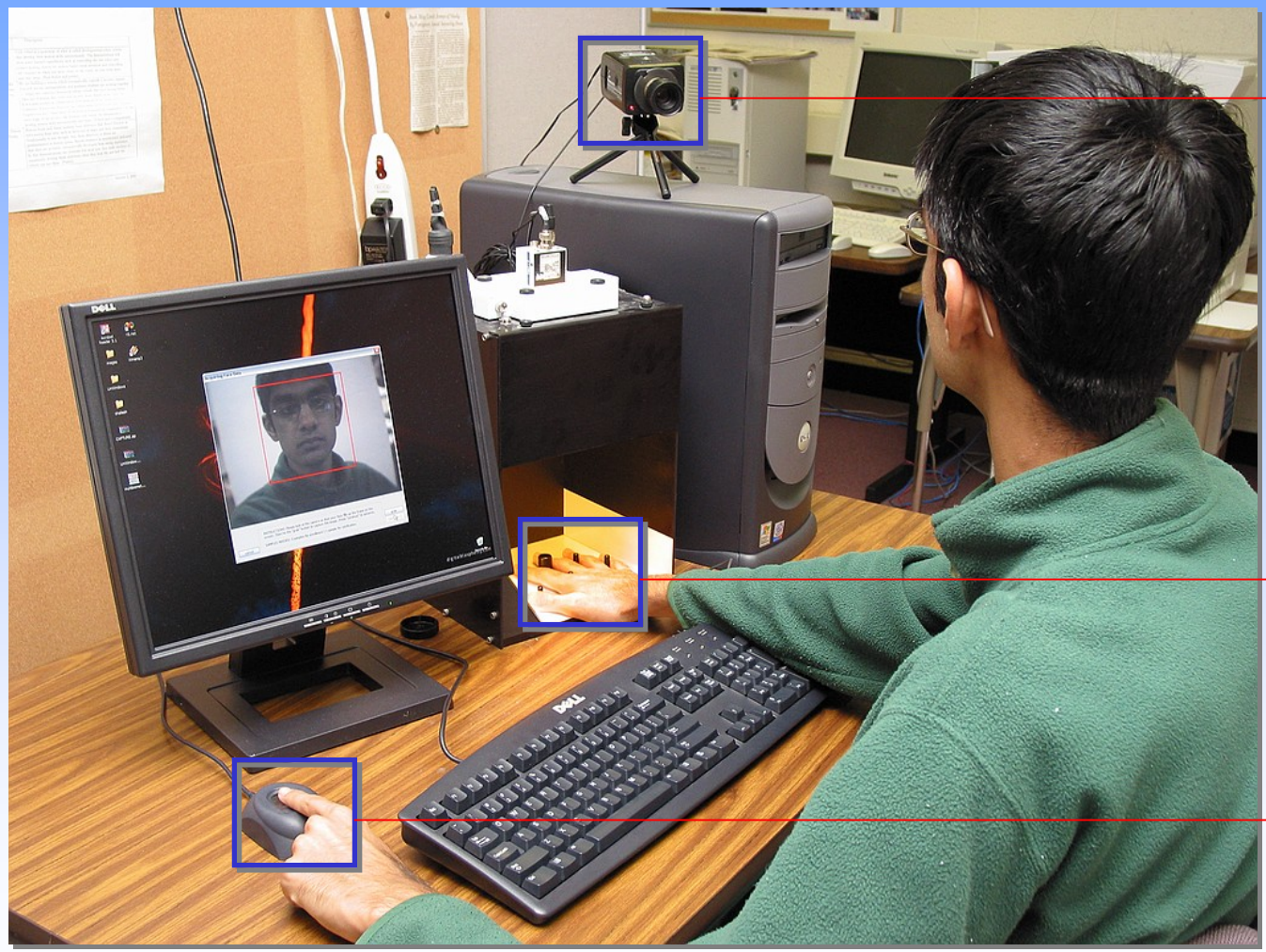
(a) M=52
m=n=q=26
$P = 2.40 \times 10^{-30}$

(b) M=52
m=n=26, q=10
$P = 5.49 \times 10^{-4}$

*Pankanti, Prabhakar, Jain, "On the Individuality of Fingerprints", IEEE Transactions on PAMI, Vol. 24, No. 8, pp. 1010-1025, 2002.

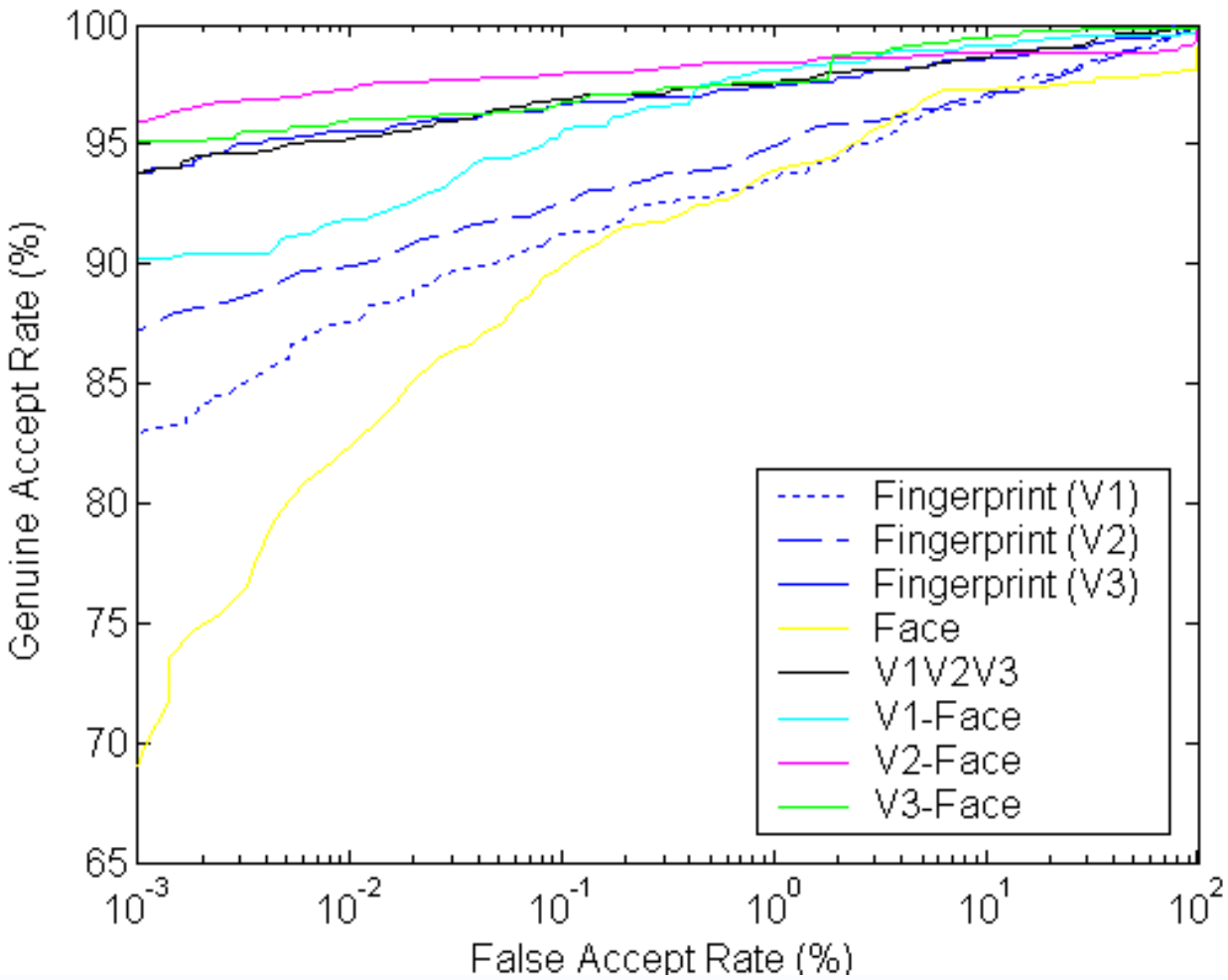
Multibiometrics

Limited discrimination and non-universality of a biometric



Helps improve accuracy and population coverage

Fusing Face & Fingerprint Systems

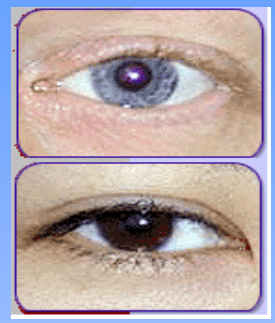


- Min-Max Normalization of matching scores
- Sum Rule
- 1000 Subjects
- EER is reduced from ~3% for the best individual matcher to <1% for multimodal system

Soft Biometrics

Gender, Skin Color, Hair color

http://anthro.palomar.edu/adapt/adapt_4.htm
© Corel Corporation, Ottawa, Canada



Eye color

http://ology.amnh.org/genetics/longdefinition/index3.html
© American Museum of Natural History, 2001

Weight

http://www.laurel-and-hardy.com/goodies/home6.html © CCA

Height

http://www.altonweb.com/history/wadlow/p2.html
© Alton Museum of History and Art

Identification at a Distance

Height: 5.9 ft.

Eye color: black

Gender: Male

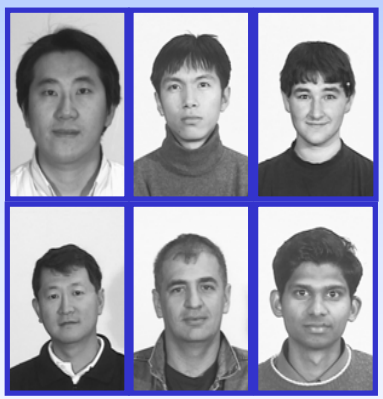
Ethnicity: Asian

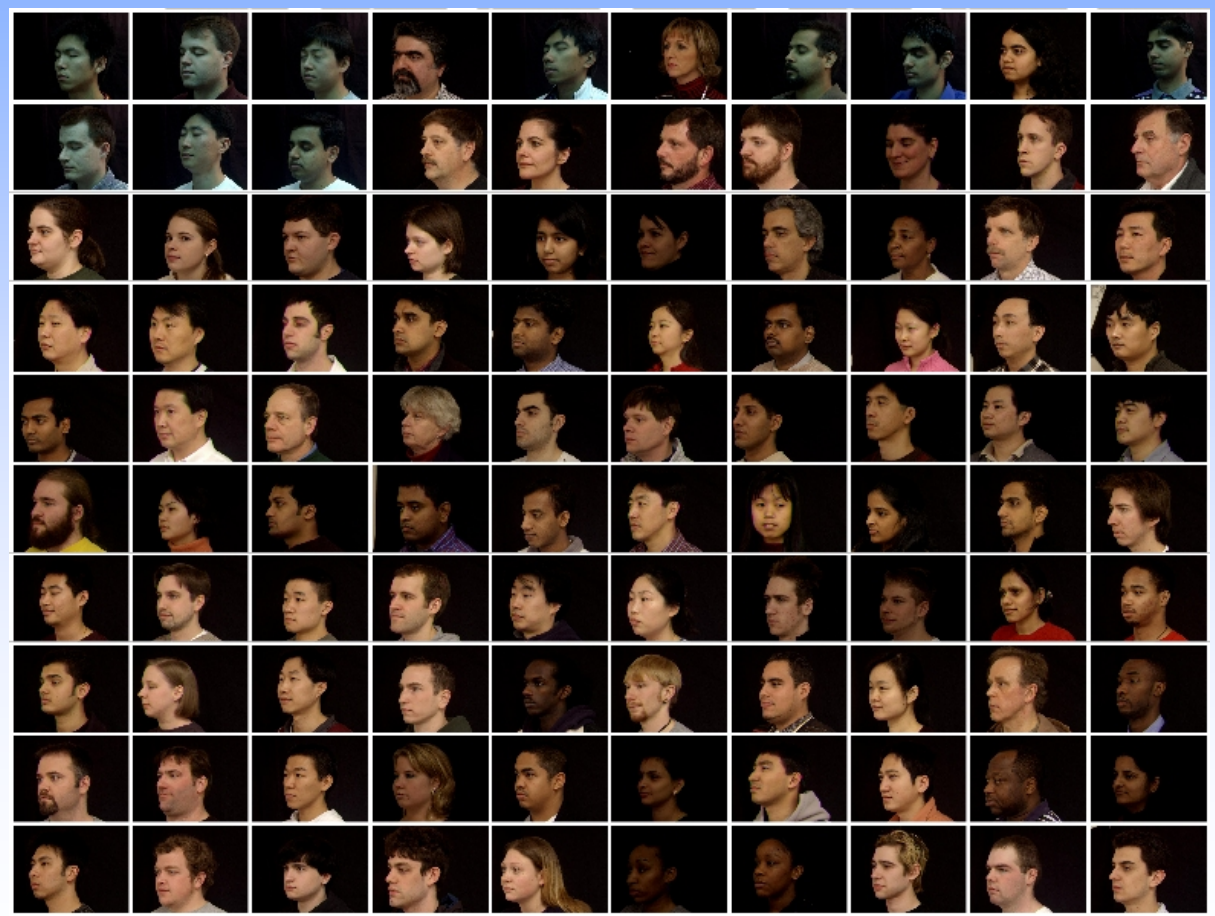
Face: LDA Coefficients

Identity: Unsang

Scalability of Biometric Systems

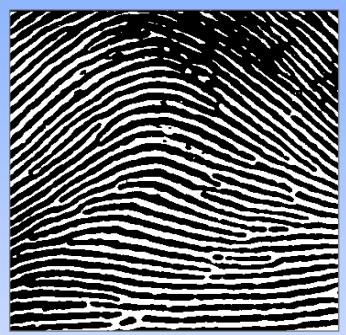
- How does the number of identities in the database affect the speed and accuracy of the system?
- Few published studies on reliable indexing of biometric patterns





Fingerprint Classification

- Assign fingerprints into one of pre-specified types (coarse classification for indexing);
- Best 4-class performance is only ~95%


Plain Arch


Tented Arch


Right Loop


Left Loop


Accidental

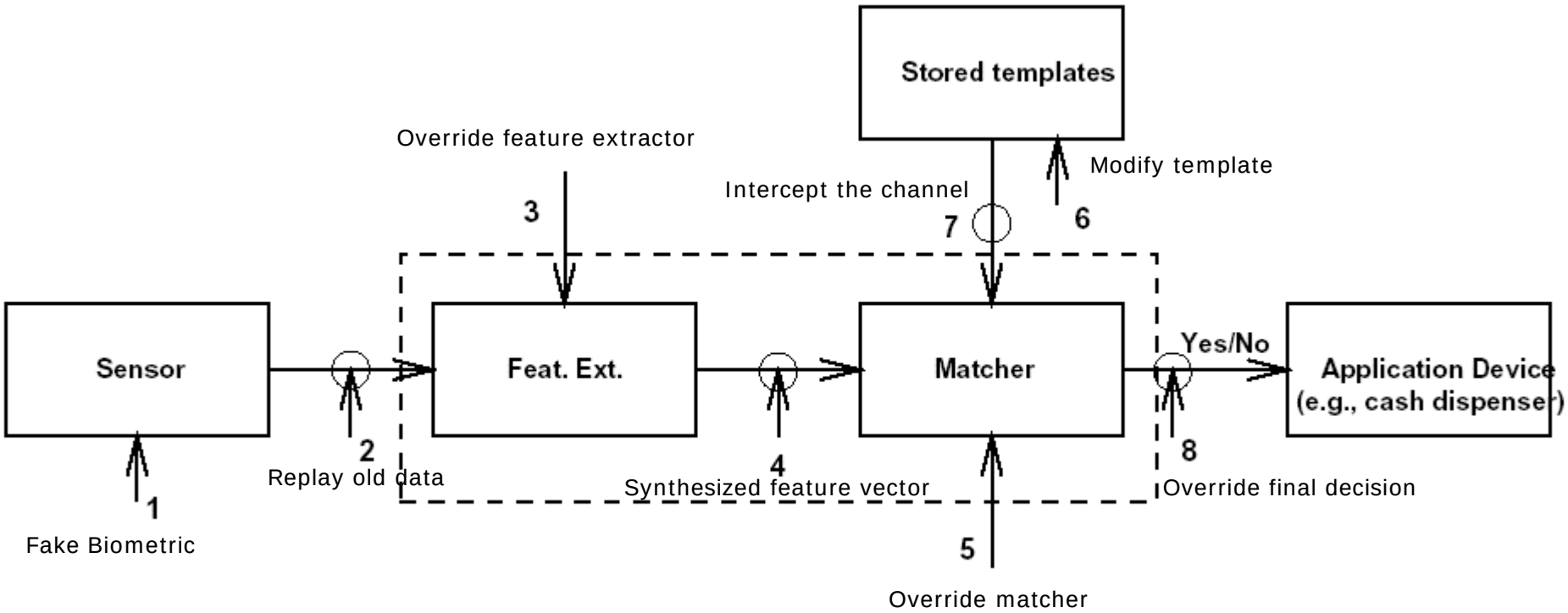

Pocket Whorl


Plain Whorl


Double Loop

Vulnerability of a Biometric System

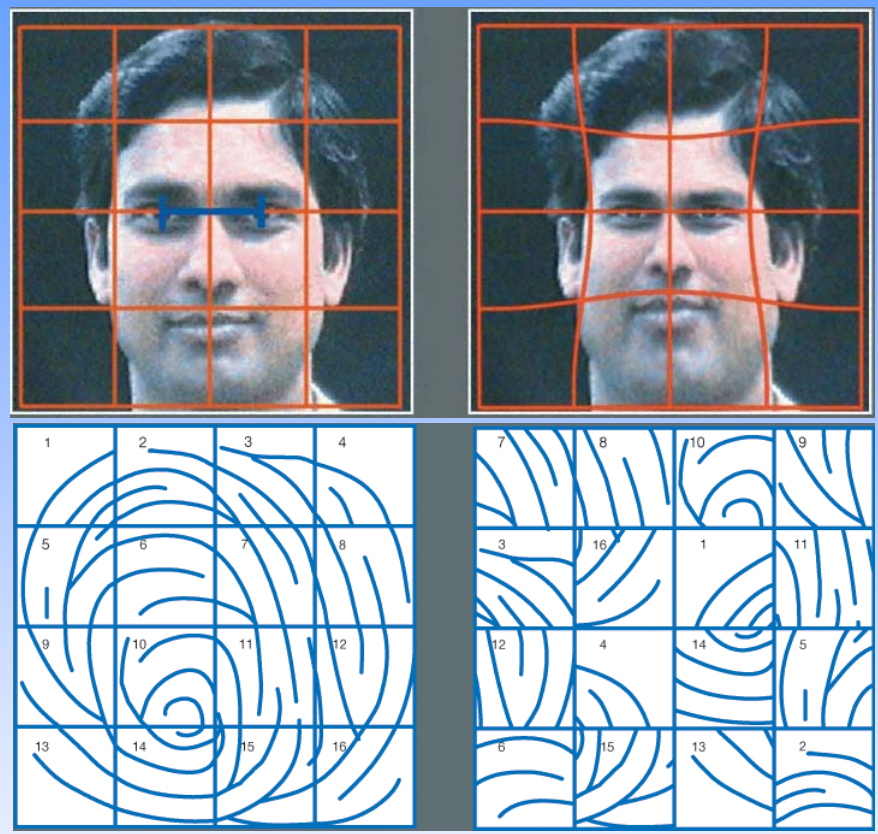
Like *any* system, biometric systems can be attacked in different ways



Liveness detection

Ratha et al., An Analysis of Minutiae Strength, AVBPA 2001

Template Protection



© *Ratha, Connell, Bolle (IBM)*

- Encrypting or watermarking templates in the database
- Storing only a transformed and unrecoverable version of a user's template to protect the original template
- Cancelable biometric

Jain,Uludag, Hsu, "Hiding a Face in a Fingerprint Image", Proc. of ICPR, Aug., 2002
Ratha, Connell, Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, vol. 40, no. 3, 2001, pp. 614-634.

Biometric Enabled Smart Card

- Template resides in the personal smart card of a user
- Verification takes place via a built-in chip on the card
- Template does not leave the card; no centralized biometric database is required

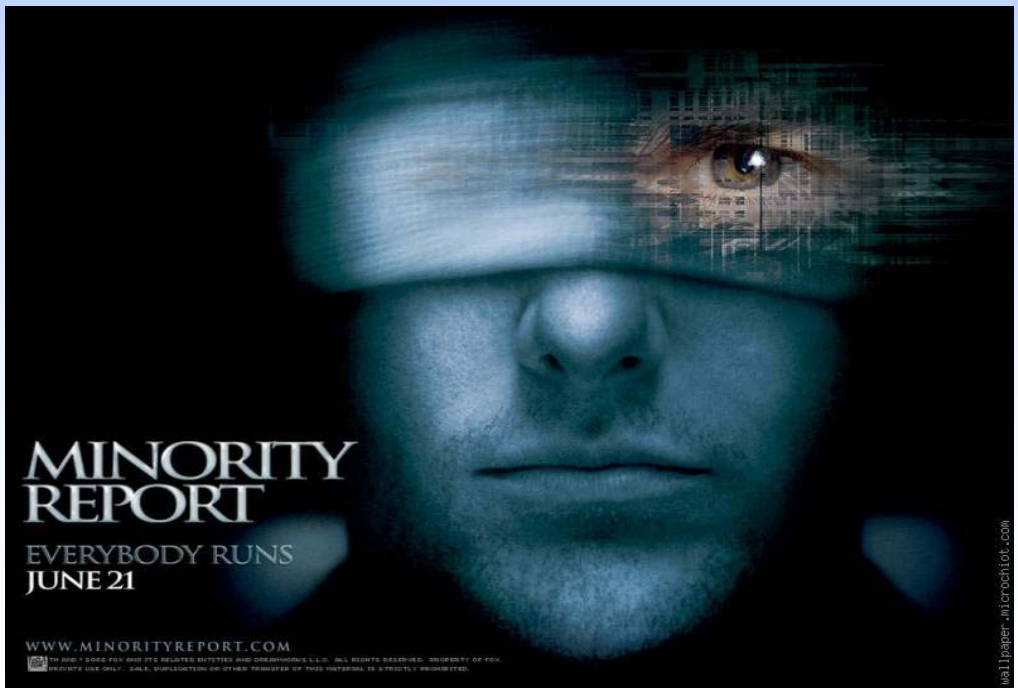
Siemens Matcher on Card Version 1.1

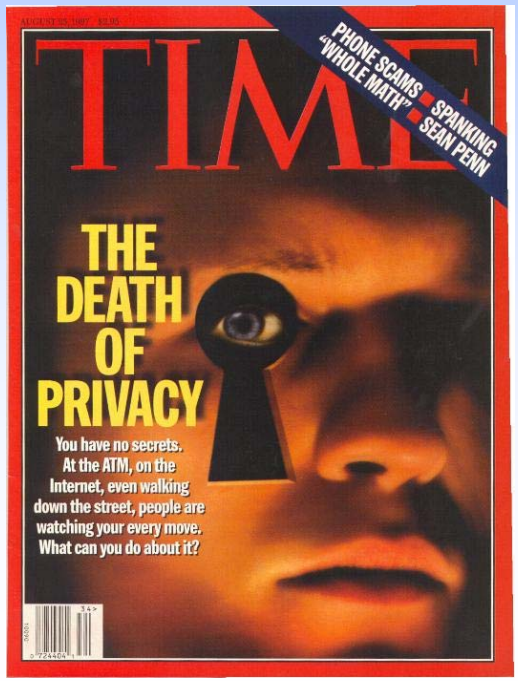
Precise Biometrics

5th Sense from Veridicom

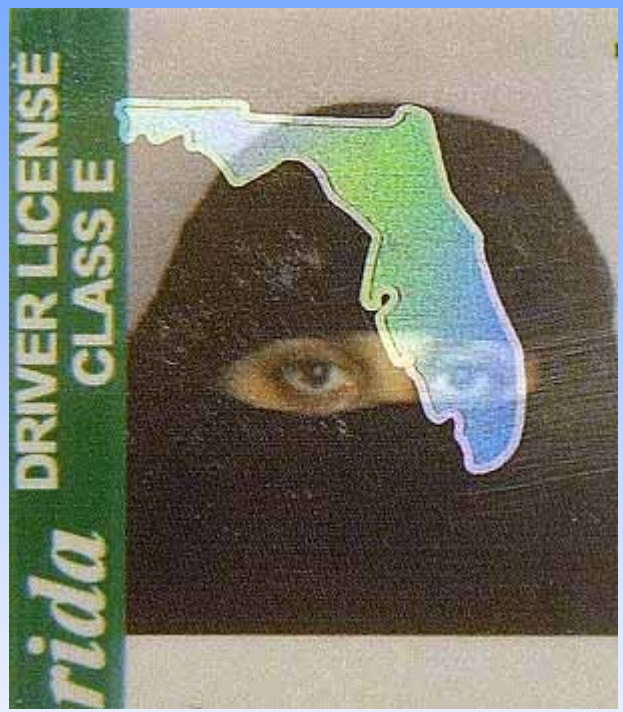
Privacy Concerns

- Biometric can help in protecting individual privacy; because biometrics provides stronger identification than password, it can be used to guard personal & sensitive information (Health Information Privacy Protection Act)
- Will biometric data be used to track people (secretly) violating their right to privacy?
- Functionality creep: Will biometric data be used only for their intended purpose? Will various biometric databases be “linked”?





Religious/Cultural Objections



© Orlando Sentinel

This is no different than acceptance of some other technologies

Summary

- Reliable and automatic person identification is becoming a necessity; emerging applications include national ID card, border crossing, access control Internet shopping, and computer data security
- There is no substitute to biometrics for effective person identification; it is becoming a necessary component of any ID management system
- Biometric sensors are cheap; fingerprint, face and voice sensors are available in laptops & mobile phones
- But, biometric system performance is not meeting the expectations

Summary

- Research is needed in (i) new representations, (ii) matching algorithms, (iii) database indexing, (iv) fusion of biometric modalities, (v) liveness detection, (vi) template protection, (vi) error rate estimation
- Need more system testing and evaluation on large standardized databases
- Biometrics has great potential to improve our privacy, but government regulations are needed
- No security system, including biometric system, is foolproof
- Need cost/benefit analysis for the deployment of biometric systems; quantifying deterrence has proved extremely difficult

Future Directions

- User Adaptation
  - Observing how the user interacts with the biometric device (e.g., user approaching a hand geometry device)
- Soft Biometrics
  - Utilize soft biometric traits like color of eye, color of hair, gender to reinforce identity
- Tracking
  - Monitor user behavior over an entire session (e.g., not just at login time) in order to validate identity

Verichip

(AP Photo/Applied Digital Solutions)

Applied Digital Solutions new "Verichip" about the size of a grain of rice, is the first-ever computer ID chip, that could be embedded beneath a persons skin.

Yahoo! News 27 Feb '02