Multimodal User Interfaces: Who's the User?

Anil K. Jain

Dept. of Computer Science and Engineering

Michigan State University

http://biometrics.cse.msu.edu

Outline

- Biometric recognition
- Applications
- Biometric characteristics
- Difficult pattern recognition problem
- Fingerprint matching
- Multimodal biometrics
- Summary

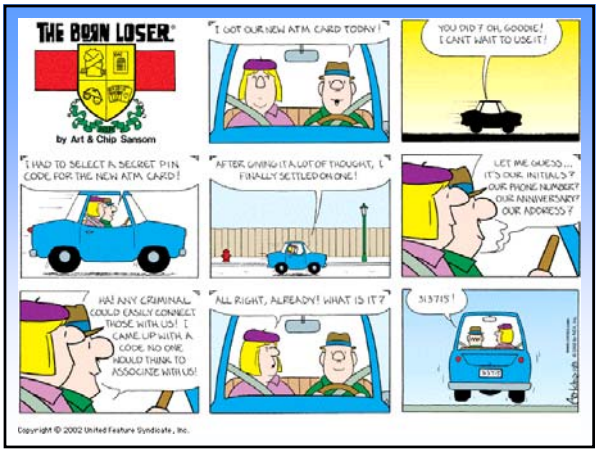
Questions on Identity

- Is this the person who he or she claims to be?
- Has this applicant been here before?
- Should this individual be given access to our system?
- Is this person on a watch list?

Traditional Identification Methods

1. Insert ATM card 2. Enter PIN

ATM does not know the difference between a genuine user, and an impostor who stole the card and guessed the PIN



Too Many Passwords!!

- 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)*
- A system help desk call to reset the password costs about $40

Fake Documents

- Identity fraud is the fastest growing crime in the United States; Federal Trade Commission Estimates:
  - 3.3 million identity thefts in U.S. in 2002
  - 6.7 million victims of credit card fraud
- Easy to obtain driver licenses based on false birth certificates, utility bills and other fraudulent documents
- Identity Fraud Cost:
  - Welfare disbursements: $1 billion
  - Credit card transactions: $1 billion
  - Cellular phone: $1 billion
  - ATM withdrawals: $ 3 billion

Biometric Recognition

iometrics: A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an enrollee

iometric recognition: Personal recognition based on "who you are or what you do" as opposed to "what you know" (password) or "what you have" (ID card)

Verification vs Identification

- Verification (1:1 match)
- Identification (1:Many match)
- Watchlist (1:Few match)

Advantages of Biometrics

- Positive Identification: Is this the person she claims to be? **Provide log-in access to a valid user**
- Negative Identification: Is this the person she denies to be? **Prevent issuing multiple driver licenses to the same person**
- Cannot be transferred, forgotten, lost or copied
- Eliminate repudiation claims
- Automatic personalization of user interfaces

Biometrics for Personalization

- Automatic personalization of vehicle settings:
  - Seat position
  - Steering wheel position
  - Mirror positions
  - Lighting
  - Radio station preferences
  - Climate control settings
- URLs at your fingertips

http://www.visteon.com

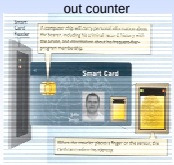
Biometric Applications

Iris-based ATM

Fingerprint at check-out counter

Disney World

Face scan at airports



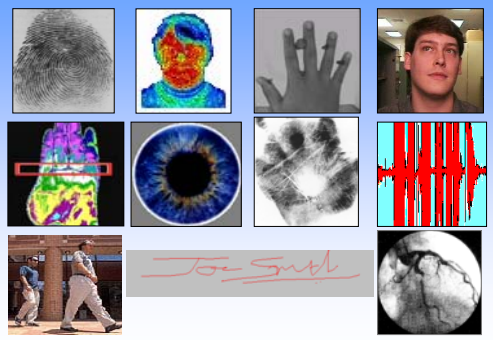
Smart card with fingerprints

Smart gun

Ben Gurion Airport

Saudi Arabia

Biometric Characteristics



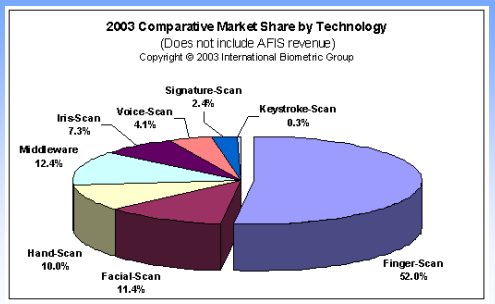
Verichip

(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

Biometric Market Share

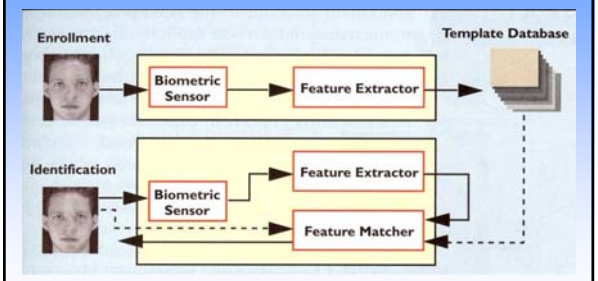


International Biometric Group

Which Biometric is the Best?

- **Universality** (everyone should have this trait)
- **Uniqueness** (different values for different persons)
- **Permanence** (should be invariant with time)
- **Collectability** (can be measured quantitatively)
- **Performance** (achievable recognition accuracy, resources required, operational/environment factors)
- **Acceptability** (are people willing to accept it?)
- **Circumvention** (how easy it is to fool the system)

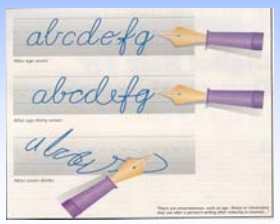
Biometrics as a Pattern Recognition System



Challenges in Biometric Recognition

- Large number of classes (~ 6 billion faces)
- Intra-class variability and inter-class similarity
- Segmentation
- Noisy and distorted images
- Population coverage & scalability
- System performance (error rate, speed, cost)
- Attacks on the biometric system
- Individuality of biometric characteristics

Large Intra-class Variability



Small Inter-class Variability

www.marykateandashley.com

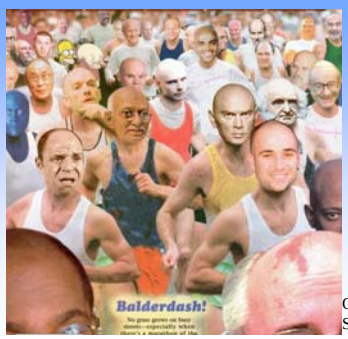
Twins

news.bbc.co.uk/hi/english/in_depth/americas/2000/us_elections

Father and son

Segmentation: Face Detection

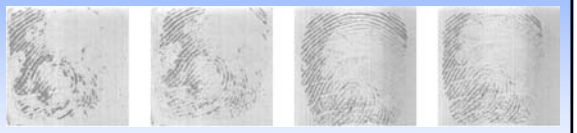
Picking Faces in a Crowd



Games Magazine
September 2001

Population coverage

- ~ 3% of the population has poor quality fingerprint images which means they have to be identified by some other means



Four impressions of a user's fingerprint

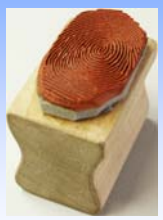
"State-of-the-art" Error Rates

	Test	Test Parameter	False Reject Rate	False Accept Rate
Fingerprint	FVC [2002]	20 years (average age)	0.2%	0.2%
Face	FRVT [2002]	Varied lighting, outdoor/indoor	10%	1%
Voice	NIST [2000]	Text Independent	10-20%	2-5%

At NY airports, an average of ~ 300,000 passengers pass through daily. If all of these used biometric-authenticated smart cards for identification, there would be 600 falsely rejected (and inconvenienced) passengers per day for fingerprints, 30,000 for face and 45,000 for voice. Similar numbers can be computed for false accepts

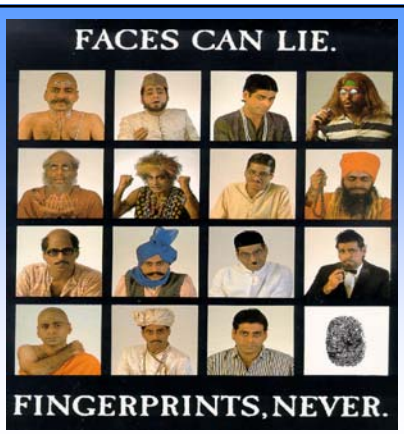
Attacks on Biometric Systems

- Commercial biometric systems cannot distinguish between real and artificial fingerprints (faces)



Dummy finger created from a lifted impression

Circumvention



Interest in Face Scanning

September 18, 2001
PluggedIn: Interest in face scanning grows after attacks
By Andy Sullivan
WASHINGTON, Sept 18, 2001 (Reuters)

After nine months of intense scrutiny by lawmakers and privacy hawks, makers of controversial facial-surveillance technology have found themselves struggling to meet commercial demand in the wake of last week's deadly attacks.

Executives say their systems could have saved lives had they been in place at airports, border crossings and other checkpoints last Tuesday.

Face Recognition Technology Fails to Flag "Suspects" at Airport

September 4, 2003

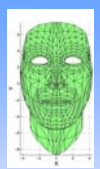
Camera Technology designed to spot potential terrorists by their facial characteristics at airports failed its first major test.

Last Year, two separate face recognition systems at Boston's Logan Airport failed 96 times to detect volunteers who played potential terrorists as they passed security checkpoints during a three-month test period. The system correctly detected them 153 times. The airport's report called the rate of inaccuracy "excessive". The report was completed in July 2002 but not made public. The ACLU obtained a copy last month through a Freedom of Information Act request.

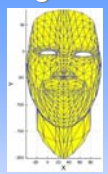
Logan is where 10 of the 19 terrorists boarded the flights that were later hijacked Sept. 11, 2001. The airport is now testing other security technology, including infrared cameras and eyeball scans.

http://www.usatoday.com/usatonline/20030902/5460651s.htm

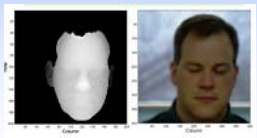
Model-based Face Recognition



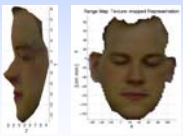
Generic Model



Face model of Pat Flynn



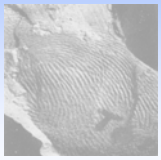
Facial Measurements



Rendered face image of Pat Flynn

Fingerprints

- Fingerprint-based identification has a 100-year history
- Different fingers have different ridge characteristics (minute details). **Identical twins have different fingerprints**
- Minute details are permanent
- Fingerprint identification is acceptable in courts



Fingerprint on Palestinian lamp (400 A.D.)

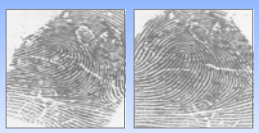
Bewick's trademark

Fingerprint Sensors

- Optical, capacitive, ultrasound, pressure, thermal, electric field

Fingerprint Matching

Find the similarity between two fingerprints

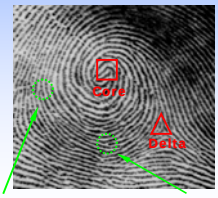


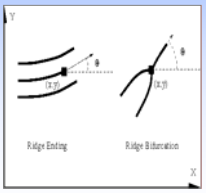
Two fingerprints from the same finger

Fingerprints from two different fingers

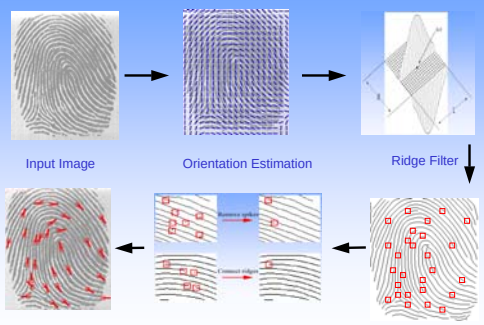
Fingerprint Representation

- Local ridge characteristics (minutiae): ridge ending and ridge bifurcation.
- Singular points: ridge orientation tendency not continuous.





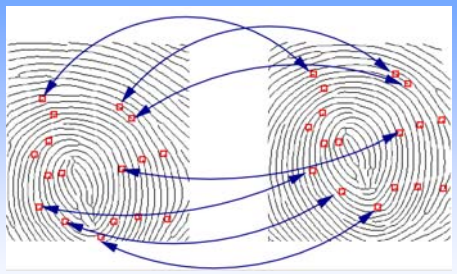
Minutiae Extraction



Fingerprint Deformation

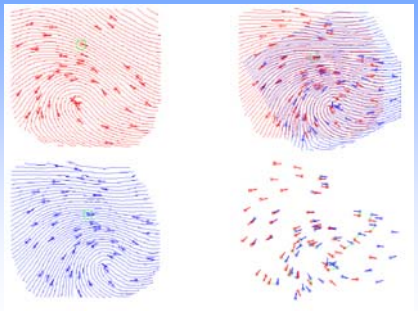
- Fingerprint imaging introduces non-linear deformations

Minutiae Correspondence



- Use elastic string matching to obtain minutiae correspondences

Minutiae Matching



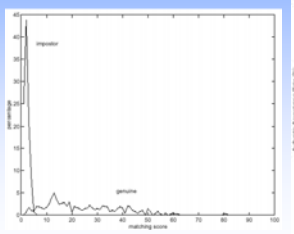
Matching Scores

(a) (b) (c)

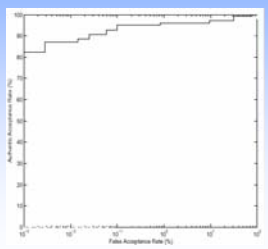
$S_{ab} = 97$; $S_{bc} = 5$; $S_{ac} = 2$

Matching Score Distributions

- NIST-9 database (1,350 mated fingerprints)

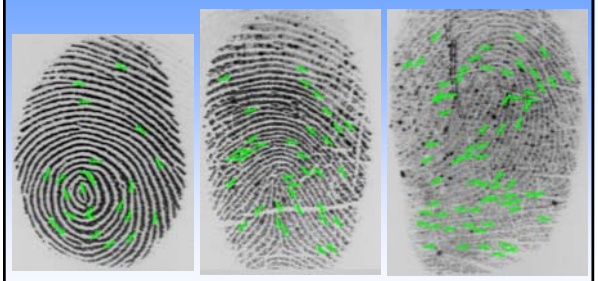


Matching Score Distribution



ROC Curve

Noisy Fingerprint Images

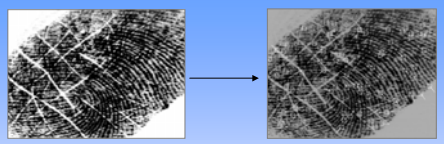


Quality Index = 0.96
False Minutiae=0

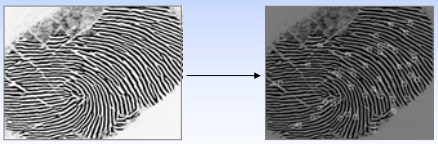
Quality Index = 0.53
False Minutiae=7

Quality Index = 0.04
False Minutiae=27

Fingerprint Enhancement

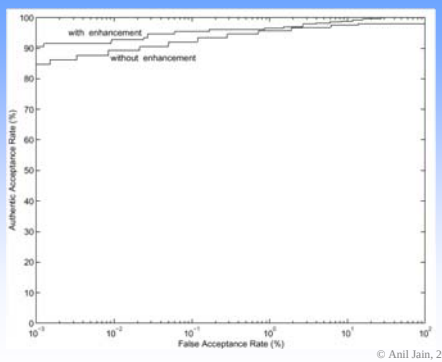


Minutiae extraction before enhancement



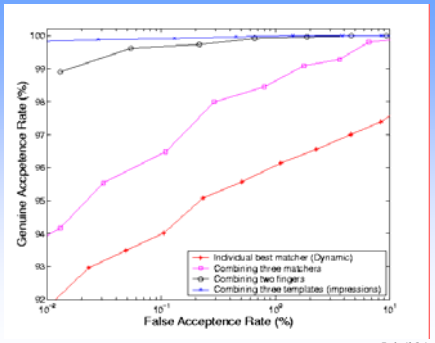
Minutiae extraction after enhancement

Performance with Enhancement



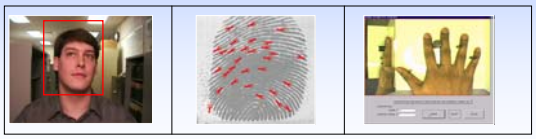
Multimodal Biometrics

Multiple Fingers, Matchers and Templates



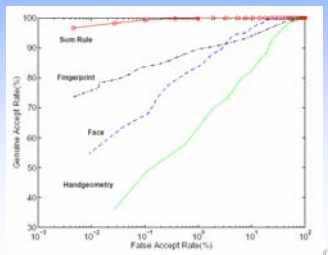
Using Multiple Biometrics

- Limitations of using a single biometric:
  - Failure to enroll rate (~3% for fingerprints)
  - Noise in sensed data (repeated use of sensor)
  - Lack of permanence (voice altered due to cold)
  - Limited discriminability (high FAR/FRR)
  - Easier to spoof (fake fingerprint)



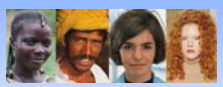
Fusion Methodology

- Variety of techniques to combine scores output by individual biometrics – KNN, decision trees, discriminant analysis,…
- Sum rule (weighted sum of individual scores) performs well

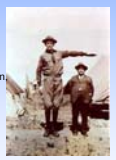


Soft Biometrics

Soft biometrics provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate them



Ethnicity, Skin Color, Hair color
(Sub-Saharan African, Indian, Southern European and Northwest European)
http://anthro.palomar.edu/adapt/adapt_4.htm
© Corel Corporation, Ottawa, Canada

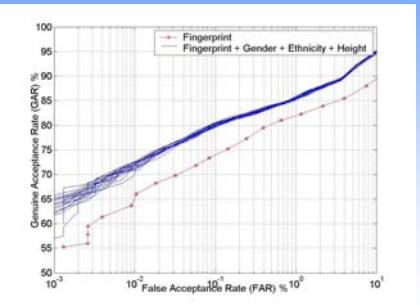


Height
http://www.altonweb.com/history/wadlow/p2.html
© Alton Museum of History and Art

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

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

Combining Fingerprints with Soft Biometrics



Template Protection

Summary

- Automatic authentication is becoming a necessity
- Fingerprint sensors can now be embedded in laptops, cellular phones and smart cards
- Performance claims by vendors are overly optimistic; too much hype is not good for this techno
- Popular misconception that biometric authentication is “solved”; need research in sensor design, signal and image processing and pattern recognition
- Biometric fusion will improve population "coverage" as well as performance
- Investigate uniqueness/individuality of biometrics
- Need to ensure user privacy and template security