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!!
“Sorry about the odor. I have all my passwords tattooed between my toes.”
- 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 Mentor 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

---

**Biometric Applications**

- Iris-based ATM
- Face scan at airports
- Fingerprint at checkout counter
- Smart card with fingerprints
- Disney World
- Smart gun
Verichip

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 person’s skin.

Yahoo! News 27 Feb ’02

© Anil Jain, 2003

Biometric Market Share

© Anil Jain, 2003

Biometrics as a Pattern Recognition System

© Anil Jain, 2003

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/environmental factors)
- **Acceptability** (are people willing to accept it?)
- **Circumvention** (how easy it is to fool the 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

Twins

Father and son

Segmentation: Face Detection

Picking Faces in a Crowd

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
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.
**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 Sensors**

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

**Fingerprint Matching**

Find the similarity between two fingerprints

**Fingerprint Representation**

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

**Minutiae Extraction**

- Input Image → Orientation Estimation → Ridge Filter → Minutiae Detection → Postprocessing
Fingerprint Deformation

- Fingerprint imaging introduces non-linear deformations

Minutiae Correspondence

- Use elastic string matching to obtain minutiae correspondences

Minutiae Matching

Matching Scores

(a) \( S_{ab} = 97; S_{bc} = 5; S_{ac} = 2 \)

Matching Score Distributions

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

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

© Anil Jain, 2003

Performance with Enhancement

© Anil Jain, 2003

Multimodal Biometrics

© Anil Jain, 2003

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)

© Anil Jain, 2003

Multiple Fingers, Matchers and Templates

© Anil Jain, 2003

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

© Anil Jain, 2003
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
- Eye color
- Height
- Weight

Ethnicity: Sub-Saharan African, Indian, Southern European, and Northwest European

http://www.laconest.com/history/evolution/2.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 technology
- 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