An Overview of Biometrics

Peter T. Higgins
Higgins & Associates, International
202-625-7780
HigginsAssoc@aol.com
Session One

♦ State-of-the Art
  - What are biometrics and how do they work
  - Fingerprint recognition
  - Face recognition
  - Voice recognition
  - Hand recognition
  - Iris recognition
Session Two

♦ Implementation Issues & Challenges
  ■ What biometrics are used for
  ■ Factors that influence the performance
  ■ What are some of the challenges
  ■ Applications for Homeland defense and INS
  ■ The role of biometric standards
What are Biometrics?

♦ Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic.

■ *Biometrics Consortium definition*
Key Terms

- **Identify**: Determine if the person is already enrolled in the system.
- **Verify**: Determine if identity claim is true.
- **Automated**: Machine identity decision based on score relative to threshold; **Authorization decision** is **Red** or **Green** based on security, access requirements, and identity.
Key Terms

♦ Best reference for terms:
  - Best Practices in Testing and Reporting Performance of Biometric Devices
What Characteristics?

◆ Physiological:
  - Eye
  - Face
  - Fingerprint
  - Hand

◆ Behavioral:
  - Gait
  - Keystrokes
  - Signature
  - Voice
  - Both

• The Challenge: Biometric samples are never exactly the same as last time they were acquired.
Statistical Underpinnings

♦ Measure differences in samples collected
  ■ Score distribution across a large sample is bi-modal.
  ■ Threshold of closeness is set-dependent based on multiple variables:
    ▷ Technology
    ▷ Purpose of system
    ▷ Degree of cooperation
    ▷ Amount of supervision
    ▷ Target population
Score Distribution
Typical Process Flow

♦ Enrollment
  ■ Voluntary or involuntary
  ■ Token extracted and stored

♦ Subsequent Use
  ■ Supervised or unsupervised
  ■ Cooperative or non-cooperative
  ■ In-use token compared to enrollment token
    ♦ Statistical threshold determines match or not
Performance Characteristics

♦ Threshold driven
  ■ Fixed setting or dynamic setting
  ■ Trade-off between false rejects and false accepts

♦ Metrics used
  ■ Failure to Enroll and Failure to Acquire Rates
  ■ False Reject Rate = False Non-Match Rate
  ■ False Accept Rate = False Match Rate
For each biometric:
- History
- Technology
- Status
- Performance
- Applications
- Sample tokens

Biometrics:
- Fingerprint
- Face
- Voice
- Hand
- Eye
Fingerprints - History

♦ Automation started in 1970s
  - FBI funded R&D
  - RCMP installed first system
♦ 1970s computer performance influenced design
  - Special purpose comparison boards
  - Searches limited to *binned* records
  - Inked cards imaged at central site
Fingerprints - History

♦ Civil applications successfully started in late 1980s
  ♦ Welfare fraud reduction

♦ Early 1990s - 2 key National Programs
  ♦ US & UK
  ♦ Federal R&D investments
  ♦ Update of standards

♦ Desktop applications - late 1990s
Fingerprints - History

♦ Technology and cost breakthroughs in late 1990s
  ■ Single finger scanners
    ◦ Optical, ultrasonic, thermal imaging, capacitive
  ■ Fast PCs
    ◦ Single finger algorithms
    ◦ Smaller repositories
  ■ Permitted broader target audience
    ◦ Replace passwords
    ◦ Support digital signatures, etc
Fingerprints - Technology

- Large Scale AFIS
  - Law enforcement
  - Civil applications
  - Handful of players

- Tactical AFIS
  - Access control
  - Identity verification
  - Hundreds of *players*
Fingerprints - Technology

♦ Capture
  ■ Standards driven
  ■ Quality key to successful comparison
  ■ Flat or rolled impressions
Fingerprints - Technology

♦ Feature extraction
  ■ Minutiae based
  ■ 20 to 100 minutiae per image
  ■ Many attributes per minutiae point
    ♦ X, Y, Theta, type, neighbors, quality, etc.
  ■ 150 to 1,000 bytes per finger
Fingerprints - Technology

- Comparison
  - Drop out areas
  - Rotation
  - Ridge crossings
  - Pattern type
  - Templates stored in memory and compared rapidly
Fingerprints - Technology

♦ Scoring
  ■ Ranked / Dynamic or static threshold

♦ Single finger scanners
  ■ Solid state or optical
  ■ $20 to $33 US per chip set - $60 to $200 US for product with s/w
  ■ 3.3 to 5 v
  ■ Surface mounted, on a mouse, or stand alone
Cost of Securing a Computer with Biometrics

Chart Courtesy of Paul Collier
Fingerprints - Status

♦ Most accurate for large scale identification
♦ Well defined standards
♦ Ten print systems are almost perfect
♦ Many competing algorithms and scanners for desktops
  ■ Minutiae and Correlation based algorithms
Fingerprints - Performance

♦ Single finger systems, best of 3 tries

<table>
<thead>
<tr>
<th>FAR</th>
<th>FRR</th>
<th>Solid State</th>
<th>Optical</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤0.1%</td>
<td>≤2%</td>
<td>≤10%</td>
<td></td>
</tr>
</tbody>
</table>

AFIS Vendors report results that are quite opposite. Algorithm maturity issue?
Fingerprints - Vulnerabilities

♦ Biometrics are susceptible to attack
♦ Two papers on vulnerabilities of fingerprint systems in open literature
  ■ Biometric Fingerprint Recognition – Don’t Get Your Fingers Burned
    ♦ September 2000: Van der Putte an Keuning
  ■ Impact of Artificial “Gummy” Fingers on Fingerprint Systems
    ♦ January 2002: Matsumoto et al
Devices in *Burned Fingers* paper

- Identix TS-250
- Fingermatrix Checkone
- Dermalog DermalogKey
- STMicroelectronics TouchChip
- Veridicon FPS110
- Identicator DFR200

All but one was fooled on first attempt – Fingermatrix took two attempts
Fingerprints - Vulnerabilities

- Devices in *Gummy Fingers* paper:
  - Compaq DRF-200
  - Mitsubishi FPR-DT mkII
  - NEC N7950-41
  - Omron FPS-1000
  - Sony FIU-002-F11
  - Fujitsu FS-200U

- NEC PK-FP02
- Siemens Eval Kit
- Sony FIU 710
- SecuGen SMB-800
- Ethentica MS 3000

Artificial fingerprint enrolment test with live finger verification – the best system was still fooled 65% of the time
Fingerprints - Applications

♦ Low cost verification solutions available to secure PCs
  ■ Networks with 1,000 + users have migrated to fingerprints
  ■ Dramatic help desk savings possible
Fingerprints - Sample Token
Faces - History

♦ 1888 Galton proposed facial comparison
♦ Late 1980s - semi automated
  ■ Ratio based technique
    ♦ Permitted matching independent of image scale
    ♦ Required manual registration of key points
  ■ Based on work in Stanford U. Dissertation
  ■ Intelligence Community funded implementation
♦ DARPA Research in mid 1990s led to commercial products by 1997
Approach
- Image capture (still vs. video)
- Segmentation
- Feature identification & encoding
  - Eigenfaces the core technical underpinning
  - 128 face basis vectors - algorithm computes scalar values in 128 dimension space
- Comparison
  - Sparsely populated 128 dimension space search
Very sensitive to light conditions, orientation, facial expressions, noise in the image, glasses, hair changes, etc.
Verification and surveillance use

Only biometric that *a non-specialist can try to confirm*

Face in the crowd problem being addressed for overt & covert use

DOD competitions and funding of academicians help drive performance
# Faces - Performance

<table>
<thead>
<tr>
<th>Conditions</th>
<th>FAR</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same day, same illumination</td>
<td>2%</td>
<td>0.4%</td>
</tr>
<tr>
<td>Same day, different illumination</td>
<td>2%</td>
<td>9%</td>
</tr>
<tr>
<td>Difference days</td>
<td>2%</td>
<td>11%</td>
</tr>
<tr>
<td>1.5 years later</td>
<td>2%</td>
<td>43%</td>
</tr>
</tbody>
</table>

NIST Facial Competition run this Summer - initial results to be available in October.
Faces - sample data flow

Detection & Alignment

Recognition & Coding
Voice - History

- Technology is called Speaker Verification or Voice ID
  - Speech recognition technology spin-off
- DOD funding helped drive industry
  - NSA R&D area
  - University and corporate R&D labs
- Late 1980s first companies
  - By 1995 20+ companies including VARs
Voice - Technology

♦ Capture using existing devices
  ■ PC microphone or telephone

♦ Sample ambient noise
  ■ Calibrate capture device

♦ Prompt user
  ■ Predefined utterance or random utterance

♦ Very sensitive to speaker’s stress level and health, length of time since enrolment, time of day, background and electronics noises
Voice - Technology

♦ Extract features
  - Statistical noise reduction
  - Need to balance acoustic parameters:
    ♦ Behavioral patterns
    ♦ Physiology features

♦ Save tokens (one of these ways):
  - Templates
  - Hidden Markov models
  - Neural networks
Voice - Technology

♦ Templates
  ■ Direct acoustic representation of the sound patterns for a known text string

♦ Hidden Markov models
  ■ Statistical information about sound patterns and their statistical variability
  ■ Can support random text strings
  ■ Typically require more sample utterance collection

♦ Neural networks
  ■ Pattern matching
Voice - ID Decisions

♦ Fixed and Dynamic thresholds
  - Random prompted utterances permit more flexibility in scoring
  - Adjustable for high-use enrollees

♦ Cohort Models
  - Can be used in Template and Hidden Markov models
  - At enrollment all *similar* speakers are flagged
  - At verification - compare sample to whole cohort
Voice - Status

♦ In commercial production systems
  ■ Optional log-on feature in Mac OS9
  ■ Home Shopping Network
  ■ Both dropped the technology

♦ Interoperability standards for templates established.
## Voice - Performance

<table>
<thead>
<tr>
<th>Conditions</th>
<th>FAR</th>
<th>FRR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Same # and handset</td>
<td>1%</td>
<td>7%</td>
</tr>
<tr>
<td>Different #, same handset</td>
<td>1%</td>
<td>21%</td>
</tr>
<tr>
<td>Different # and handset</td>
<td>1%</td>
<td>63%</td>
</tr>
</tbody>
</table>
Hands - History

♦ Automation started in late 1980s
  ■ Various competitors introduced:
    ◦ Two finger devices
    ◦ Vein checking
    ◦ Heat sensing

♦ Verification-only devices
Hand - Technology

♦ Two camera system
  ■ Pins guide hand placement
  ■ Images top view and side view
♦ Features extracted
  ■ Finger length, width and features
  ■ Hand thickness profile
♦ Smallest biometric template - 9 to 14 bytes
Hand - Status

- Mass production
- Easy to use
- Single company dominates industry
- Low reject rate at time of use
- Two finger version in use at Disney
Hands - Status

♦ Recognition Systems Unit for time and Attendance
  ■ ~$1,500 US
  ■ Just uses 4 fingers but requires placement of whole hand

♦ Biomet Partners
  ■ ~$400 US for standalone unit

♦ System used for trusted travelers in many countries
Hand - Performance

Error Rates ≤0.5%
Eyes – History

- **Retina**: Back of eye imaging
  - 20 years or more (Paper in 1929)
  - High collection error rate
  - Possible medical - privacy issues
  - New product announcements - little market penetration
Eyes – History

♦ Iris: Eye surface imaging

■ Mid 1990s
  - Sarnoff - NSA - Sensar
    - Patents
  - IriScan - Medical & Dr. Daugman
    - Patents
    - Defense Nuclear Agency
  - Iridian - merger in late 2000
IRIS – Technology

- Near IR cameras to find & capture eye
- Segment eye constituents
  - Sclera, Iris and Pupil
- Perform 192 radial measurements
- Map iris into 256 sectors
- Run 2 transforms on each sector
- Generate and store 256 byte string
IRIS – Technology (Continued)

♦ Can perform identification as well as verification
♦ Very low error rates
♦ Very fast search times
  - Tokens (bit strings) held in RAM
  - Exclusive OR instruction
  - 30% match threshold (Hamming Distance)
♦ Sensitive to certain contact lens styles and possibly eye color
Eyes – Iridian Product

♦ Desktop unit for verification and conference calls
  ■ IR light source in unit
  ■ Two cameras
    ✦ Face acquisition
    ✦ Eye imaging
  ■ Smart card reader for identity claim

♦ Access control unit for doors
IRIS – Status

♦ Cost and unit size decreasing
♦ Very accurate but no large scale use
IRIS – Performance

- No reported false matches
- Few Failure to Match events
- Vulnerabilities
  - Spoof under unsupervised use
  - Mask with special contact lens
Eyes - Sample Token
Questions?
Contact Information

Peter T. Higgins
Higgins & Associates, International
Washington, DC
202-625-7780 (voice)
202-625-7781 (fax)
HigginsAssoc@aol.com (business)
PeterTHiggins@aol.com (personal)