Biometrics

- Introduction
- Face recognition
- Iris recognition
- Hand-based biometrics (palmprint)
- Mobile biometrics
Identity questions

How can I know who you are?
We now live in a global society of increasingly desperate and dangerous **people who cannot be trusted based on identification documents**

- Is Mary authorized to enter the secure facility?
- Can Steve access the secure website?
- Is Cathy the owner of the bank account?
- Should John be granted a visa?
- Does Alice already have a passport?
- Has Robert already voted?
- Does Charlie have a criminal record?
people took greater care of their mobile phones and iPods despite passports being worth thousands of pounds to criminals and identity fraudsters. Other research also found that only 7% of people keep their passports in a safe place when at home and 61% fail to fill in the emergency contacts section at the back of the passport.

In 2006, 290,996 British passports were reported lost or stolen. While many people safeguard their wallet and personal valuables abroad, their passport is not always such a priority. Last year IPS research showed that 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.

Source: press.homeoffice.gov.uk
Identity questions

Identity thieves steal customer ID & password to create financial nightmare for customers

Identity theft surveys and studies:
How many identity theft victims are there? What is the impact on victims? https://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007
Authentication methods

- **Something the user *knows* (PIN, password)**
  
  Poor use widely documented; most common passwords: password, 123456, abc123, letmein, monkey, myspace1

- **Something the user *has* (token)**
  
  User tends to leave token in device for convenience

- **Something the user *is* (biometric)**
# Authentication methods

## Comparison of Authentication Protocols

<table>
<thead>
<tr>
<th>Method</th>
<th>Examples</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>What you have</td>
<td>User IDs, accounts, cards, badges, keys</td>
<td>Can be shared, can be duplicated,</td>
</tr>
<tr>
<td>(P)</td>
<td></td>
<td>can be lost/stolen</td>
</tr>
<tr>
<td>What you know</td>
<td>Password, PIN, Personal knowledge</td>
<td>Can be shared, can be forgotten,</td>
</tr>
<tr>
<td>(K)</td>
<td></td>
<td>can be guessed</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Fingerprint, Face, Iris ..</td>
<td>Cannot be shared, non-repudiable,</td>
</tr>
<tr>
<td>(B)</td>
<td></td>
<td>cannot be lost</td>
</tr>
</tbody>
</table>
Bertillon system: Measurements of certain bony portions of the body (skull width, foot length, cubit, trunk, left middle finger, etc.) along with hair colors, eye color, and front and side view photographs.
Biometric (pattern recognition) systems

**Biometrics:** Study of techniques for using *physical or behavioral features* of a person or animal to verify or determine identity.

**Warning:** The term biometrics also has an older meaning – the statistical study of biological phenomena. The journal *Biometrics* published by the International Biometrics Society has nothing to do with biometrics as we use the term.
Characteristics of good biometric features:

- **Universality** (everyone should have this trait)
- **Uniqueness** (everyone has a different value)
- **Permanence** (should be invariant with time)
- **Collectability** (can be measured quantitatively)
- **Performance** (achievable recognition accuracy, resources required, operating environment)
- **Acceptability** (are people willing to accept it?)
- **Circumvention** (how easily can it be spoofed?)
Biometric (pattern recognition) systems

**Head**
- face
- iris
- ear

**Hand**
- fingerprint
- hand geometry
- palmprint
- finger-knuckle
- vein

**Behavior**
- signature (2D/3D)
- keystrokes
- gait
- speech
### Biometric (pattern recognition) systems

<table>
<thead>
<tr>
<th></th>
<th>Finger Scan</th>
<th>Facial Scan</th>
<th>Hand Scan</th>
<th>Iris Scan</th>
<th>Voice Recognition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accuracy</strong></td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>Very High</td>
<td>Low to Medium</td>
</tr>
<tr>
<td><strong>Ease of Use</strong></td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Low to Medium</td>
<td>High</td>
</tr>
<tr>
<td><strong>User Acceptance</strong></td>
<td>Medium</td>
<td>High (overt)</td>
<td>High</td>
<td>Low to Medium</td>
<td>High</td>
</tr>
<tr>
<td><strong>Privacy Concerns</strong></td>
<td>High</td>
<td>Very High (overt)</td>
<td>Medium</td>
<td>High</td>
<td>Very Low</td>
</tr>
<tr>
<td><strong>Cost</strong></td>
<td>Low to Medium</td>
<td>Low to Medium</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Potential for Circumvention</strong></td>
<td>Medium</td>
<td>High</td>
<td>Low to Medium</td>
<td>Very Low</td>
<td>High</td>
</tr>
<tr>
<td><strong>Distinctiveness</strong></td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>Very High</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Barriers to Universality</strong></td>
<td>Worn ridges; hand or finer impairment</td>
<td>None</td>
<td>Hand impairment</td>
<td>Visual impairment</td>
<td>Speech impairment</td>
</tr>
<tr>
<td><strong>Susceptibility to Changes in Biometric</strong></td>
<td>Low to Medium</td>
<td>Medium to High</td>
<td>Medium</td>
<td>Low</td>
<td>Low to Medium</td>
</tr>
<tr>
<td><strong>Susceptibility to Changes in the Environment</strong></td>
<td>Low</td>
<td>High</td>
<td>Very Low</td>
<td>Low</td>
<td>Medium to High</td>
</tr>
</tbody>
</table>

Biometric (pattern recognition) systems

Source: International Biometric Group, NY, 1.212.809.9491
Biometric (pattern recognition) systems
Biometric (pattern recognition) systems

**Enrollment**:
- **Biometric Sensor** → **Feature Extraction**
  - $B_1 = f(ID_1)$
  - $T_1$

**Authentication**:
- **Biometric Sensor** → **Feature Extraction**
  - $B_2 = f(ID_2)$
  - $T_2$

**Matching**
- $S(T_1, T_2)$

**Decision**
- If $S > T$ then **YES**
- If $S < T$ then **NO**
Biometric (pattern recognition) systems

- Positive verification (1:1)
  - ✓ claim is made (usename)

- Large scale identification (1:N)
  - ✓ no claim is made
  - ✓ claim is not trusted

- Screening
  - ✓ matching against a watch list
Biometric (pattern recognition) systems

Applications:

- Smart Card
- Physical Access Control
- Logical Access Control
- Forensics
- Border Control
- Consumer Products
- ATM
Biometric (pattern recognition) systems

Border security:

Started in August 2006

UAE border crossing
Biometric (pattern recognition) systems

Person control (Afghanistan):

U.S. forces use scanned fingerprints and irises for finding insurgents. The devices connect to a remote Defence Department database (Automated Biometric Information System – ABIS), which gathers identification data from U.S. and coalition partners.

http://online.wsj.com/article/SB125910374196463061.html
Biometric (pattern recognition) systems

Non-security applications: entrance control systems

Disney World, Orlando (20K visitors per day, 365 days per year)
Biometric (pattern recognition) systems

Non-security applications: payment systems

Meijer supermarket, Okemos

Mobile phone transaction

Citibank, Singapore: pay by fingerprints

Bank in Malawi uses fingerprints for micro-loans
Biometric (pattern recognition) systems

Non-security applications: user profiling

Technology
Identify the audience, categorize them (alone, family, friends); determine viewer sentiment

Applications
Content recommendation, target advertisements, secure TV commerce, real-time audience measurement
“By 2020, Biometrics will be a key enabler of trusted transaction control for data access and flow for consumer, commercial, and government applications.”

http://www.prweb.com/releases/2007/05/prweb526801.htm
Face detection
Face detection

Viola/Jones face detector:


- A “paradigmatic” method for real-time object detection
- Training is slow, but detection is very fast
- Key ideas
  - Integral images for fast feature evaluation
  - Boosting for feature selection
  - Cascade for fast rejection of non-face windows
Face detection

Rectangle image feature:
\[ \sum \text{ (pixels in white area)} - \sum \text{ (pixels in black area)} \]
Face detection

- For a 24x24 detection region, the number of possible rectangle features is ~180,000!
- At test time it is impractical to evaluate all features
- Can we create a good classifier using just a small subset of all possible features? How to select such a subset?
Face detection

AdaBoost for feature selection

- Standard AdaBoost scenario: boost classification performance of a “weak” classifier, e.g. perceptron
  - Apply to successively harder problems
  - Tweak parameters at each classification stage

- Face detection: use box sum features as weak classifiers
  - AdaBoost finds sequence of best features
Face detection

Weak classifier:

\( h(x, f, p, \theta) \) consists of a feature \((f)\), a threshold \((\theta)\) and a polarity \((p)\) indicating the direction of the inequality:

\[
    h(x, f, p, \theta) = \begin{cases} 
    1 & \text{if } pf(x) < p\theta \\
    0 & \text{otherwise}
    \end{cases}
\]

\( x \) is a \(24 \times 24\) pixel sub-window of an image.
Face detection

Boosting learning. $T$ hypotheses are constructed each using a single feature. The final hypothesis is a weighted linear combination of the $T$ hypotheses where the weights are inversely proportional to the training errors.

- Given example images $(x_1, y_1), \ldots, (x_n, y_n)$ where $y_i = 0, 1$ for negative and positive examples respectively.
- Initialize weights $w_{1,i} = \frac{1}{2m}, \frac{1}{2l}$ for $y_i = 0, 1$ respectively, where $m$ and $l$ are the number of negatives and positives respectively.
- For $t = 1, \ldots, T$:
  1. Normalize the weights, $w_{t,i} \leftarrow \frac{w_{t,i}}{\sum_{j=1}^{n} w_{t,j}}$
  2. Select the best weak classifier with respect to the weighted error
     
     $$
     \epsilon_t = \min_{f, p, \theta} \sum_i w_i \left| h(x_i, f, p, \theta) - y_i \right|
     $$
     
     See Section 3.1 for a discussion of an efficient implementation.
  3. Define $h_t(x) = h(x, f_t, p_t, \theta_t)$ where $f_t$, $p_t$, and $\theta_t$ are the minimizers of $\epsilon_t$.
  4. Update the weights:
     
     $$
     w_{t+1,i} = w_{t,i} \beta_t^{1-\epsilon_t}
     $$
     
     where $\epsilon_t = 0$ if example $x_i$ is classified correctly, $\epsilon_t = 1$ otherwise, and $\beta_t = \frac{\epsilon_t}{1-\epsilon_t}$.

- The final strong classifier is:

  $$
  C(x) = \begin{cases} 
  1 & \sum_{i=1}^{T} \alpha_i h_t(x) \geq \frac{1}{2} \sum_{i=1}^{T} \alpha_i \\
  0 & \text{otherwise}
  \end{cases}
  $$

  where $\alpha_i = \log \frac{1}{\beta_t}$
Face detection

- Given: example images labeled +/-
- Repeat $T$ times
  1. Select classifier with lowest weighted error over all
     - Features
     - Thresholds
     - Polarities
  2. Selected classifier is the hypothesis of this iteration
  3. Update the weights to emphasize examples on which this step’s classifier is wrong
- Final (strong) classifier is a weighted combination of the weak classifiers (weighted according to their accuracy)
Face detection

First two features selected by boosting:
Face detection

Cascading classifiers:

- We start with simple classifiers which reject many of the negative sub-windows while detecting almost all positive sub-windows.
- Positive results from the first classifier triggers the evaluation of a second (more complex) classifier, and so on.
- A negative outcome at any point leads to the immediate rejection of the sub-window.
Face detection

- Adjust weak learner threshold to minimize *false negatives* (as opposed to total classification error)
- Each classifier trained on false positives of previous stages
  - A single-feature classifier achieves 100% detection rate and about 50% false positive rate
  - A five-feature classifier achieves 100% detection rate and 40% false positive rate (20% cumulative)
  - A 20-feature classifier achieves 100% detection rate with 10% false positive rate (2% cumulative)
Face detection

Implemented system:

- **Training Data**
  - 5000 faces: rescaled to 24x24 pixels
  - 9500 non-face images

- **Many variations**
  - Illumination
  - Pose

- **Training time**: “weeks” on 466 MHz Sun workstation

- **Avg. of 10 features evaluated per window on test set**

- **Process a 384x288 image in ~.067 seconds (15 Hz)**
Face recognition

- **Appearance-based** methods use holistic texture features and are applied to either whole-face or specific regions in a face image.

- **Feature-based** methods use geometric facial features (mouth, eyes, brows, cheeks etc.) and geometric relationships between them.

- **Hybrid** methods combine global holistic and local face features.
Face recognition

Subspace analysis:
Project an image into a lower dimensional space (subspace) and recognition is then performed by measuring the distances between known images and the image to be recognized. The most challenging part of such a system is finding an adequate subspace.

- Eigenface (see Chapter 2 “Merkmale“)
- Fisherface
- Independent Component Analysis
- Many others
Face recognition

- AT&T (ORL) database: 400 images of 40 subjects

<table>
<thead>
<tr>
<th>Method</th>
<th>Reduced Space</th>
<th>Error Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICA</td>
<td>40</td>
<td>6.25 (25/400)</td>
</tr>
<tr>
<td>Eigenface</td>
<td>30</td>
<td>2.75 (11/400)</td>
</tr>
<tr>
<td>Fisherface</td>
<td>14</td>
<td>1.50 (6/400)</td>
</tr>
<tr>
<td>Kernel Eigenface, d=2</td>
<td>50</td>
<td>2.50 (10/400)</td>
</tr>
<tr>
<td>Kernel Eigenface, d=3</td>
<td>50</td>
<td>2.00 (8/400)</td>
</tr>
<tr>
<td>Kernel Fisherface (P)</td>
<td>14</td>
<td>1.25 (5/400)</td>
</tr>
<tr>
<td>Kernel Fisherface (G)</td>
<td>14</td>
<td>1.25 (5/400)</td>
</tr>
</tbody>
</table>
Face recognition

- Yale database: 165 images of 15 subjects

![Image of Yale database]

<table>
<thead>
<tr>
<th>Method</th>
<th>Reduced Space</th>
<th>Error Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICA</td>
<td>30</td>
<td>29.09 (48/165)</td>
</tr>
<tr>
<td>Eigenface</td>
<td>30</td>
<td>28.48 (47/165)</td>
</tr>
<tr>
<td>Fisherface</td>
<td>14</td>
<td>8.48 (14/165)</td>
</tr>
<tr>
<td>Kernel Eigenface, d=2</td>
<td>80</td>
<td>27.27 (45/165)</td>
</tr>
<tr>
<td>Kernel Eigenface, d=3</td>
<td>60</td>
<td>24.24 (40/165)</td>
</tr>
<tr>
<td>Kernel Fisherface (P)</td>
<td>14</td>
<td>6.67 (11/165)</td>
</tr>
<tr>
<td>Kernel Fisherface (G)</td>
<td>14</td>
<td>6.06 (10/165)</td>
</tr>
</tbody>
</table>
Face (profile) recognition

Profile provides sufficient information for person identification, in particular in combination with frontal images; see Chapter 5 “Kombination von Klassifikatoren“
3D face recognition

Using range data has the potential to overcome several problems inherent in intensity-based biometrics:

Because we are working in 3D, we overcome limitations due to viewpoint and lighting variations.

Medioni/Waupotitsch:

Depth and curvature features have several advantages over more traditional intensity-based features. Specifically, curvature descriptors: (1) have the potential for higher accuracy in describing surface-based events, (2) are better suited to describe properties of the face in areas such as the cheeks, forehead, and chin, and (3) are viewpoint invariant.
3D face recognition


A single subject with neutral, surprise, happiness, disgust, and sadness expressions along with the corresponding fitted models
3D face recognition

FRGC Database:
http://www.frvt.org/FRGC/

4,007 3D scans of 466 persons of resolution 480 x 640 using Minolta Vivid 910


FRGC is open to all interested researchers — there is no fee to participate
Face recognition: Challenges

- Pose, lighting, expression
- Occlusion
- Aging
- Sketch vs. photo
Face recognition: Literature

- http://www.face-rec.org
Iris recognition

Advantages:
- iris stays stable throughout the live
- more unique than fingerprint
- can’t be forged, impossible to fake
Iris recognition

An arriving passenger at Dubai Airport being compared against 420,000 registered iris patterns in about one second

http://www.cl.cam.ac.uk/~jgd1000/UAEdeployment.pdf

An infrared wavelength iris camera at Schiphol Airport, NL
Iris recognition

- Health care industry: Biometric patient ID at Urban Health Plan
  http://www.youtube.com/watch?v=cFznBdlJdgk

- In policing and prisons: Cororado cops ID / Track suspects
  http://www.youtube.com/watch?v=vuDOpjp22nY
Iris recognition

History:

- The idea of using iris patterns for personal identification was originally proposed in 1936 by ophthalmologist Frank Burch.
- By the 1980's the idea had appeared in James Bond films, but it still remained science fiction and conjecture.
- In 1987 two other ophthalmologists, Aran Safir and Leonard Flom, patented this idea, and in 1989 they asked John Daugman (then teaching at Harvard University) to try to create actual algorithms for iris recognition.
- These algorithms, which Daugman patented in 1994 and are owned by Iridian Technologies, are the basis for all current iris recognition systems and products.
Iris recognition

Most commercial iris biometrics systems use near-IR illumination; thus think “monochrome” rather than “RGB”

![Approximate near-IR range for iris biometrics](image)
Iris recognition

Light-colored irises may look similar in visible light (left) and near infrared (right)

Using near-IR illumination allows usable texture imaging even for “dark” irises
Iris recognition

Iris code (256 bytes) of John Daugman:

Iris recognition

Hamming distance:

\[ HD = \frac{\| (\text{code}A \otimes \text{code}B) \cap \text{mask}A \cap \text{mask}B \|}{\| \text{mask}A \cap \text{mask}B \|} \]
Iris recognition

Examples of Gabor filters

Gabor Filter, Re Part, $\alpha=0.2$, $\beta=0.2$, $\omega=5$

Gabor Filter, Re Part, $\alpha=0.2$, $\beta=0.2$, $\omega=25$

Gabor Filter, Re Part, $\alpha=0.15$, $\beta=0.15$, $\omega=25$

Gabor Filter, Im Part, $\alpha=0.2$, $\beta=0.2$, $\omega=5$

Gabor Filter, Im Part, $\alpha=0.2$, $\beta=0.2$, $\omega=25$

Gabor Filter, Im Part, $\alpha=0.15$, $\beta=0.15$, $\omega=25$
Iris recognition

Binomial Distribution of IrisCode Hamming Distances

Solid curve: binomial PDF, N=249 degrees-of-freedom, p=0.5

9,060,003 different iris comparisons

mean = 0.499, std.dev. = 0.0317
min = 0.334, max = 0.664

Distribution of HDs obtained from 9.1 million comparisons between different pairings of iris images (UK, USA; Japan, Korea).
Distribution of HDs between genetically identical irises, in 648 paired eyes from 324 persons. The data are statistically indistinguishable from that from comparing unrelated irises (last slide).
Iris recognition

Story of Afghan girl:
http://www.youtube.com/watch?v=cK6EnFu3NHc&feature=fvw
Iris recognition

1984

2002

left, HD=0.24

right, HD=0.31
Hand-based biometrics

Fingerprint + palmprint + finger-knuckle

Perhaps the most beautiful and characteristic of all superficial marks (on human body) are the small furrows with the intervening ridges and their pores that are disposed in a singularly complex yet even order on the under surfaces of the hands and feet.

Francis Galton, Nature, June 28, 1888
Hand-based biometrics

Fingerprint + palmprint + finger-knuckle
Palmprint recognition

Originally from Chinese hand book for future
Palmprint recognition

Competitive code:

- Gabor filtering
- encode each winning direction index into 3 bits
- angular distance matching

\[
D(P, Q) = \sum_{x=1}^{n} \sum_{y=1}^{n} \sum_{i=1}^{3} P_M(x, y) \land Q_M(x, y) \land (P_i^b(x, y) \oplus Q_i^b(x, y))
\]

\[
3 \sum_{x=1}^{n} \sum_{y=1}^{n} P_M(x, y) \land Q_M(x, y)
\]
Multibiometric systems

- Fingerprint Matcher
- Signature Matcher
- Hand Geometry Matcher
- Face Matcher
- Speaker Matcher
- Gait Matcher
- Pulse Matcher

All Modalities have different input signals

- Independent
Biometrics: Challenges

- Large scale systems
- Uniqueness of biometric traits
- Sensors & interoperability
- Mutilbiometric systems
- Less controlled data acquisition
- Continuous authentication
- Soft biometrics (eye/hair/skin color, height, weight)
- Biometric system security
Biometrics: Threats

Matsumoto’s technique

Put the plastic into hot water to soften it.

Press a live finger against it.

It takes around 10 minutes.

The mold
You can place the “gummy finger” (clone) over your real finger. Observers aren’t likely to detect it when you use it on a fingerprint reader. Only a few dollars’ worth of materials.
New era of biometrics

Embedded systems:

- Cheap & compact sensors
- Requirements: throughput, cost & HCI
New era of biometrics

Distant systems (surveillance, etc.):

- Performed by German Federal Police (Oct 06 to Jan 07)
- Purpose: Test face recognition systems in a real environment (train station); camera views at escalator & stairs
- Performance: Identification rate of 60% at a FAR of 0.1% based on a gallery (watch list) of 200 enrolled persons
New era of biometrics

Mobile systems:

- 320x240
  - $10

- 640x480
- 1280x960
- 3500x2200
  - $1000
Mobile biometrics

- Mobile computing (intelligence)
- Mobile biometrics
  - challenges
  - architectures
  - case studies
  - datasets
- Implementation issues
Mobile computing

1) Mainframe
   1 Computer
   Many users

2) PCs
   1 Computer
   1 User

3) PDA, Smart Phone
   Smart Card
   1 User
   Many computers

Source: Mark Weiser (adapted)
Era of mobile computing (intelligence)

Impact 1: Mobile intelligence substantially expands the user population

Source: Morgan Stanley, The Mobile Internet Report
Impact 2: Mobile intelligence substantially expands information opportunities.
Impact 3: Mobile intelligence substantially expands personal query relevance
Era of mobile computing (intelligence)

- Mobile phones (smart phones)
- Personal digital assistants
- Tablets
- Notebooks
- Handheld game consoles
- Fully functional in-car computers
- .......
Era of mobile computing (intelligence)

Dedicated devices:

Source: Motorola
Protection of mobile devices

Greater levels of protection are required:

- Advanced devices
  expensive devices $\Rightarrow$ theft $=$ financial loss

- Availability of data services
  theft / misuse $\Rightarrow$ even more financial loss

- Sensitive information

  mobile phone $=$ personal safe!

  theft / misuse $\Rightarrow$ invaluable *immaterial* loss
Mobile biometrics

Perhaps likely modalities:
- 2D face recognition
- palmprint
- hand
- fingerprint (with/without embedded scanner)
- iris
- ear
- 2D signature
- keystrokes
- speech
- 3D (in-air) signature

Rather unlikely modalities:
- 3D face recognition
- gait
- vein
Challenges of mobile biometrics

- Uncontrolled environment
  - complex background (segmentation)
  - changing lighting (normalization)
  - varying pose (invariance)
  - environment noise (signal separation)
  - variation of devices

- Limited resources
  - memory
  - CPU power
# Challenges of mobile biometrics

## Environment influence factors

<table>
<thead>
<tr>
<th>Features</th>
<th>Potential impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Physical environment in which the biometric system is affects or influences the design.</td>
</tr>
<tr>
<td>Device location</td>
<td>Device's location affects the user's ability to use or access the system.</td>
</tr>
<tr>
<td>Temperature and humidity</td>
<td>External environment affects the system performance and temperature and humidity affects the capture of a high-quality sample.</td>
</tr>
<tr>
<td>Ethnicity, nationality, language and culture</td>
<td>Without a common language there can be no impact on the design of feedback and instruction guide.</td>
</tr>
<tr>
<td>Lighting</td>
<td>The light level lighting affects the reading or the visibility of the graphics device.</td>
</tr>
<tr>
<td>Noise</td>
<td>The noise level can affect the ability of an individual to hear tips and information for audio and give a feedback to the system.</td>
</tr>
<tr>
<td>Instructions</td>
<td>If there are instructions, icons and sizes of the letters must be seen as appropriate and understandable.</td>
</tr>
<tr>
<td>Help</td>
<td>In a given environment, it must be known the better way to provide feedback, errors and help information.</td>
</tr>
</tbody>
</table>

Modern mobile embedded CPUs are designed with much more than pure speed in mind. Priority is often given to factors which address requirements of a mobile operating environment such as low heat dissipation, minimal power consumption, and small size.

**GPUs** (built into most mobile devices) can help to speed up processing via parallel computing. But many algorithms are designed to be executed sequentially and cannot fully utilize GPU capabilities.
Challenges of mobile biometrics

<table>
<thead>
<tr>
<th>Feature</th>
<th>Motorola DROID</th>
<th>Typical PC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen size</td>
<td>4.6 in × 2.4 in</td>
<td>25 in × 16 in</td>
</tr>
<tr>
<td>Processor speed</td>
<td>550 MHz</td>
<td>3.0 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>256 MB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Permanent storage</td>
<td>133 MB internal 8 GB external flash</td>
<td>500 GB disk</td>
</tr>
<tr>
<td>Internet access</td>
<td>Typically 3G or WiFi at hotspots</td>
<td>WiFi or wired Ethernet</td>
</tr>
<tr>
<td>Telephony</td>
<td>Core feature</td>
<td>Supplementary feature</td>
</tr>
<tr>
<td>Camera</td>
<td>5 MP camera embedded</td>
<td>External webcam</td>
</tr>
</tbody>
</table>

Source: David Chen
Architectures for mobile biometrics

- **Embedded:**
  The complete processing is performed on mobile device

- **Distributed**
  The mobile device (client) sends the image/video/speech data to a server for computation. The results are transmitted back to the mobile device for further use.

- **Hybrid**
  The processing is shared by the mobile device and server

  → Stable network connection required
Architectures for mobile biometrics

Distributed architecture (example: speech recognition)

Source: Tan/Lindberg
Architectures for mobile biometrics

Hybrid architecture (example: speech recognition)

- Source and Channel Encoder
- Mobile / IP Networks
- Channel and Source Decoder

Input: Speech Signal

Output: y(t)

Source: Tan/Lindberg
Case studies

- Palmprint
- Hand
- Keystroke
- 3D (in-air) signature

Hand-based

- Teeth
- Speech
Palmprint

- Using the built-in LED-flash to “override” illumination influences
- Color-based hand segmentation
- Detection of ROI
  - rough orientation normalization
  - valley detection
  - derivation of ROI
- Competitive code

Palmprint

Left: input image.
Middle: imperfect hand segmentation.
Right: rough orientation normalization, valley detection (two red points), and ROI derived from the valley points.
Palmprint

Dealing with misalignment after preprocessing

- a number of horizontal/vertical translations are probed and the minimum angular distance is regarded the final matching score
- shift -4 to 4 for tests
Palmprint

Computing $d(P,Q_t)$ for competitive code $P$ and another one $Q$ subject to a translation $t$:

- Compare the whole content of $P$ and $Q_t$

- **Speedup:**
  The comparison for optimal shift is restricted to a small part only, say the two rows in the middle. The final matching score is then computed for the full size based on the optimal translation determined by the reduced search.
Modes of flash illumination:

- The image is captured immediately after the flash is switched on
- The flash is permanently on

The behavior of different mobile phones varies

- 1\textsuperscript{st} mode does work slightly better for iPhone
- On some models the reaction time of the camera chip does not match the flash well and leads to improper exposure $\rightarrow$ 2\textsuperscript{nd} mode is generally more favorable
Palmprint

Related to so-called touch-less palmprint biometrics:


- More restricted setup compared to mobile palmprint
- PC computational power
Hand

Hand

- Feature extraction
  - length of the finger from the tip of the finger
  - dividing the finger in \( m \) parts, measuring perpendicularly finger widths at each position
  - distance based on the finger tip curvature

- SVM with linear kernel function (best results when compared to other classifiers or kernel functions)

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Equal error rate (%) performance in relation to parameters ( m ) and ( q )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( m = 5 )</td>
</tr>
<tr>
<td>( q = 5 )</td>
<td>7.3 ± 0.2</td>
</tr>
<tr>
<td>( q = 10 )</td>
<td>7.5 ± 0.3</td>
</tr>
<tr>
<td>( q = 15 )</td>
<td>7.3 ± 0.1</td>
</tr>
<tr>
<td>( q = 20 )</td>
<td>7.9 ± 0.2</td>
</tr>
</tbody>
</table>

Notice that a greater number of features does not imply better results in terms of identification and verification.
Keystroke characteristics

- Keystroke latency (time between successive keystrokes)
- Hold-time characteristic (time to press and release a key)

Neural neural networks used for classification


Keystroke

Continuous or periodic authentication of the user, so that the confidence in the identity of the user can be maintained throughout the life of the device.
3D (in-air) signature

User performs his/her identifying gesture in the air by holding a telephone with an embedded accelerometer in his/her hand

- Accelerations of the gesture in the three axes sampled at frequency rate of 50 Hz
- Variant of dynamic time warping (DTW) for global sequence alignment
- Eight different score definitions defined to quantify the differences

## 3D (in-air) signature

<table>
<thead>
<tr>
<th>Score</th>
<th>Optimal EER</th>
<th>Threshold $\theta_{\text{EER}}$</th>
<th>$\text{FAR}(\theta_{\text{EER}})$</th>
<th>$\text{FRR}(\theta_{\text{EER}})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\psi_1$</td>
<td>5.46 ± 1.61</td>
<td>0.96 ± 0.01</td>
<td>8.26 ± 6.49</td>
<td>10.19 ± 6.65</td>
</tr>
<tr>
<td>$\psi_2$</td>
<td>7.87 ± 1.01</td>
<td>1.26 ± 0.02</td>
<td>9.05 ± 3.00</td>
<td>9.30 ± 2.76</td>
</tr>
<tr>
<td>$\psi_3$</td>
<td>3.95 ± 0.96</td>
<td>1.36 ± 0.03</td>
<td>4.01 ± 2.41</td>
<td>5.03 ± 2.43</td>
</tr>
<tr>
<td>$\psi_4$</td>
<td>3.73 ± 0.86</td>
<td>1.42 ± 0.04</td>
<td>6.38 ± 2.71</td>
<td>5.66 ± 1.70</td>
</tr>
<tr>
<td>$\psi_5$</td>
<td>4.60 ± 1.76</td>
<td>0.96 ± 0.02</td>
<td>6.05 ± 3.45</td>
<td>6.23 ± 3.32</td>
</tr>
<tr>
<td>$\psi_6$</td>
<td>7.77 ± 1.49</td>
<td>1.37 ± 0.03</td>
<td>11.81 ± 3.89</td>
<td>8.04 ± 1.85</td>
</tr>
<tr>
<td>$\psi_7$</td>
<td>4.67 ± 1.51</td>
<td>1.43 ± 0.06</td>
<td>6.76 ± 3.31</td>
<td>4.45 ± 2.78</td>
</tr>
<tr>
<td>$\psi_8$</td>
<td>3.42 ± 1.22</td>
<td>1.54 ± 0.07</td>
<td>3.67 ± 3.11</td>
<td>4.10 ± 2.63</td>
</tr>
</tbody>
</table>
Teeth

- Teeth region detection: AdaBoost algorithm based on Haar-like (like face detection)
- 2D-DCT features
- Embedded HMM (for dealing with 2D data)

Teeth

Pre-processing. (a) teeth region detection; (b) detected teeth region; (c) thresholded image; (d) centers of mass; (e) image applied to the centers for authentication; (f) rotated image with horizontal line connecting the both centers; (g) pre-processed teeth image.
Speech


Multimodal biometrics

Teeth image

2D-DCT → Teeth Model Templates

Pitch, MFCC → GMM

Score Normalize → Score Fusion

Sum of score

Accept/Reject Decision
Multimodal biometrics

![Graph showing multimodal biometrics data](image-url)

- **Graph 1**: Scatter plot of Voice Scores vs. Teeth Scores, with separate points for Genuine and Imposter samples.
- **Graph 2**: ROC curve for False Rejection Rate (%) vs. False Acceptance Rate (%), with lines representing Fusion, Teeth, and Voice modalities.
Datasets

- Pamprint:
  - 30 persons, 20 palms per person (10 for each hand)
  - in-door and out-door, different background/illumination, sitting/standing
  - iPhone

- Hand:
  - 50 persons (age 16-60, different races)
  - no removal of rings, bracelets, or watches
  - no control on illumination, background, hand orientation
  - iPhone at 10-15cm of distance

- 3D (in-air) signature
  - 80 persons
  - iPhone
Developing mobile multimedia applications

Popular mobile platforms

- **Symbian**
  - Nokia N8
  - Nokia N97

- **Windows 7**
  - HTC Arrive
  - Samsung Focus

- **Apple iOS**
  - iPhone
  - iPad

- **Android**
  - Motorola Droid
  - Samsung Galaxy Tab

Source: David Chen
Kapitel 10 “Biometrics” – p. 104
Developing mobile multimedia applications

David Chen: Lecture “Mobile Image Processing on Android“, 2011
http://stanford.edu/~dmchem/teaching.html


Developing mobile multimedia applications

OpenCV: Open Source Computer Vision

General Image Processing Functions
Image Pyramids
Segmentation
Geometric descriptors
Camera calibration, Stereo, 3D
Features
Utilities and Data Structures
Transforms
Tracking
Fitting
Machine Learning:
- Detection,
- Recognition
Matrix Math

Source: David Chen

http://opencv.willowgarage.com/wiki/Android
Developing mobile multimedia applications

Apple Accelerate framework:
A set of libraries containing high-performance vector-accelerated libraries

- Reference PDF:

It works with vectorized versions of routines that utilize the SIMD units on the CPU (e.g. SSE on Intel).

- Gabor filtering: 4.258 sec. to 0.116 sec
Mobile biometrics

- Mobile biometrics has substantial potential and impact
- Mobile biometrics is still in its infancy
- Mobile biometrics has many additional challenges compared to classical biometrics
  - complex background (segmentation)
  - changing lighting (normalization)
  - varying pose (invariance)
  - environment noise (signal separation)
  - variation of devices
- limited resources
Mobile biometrics

As much as TV transformed entertainment and PC transformed work, mobile technology is transforming the way that we will interrelate. Michael Gold (SRI Consulting)

As mobile computing becomes pervasive in both personal and professional lives, people are discovering more and more opportunities to make complete use of these powerful devices. From the moment they wake, they can use applications that not only enhance their personal lives but also make them more productive and effective at work.

MicroStrategy

Dream or nightmare? ……

Every Waking Second
Sources

- Courses: e.g. K. Bowyer, V. Govindaraju
- Presentations of Anil Jain
  http://biometrics.cse.msu.edu/pres/index.html
- Iris: John Daugman’s homepage
  http://www.cl.cam.ac.uk/~jgd1000/