Introduction to Biometrics

Dr. Bojan Cukic
Center for Identification Technology Research
West Virginia University
CITeR

Outline (1)

Module 1: Biometric Systems
- Definitions, Terminology
- Technological, Ethical, and Socio-legal Implications
- System Architecture, Subsystems, and Components
- Classification and Templates
- Standardization

Identification Methods
- Seek to identify an individual within a population of possible "users".
- Identity means person's
  - Appearance
  - Physiological makeup
  - Actions
  - Belief Systems, Sense of Self, etc....
- We need a manageable engineering definition!
Introduction

Engineering Approach

Reduce the problem of confirming a person’s identity to the problem of authentication of a concrete entity related to a person.

Most Common:
1. Possession (What you have).
   - Keys, ATM card, ID card/badge, etc.
   - Problems: Loss, theft, forgery.
2. Knowledge of a piece of information (What you know).
   - Password, PIN, mother’s maiden name, etc.
   - Problems: Forgetfulness, theft.
3. Combination of both (e.g., ATM with PIN)
   - Note: BOTH require a trusted enrollment process

(2)

Who You Are.
- Biometrics: face, fingerprint, voice, hand geometry, retina scans, iris scans...
- Handling of false positives and false negatives.

What You Do.
- Other kinds of biometrics: written signatures, typing patterns, etc.
- Need to be fine tuned for specific applications.

Where You Are.
- Allow system login only from certain terminals.
- Suitable for mobile and distributed computing.
- GPS based authentication may resolve disputes about user’s identity (in case of a misuse).

Popular Biometric Technologies

- Fingerprint verification
- Hand geometry
- Voice verification
- Retinal scanning
- Iris scanning
- Signature verification
- Facial recognition
- "Bleeding edge" biometrics
  - Gait, odor, ear, hand vein, thermography...
Current Applications

- Prison visitor systems
- Drivers licenses
- Canteen administration
- Benefit payment systems
- Border control
- Voting systems
- Physical access control

Common Ideas for Future Apps

- ATM machines
- Workstation and network access
- Travel, hospitality and tourism
  - Frequent flyer, border control, air, hotel, car, etc.
- Internet transactions
- Telephony
- Public ID cards (controversial)

Biometric Systems

- Introduction
  - System architecture
  - Biometric capture/data collection
  - Template generation
  - Matching
ID Methods

Engineering Solutions
- Reduce problem to ID of physical characteristics of an individual they always possess
  - Physiological
  - Behavioral
  - Biological
- Such traits of the human biological system, suitable for use as metrics for measurement and use in identification, are referred to as Biometrics

Biometric Identification

Pervasive use of biometric ID is enabled by automated systems
- Enabled by inexpensive embedded computing and sensing.
- Computer controlled acquisition, processing, storage, and matching using biometrics.
- Biometric systems are one solution to increasing demand for strong authentication of actions in a global environment.
- Biometrics tightly binds an event to an individual
- A biometric can not be lost or forgotten, however a biometric must be enrolled.

Characteristics of a Useful Biometric

- If a biological, physiological, or behavioral characteristic has the following properties...
  - Universality
  - Uniqueness
  - Permanence
  - Collectability
  - then it can potentially serve as a biometric for a given application.
Useful Biometrics

1. Universality
   - Universality: Every person should possess this characteristic.
   - In practice, this may not be the case.
   - Otherwise, population of nonuniversality must be small < 1%.

2. Uniqueness
   - Uniqueness: No two individuals possess the same characteristic.
     - Genotypical – Genetically linked (e.g. identical twins will have same biometric).
     - Phenotypical – Non-genetically linked, different perhaps even on same individual.
   - Establishing uniqueness is difficult to prove analytically.
   - May be unique, but “uniqueness” must be distinguishable.

3. Permanence
   - Permanence: The characteristic does not change in time, that is, it is time invariant.
     - At best this is an approximation.
     - Degree of permanence has a major impact on the system design and long term operation of biometrics.
       (e.g. enrollment, adaptive matching design, etc.)
     - Long vs. short-term stability.
Useful Biometrics

4. Collectability
   - Collectability: The characteristic can be quantitatively measured.
   - In practice, the biometric collection must be:
     - Non-intrusive
     - Reliable and robust
     - Cost effective for a given application

Current/Potential Biometrics

- Voice
- Infrared facial thermography
- Fingerprints
- Face
- Iris
- Ear
- EKG, EEG
- Odor
- Gait
- Keystroke dynamics
- DNA
- Signature
- Retinal scan
- Hand & finger geometry
- Subcutaneous blood vessel imaging

What is consensus evaluation of current biometrics based on these four criteria?

System-Level Criteria

- Our four criteria were for evaluation of the viability of a chosen characteristic for use as a biometric
- Once incorporated within a system the following criteria are key to assessment of a given biometric for a specific application:
  - Performance
  - User Acceptance
  - Resistance to Circumvention
Central Privacy, Sociological, and Legal Issues/Concerns

System Design and Implementation must adequately address these issues to the satisfaction of the user, the law, and society.
- Is the biometric data like personal information (e.g., such as medical information)?
- Can medical information be derived from the biometric data?
- Does the biometric system store information enabling a person’s “identity” to be reconstructed or stolen?
- Is permission received for any third party use of biometric information?

Central Privacy, Sociological, and Legal Issues/Concerns (2)

Continued:
- What happens to the biometric data after the intended use is over?
- Is the security of the biometric data assured during transmission and storage?
  - Contrast process of password loss or theft with that of a biometric.
  - How is a theft detected and “new” biometric recognized?
- Notice of Biometric Use. Is the public aware a biometric system is being employed?

Biometric System Design

Target Design/Selection of Systems for:
- Acceptable overall performance for a given application
- Acceptable impact from a socio-legal perspective
- Examine the architecture of a biometric system, its subsystems, and their interaction
- Develop an understanding of design choices and tradeoffs in existing systems
- Build a framework to understand and quantify performance
Biometric Systems Segment Organization

- Introduction
  - System Architecture
- Biometric Capture/Data Collection
- Template Generation
- Matching

System Architecture

- Application
- Authentication Vs. Identification
- Enrollment, Verification Modules
- Architecture Subsystems

Biometric Applications

Four general classes:
- **Access** (Cooperative, known subject)
  - **Logical Access** (Access to computer networks, systems, or files)
  - **Physical Access** (access to physical places or resources)
- Transaction Logging
- **Surveillance** (Non-cooperative, known subject)
- **Forensics** (Non-cooperative or unknown subject)
System Architecture

- Architecture Dependent on Application:
  - Identification: Who are you?
    - One to Many (millions) match (1:Many)
    - One to “few” (less than 500) (1:Few)
    - Cooperative and Non-cooperative subjects
  - Authentication: Are you who you say you are?
    - One to One Match (1:1)
    - Typically assume cooperative subject
  - Enrollment and Verification Stages common to both.

System Architecture (2)

Enrollment: Capture and processing of user biometric data for use by system in subsequent authentication operations.

Authentication/Verification: Capture and processing of user biometric data in order to render an authentication decision based on the outcome of a matching process of the stored to current template.

System Architecture (3)

Authentication Application:

- Enrollment Mode/Stage Architecture
  
  Approx 512 bytes of data per template
**System Architecture (4)**

- Authentication Application:
  - Verification/Authentication Mode/Stage Architecture

```
Biometric data collection -> Transmission -> Quality sufficient?
<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

- Database:
  - Generate Template
  - Template Match
  - Decision Confidence

- Biometric Capture/Data Collection
  - Approx 512 bytes of data per template

**Biometric Systems Segment Organization**

- Introduction
- System Architecture
  - Biometric Capture/Data Collection
  - Template Generation
  - Matching

**Biometric Data Collection Module**

- Examples
  - Face/Voice/PIN (static)
  - Fingerprint (static)
  - Iris (static)
Biometric Sensor Systems

- **Modes**
  - Contact
  - Non-Contact

- **Biometric ID**
  - Ranges and technologies (non network)

Biometric Data Collection

<table>
<thead>
<tr>
<th>Contact</th>
<th>Personal Space</th>
<th>Group Perimeter</th>
<th>Extended Perimeter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-2 meters</td>
<td>10 meters</td>
<td>&gt; 10 meters</td>
<td></td>
</tr>
</tbody>
</table>

Human ID

Human activity/presence

Issues in Current Devices: Spoof/circumvention Detection

- Needs analysis part of overall threat assessment
- Employ countermeasures:
  - Multiple biometrics
  - E.G. Prompted voice and face.
  - Raise difficulty threshold for spoofing.
  - Use "liveness" tests rather than biometric (E.G. oximetry)
  - Prompt user for detectable action (E.G. Facial motion)
  - Draw upon unique characteristics associated with biometric or its acquisition.
  - Knowledge of physiology-sensor interaction.
  - Understanding of signal processing used in system
  - Typically can be software-only based solution

Issues in Current Devices: Spoof/circumvention Detection

- Examples:
  - Iris —
    - Hippus: small few Hz oscillation of the pupil
    - Raise difficulty threshold for spoofing
    - Spatial frequency signature detection of iris spoof
    - Subcutaneous Vessel Imaging
      - Blood, pulse oximetry
    - Fingerprint
      - Thermal sensing
      - Time dependent change due to perspiration
Introduction

Biomedical Signal Analysis

Image Processing to Detect Fingerprint Vitality Features

Previous Work - Algorithm

Capture time-sequence of fingerprint images over 5 seconds
- Perform image processing to clean and convert images to a fingerprint “signal”
- Calculate static and dynamic features
- Use neural network to classify
- Tested on 18 each live, cadaver and spoof

Biometric Systems Segment Organization

- Introduction
- System Architecture
- Biometric Capture/Data Collection
  - Template Generation
- Matching
Template Generation

- Generate a Minimum Size, Digital Record of the Biometric which is
  - Distinguishable from other records within some acceptable error
  - Irreversible to original raw biometric
- Implies need for Template definition and corresponding matching algorithm to compare input against stored templates.
- Template definition approaches.....

Template Definition Approaches

- Data set of Local Biometric Features
  - Mapping of biometric features
  - Type, position, orientation, etc.
  - Mathematically represented to achieve rapid matching (graph based, etc)
- Data Set Representing Global Biometric
  - Reduced Vector Representation of entire Image
  - Neural Network "trained" system
  - Correlation based representations
- Mixed Templates: Local Application of Global technology

Template Sizes

- Typical template size 512 to 1024 Bytes
  - For eight bit image, 300x300 pixels resolution, this represents an approximately 90000/1000 reduction factor
- Nonreversible
  - Original image of the biometric cannot be regenerated from the template information
  - Recall the importance of this specification for the template with regard to system acceptance
Introduction

Case Study: Fingerprint

- Fingerprint matching
  - Biometric features: Features of Ridges
    - Minutiae –
      - Types – ending and bifurcation
    - Features of a Minutia to quantify?
      - Type, location (x,y) and direction.
      - Some use additional features (core, delta, ridge flow...)

Case Study - Fingerprint

- Feature Extraction Stage
  - Using thinned image, minutiae straightforward to detect.
    - Endings found at ends of thinned feature lines
    - Bifurcations found at the junctions of three lines
    - Will have extraneous features – remove using empirical thresholds
    - Usually 10 – 100 valid minutiae
  - Determine attributes for each valid minutia found
    - Type, (x,y) location, direction.
  - Yields a Minutia Template
    - Type(1 bit), location (9 bits each for x,y) and direction (8 bits) – total 27 – say 4 bytes so template may require 400 bytes standard for fingerprints is 512 bytes.

Biometric Systems Segment Organization

- Introduction
- System Architecture
- Biometric Capture/Data Collection
- Transmission and Signal/Image Processing and Pattern Recognition
- Template Generation
  - Matching
Matching Process: System Considerations

- **One-to-One Match (1:1)** – Only one template or an identifier (PIN) is given by the claimant pointing to a single template in a large repository.  
  - Matching process of claimant to enrollee template occurs in time \( t_{\text{template}} \) (this is the time for the matching algorithm to yield a matching score.)

![PIN Associated with Only 1 Template]

- **One-to-N Match** – Multiple templates but \( N \) small (\( N < 500 \))
  - As we add more templates to the system worse case match time is \( N \ t_{\text{template}} \) as the claimant template is compared to all \( N \) enrolled templates

![Template is Compared to Enrolled Templates for Match]

- **One-to-Many Match** – Multiple templates but \( N \) large (\( N > 1000 \)). True identification system  
  - Beyond some value \( N \) max. match time \( N \ t_{\text{template}} \) becomes prohibitive. Match time grows linearly!

![Template is Compared to Enrolled Templates for Match]
Matching Process: System Considerations

- Define partitions of template database. These represent bins for sorting of templates such that $N_{bin}$ template is acceptable.

$$t = t_{bin} + N_{template}$$

Biometric System Evaluation: Introduction

- No single metric is sufficient to give a reliable and convincing indication of the identification accuracy of a biometric system.
- Let's first look at describing the decision outcomes from a biometric system.
  - This is under normal operating conditions
  - No spoofing of the system considered.

Biometric System Evaluation (2)

- A decision made by a biometric system is either a genuine individual type of decision or an imposter individual type of decision.
- There are two types of decision outcomes: true or false. Given these two types of decisions and the two decision outcomes, there are 4 possible combined outcomes
  1. A genuine individual is accepted.
  2. A genuine individual is rejected.
  3. An imposter is rejected.
  4. An imposter is accepted.
- Outcomes 1 & 3 are correct, whereas outcomes 2 & 4 are incorrect.
Biometric System Evaluation (3)

- In principle we can use the following to assess systems:
  - False (genuine individual) Rejection Rate (FRR) (also called Type I error), and
  - The False (imposter) Acceptance Rate (FAR) (also called Type II error),
  - The equal error rate (rate where FAR and FRR are equal)
- These are test population and system configuration dependent and cannot be generalized even for the same system under different populations or test conditions!
- Statistical methods are used to assess system performance.