Biometric Solutions

Wireless Business Solutions

www.vast.com

Agenda

- Biometrics Overview
- Biometric system requirements
- Privacy and Ethics
- Planning & Engineering a Biometric System
- Biometric Planning Considerations
- Biometric System Design

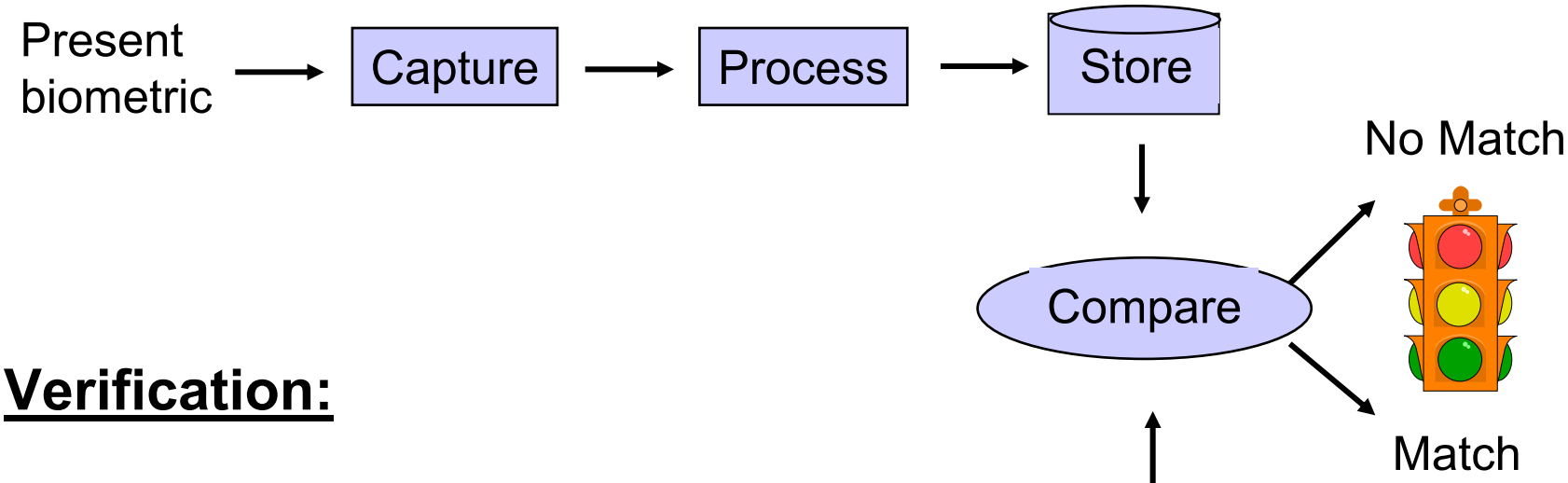
Biometric overview

- What are Biometrics?
  - Measurements of certain physical or biological characteristics of an individual to create an unique identifier which can be electronically stored, retrieved, and compared for positive identification purposes
- Examples of Biometric Types:

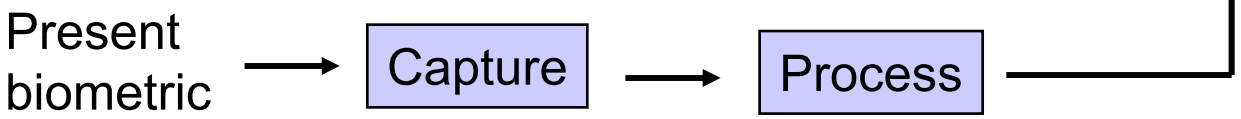
- Fingerprint
- Facial features
- Voice
- Signature
- Iris
- Retina
- Hand geometry
- Facial thermography
- Keystroke dynamics
- Palm print
- Vein patterns
- DNA

How do biometrics work?

Enrollment:



Verification:



Three basic processes

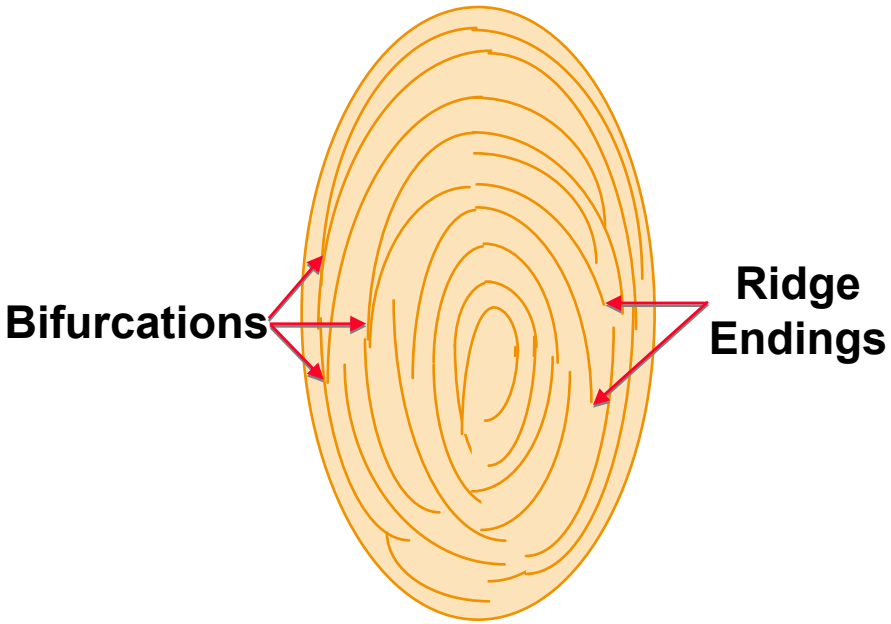
- Enrollment
  - Adding a biometric identifier to the database
- Verification (1:1)
  - Matching against a single record
  - Answers “Am I whom I claim to be?”
- Identification (1:N)
  - Matching against all records in the database
  - Answers “Who am I?”

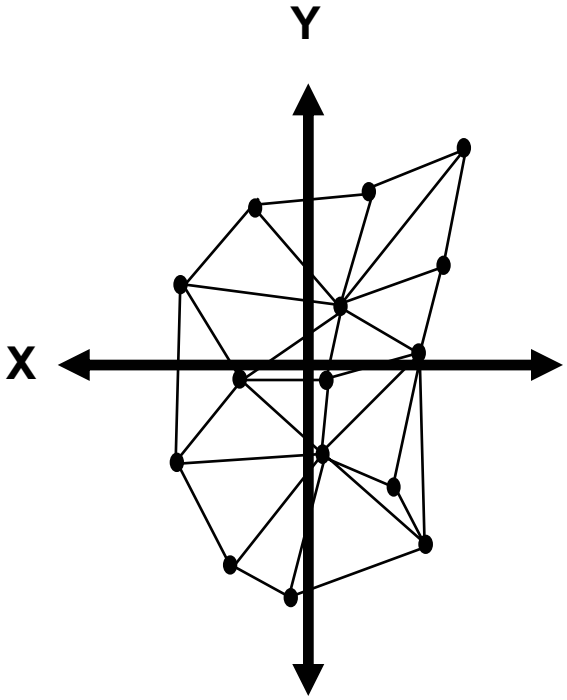
Primitive processes

- Capture
  - Measuring/sampling the raw biometric data using a sensing device
  - Raw data may be a bitmapped image, audio stream, etc.
  - A series of samples may be captured
  - Sometimes includes a quality value
- Processing
  - Converting the raw data into a numeric identifier (generally a binary record)
  - Generally involves “feature extraction”, but can also include other manipulations (sample averaging/weighting, statistics calculations, “cohort lists”, etc.)

Example - finger imaging

Minutiae Based Algorithm





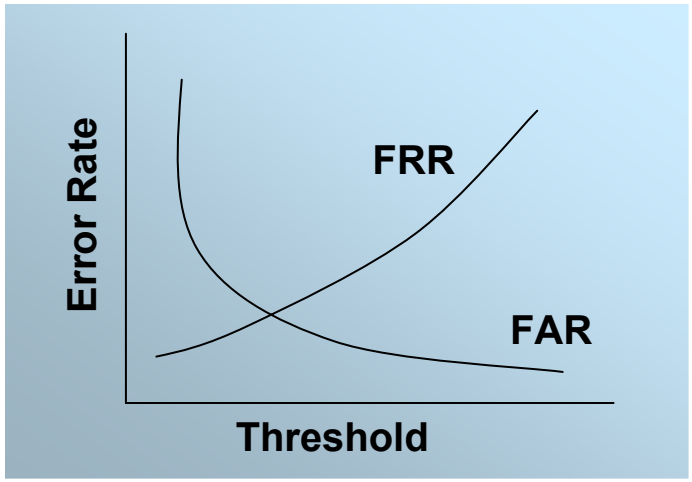
Physical Characteristics **Numerical Result**

Benefits of biometrics

- Convenient - nothing to carry or remember
- Accurate - positive authentication
- Becoming socially acceptable
- Prevents impersonation
  - Protects against identity theft
- Strong authentication
  - System/network access, encryption keys/digital certificates
  - Can't be guessed, stolen, shared, lost, forgotten, written down, forged
- Protects privacy
- Provides audit trail
- Inexpensive
- Biometrics link the event to a particular individual, not just to a password or token, which may be used by someone other than the authorized user

Accuracy

- Generally defined in terms of two parameters:
  - False Rejection Rate (FRR):
    - Measures how often an authorized user, who should be recognized by the system (granted access), is not recognized
    - Also called “False Non-Match Rate”
  - False Acceptance Rate (FAR):
    - Measures how often a non-authorized user, who should not be recognized by the system, is falsely recognized (and granted access)
    - Also called “False Match Rate”
  - Equal Error Rate (EER):
    - Point where FRR = FAR
- FAR/FRR inversely related



Thresholds

- Types of thresholds
  - System threshold
    - Single default threshold applied to all matches
  - Individual threshold
    - Different threshold applied to each subject
  - Dynamic threshold
    - Threshold set as a function of conditions
- Can have separate thresholds for 1:N and 1:1
- Threshold setting single most important settable system parameter
  - Access to tuning of this value should be carefully considered

Additional quality measurement

- Failure to Enroll Rate (FER)
  - Measures how often users are unable to enroll a biometric record
    - Physical characteristic of user prevents creation of template
    - User is not capable or willing to present biometric properly
    - Sensitive to demographics of user population

Adaptation

- Model/template adaptation
  - Upon a successful match, the biometric technology module/engine may return an updated template
  - Generally combines old + new data
  - Keeps registered enrollment data “fresh”
  - Accommodates change in measured characteristic over time
  - Examples:
    - Aging of face/voice
    - Changes in writing style

Biometric system requirements

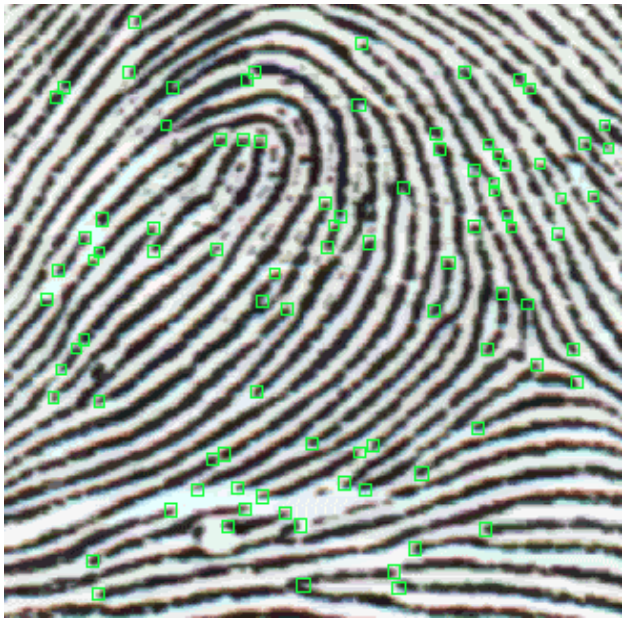
- What do I need to make it work?
  - Capture device
    - Finger scanner, microphone, video camera
  - Algorithms
    - Processing (feature extraction)
    - Matching (1:1 or 1:N comparisons)
  - Repository
    - Database to store enrolled biometric identifier records (for later comparison)
    - Should be protected (secure area, encrypted)

Fingerprints

- Measures characteristics associated with the friction ridge pattern on the fingertip
- One of the oldest and most used technologies
- Capture techniques
  - Ink & paper, “inkless” - with subsequent scan
  - Electronic: single digit flat scan, “10-printers” (rolled)
- Sensor types
  - Optical
  - Silicon chip
    - Capacitive, thermal, e-field
  - Ultrasonic

Fingerprints (cont'd)

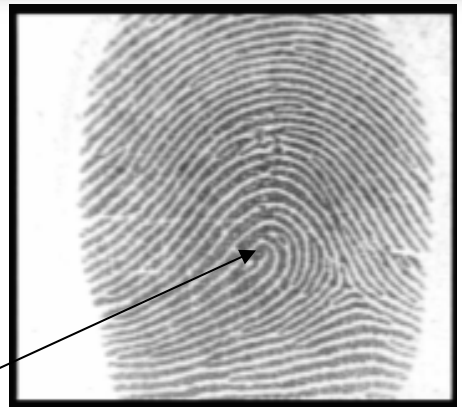
- Two general algorithm categories
  - Minutiae based
    - Maps the points where individual ridges start/stop or bifurcate (branch)
  - Image based
    - Aligns and "overlays" images to determine similarity
- Other measurements
  - Pattern type
  - Ridge counts
  - Distance between ridges
  - Pores



Fingerprint patterns

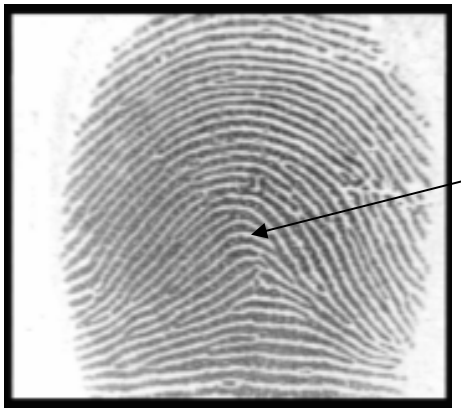
Whorl:
Ridges form a closed center

Core



Loop:
Ridges enter and exit from the same side of the finger. Sub classified by entry side - right or left

Arch:
Ridges enter from one side of the finger and exit the other side.



Core:
The highest point on the ridge with the maximum curvature

Sample fingerprint devices

Fingerprints (cont'd)

- Features
  - Long time use - proven
  - Relatively high accuracy
  - General ease and speed of use
  - Wide variety of applications
  - Numerous vendor selection
- Considerations
  - Requires dedicated device
  - Small % of population have poor prints due to injury, disease, or occupation
  - Some lingering criminal connotation
  - Overt action generally required
  - 250 - 1KB identifier

Requirements Definition

- #1 - first define the problem you are trying to solve
  - results you are trying to achieve
- Requirement come in various forms and sources
  - Tasking from management, other departments, marketing
  - Customer solicitation
  - May need to be elicited
- Requirements state WHAT not HOW

Customer service

Audit

Security

Deter theft

Reduce fraud

Terrorist surveillance

Convenience

Track inmates

Find missing children

Speed processing

Requirements Definition

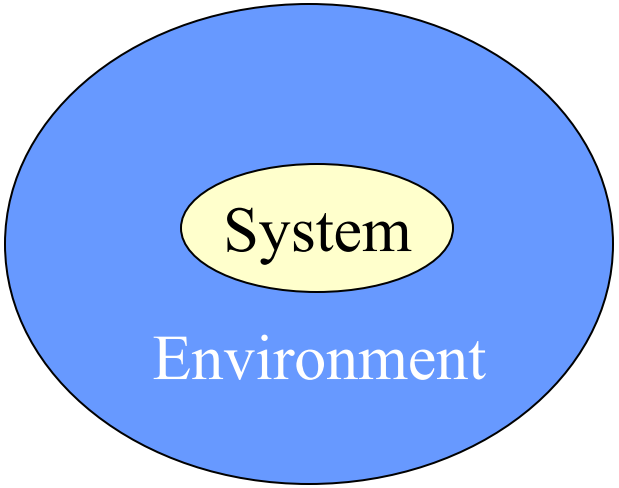
- Types of requirements
  - Physical (size, weight, material)
  - Functional (must do this, that)
  - Performance (how fast, how accurate)
  - Quality (reliability, workmanship, supportability)
- Good requirements
  - Clear, concise
  - Unambiguous
  - Testable (verifiable)

-- Written down, tracked
-- Agreed to by accepter

How do you know when you're done?

Requirements Definition

- Identify constraints
  - Environment
  - Interfaces
  - Legacy systems
  - Budget (initial + life cycle)
  - Standards
  - Physical
  - Personnel
  - Political/social/cultural/legal



Biometric Requirement Considerations

- Accuracy (FAR/FRR trade-off)
- Poor candidates/poor enrollments
- Interference sources
- Scalability
- DB size
- Response time
- Simultaneous requests
- Data protection/encryption
- Save or pitch raw data?
- Multiple biometrics?
- Interoperability/interchange
- Deployment considerations
  - Indoor/outdoor
  - Geographically dispersed (remote enrollment?)
- How tell if system working
- Use of standards
- Privacy issues
- Training
- Platform considerations
- Device issues
- Human factors

Biometric Requirements

- Know your
  - User population
  - Environment
  - Application
- Address the exception cases
  - How do I handle a false reject? A poor enrollment?
    - How do I detect a false accept?
  - What do I do with a subject with a poor biometric?
  - What happens if the device fails?
  - What if the person's biometric is temporarily unavailable (injury, laryngitis, etc.)

Biometric Project Risks

- Technology impacted by user behavior and environment
- System components new and unproven
- User perceptions can have unexpected impact
- Unrealistic expectations by stake holders
- Enrollment logistics
- Response times
- Vague requirements

- PLUS - all normal system development project risks

Biometric Planning Considerations

- Education/awareness campaign prior to roll out
  - Perception dependent on how technology is introduced
- Have privacy policy in place in advance
- Need whole solution, not just hardware and software
- Early testing
- Set expectations
- Know target environment
- Agreement from customer on requirements/design
- Enrollment plan

Consider alternatives to biometrics

- Identification numbers or aliases
- Long term secrets
  - "Mother's Maiden Name"
  - Passwords
- Identification cards/badges
  - Descriptive information (biometric?)
  - Signature
  - Photograph
- Smart Cards
- Challenge/Response systems
- Digital Certificates
- Security guards
- Keys

Reasons to choose biometrics

- Convenient - user always has it
- Accurate - positive authentication
- Becoming socially acceptable
- Prevents impersonation - protects identity
- Strong authentication
  - System/network access, encryption keys/digital certificates
- Protects privacy
- Audit trail
- Inexpensive