Understanding Biometric Technology

International Biometric Industry Association

December 5, 2005

IBIA International Biometric Industry Association

About IBIA

- Non-profit trade association based in Washington, D.C.
- Chartered under Section 501(c)(6) of the U.S. Tax Code
- Advances the collective interests of the biometrics industry
- Members include leading biometric manufacturers, integrators and solution providers

Biometric Overview

- What are Biometrics?
  - Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristics.

  - Examples of Biometric Types:

    - Fingerprint
    - Face
    - Iris
    - Hand
    - Signature
    - Retina
    - Speech
    - Keystroke
    - Palm
    - Veins
    - DNA
    - Skin

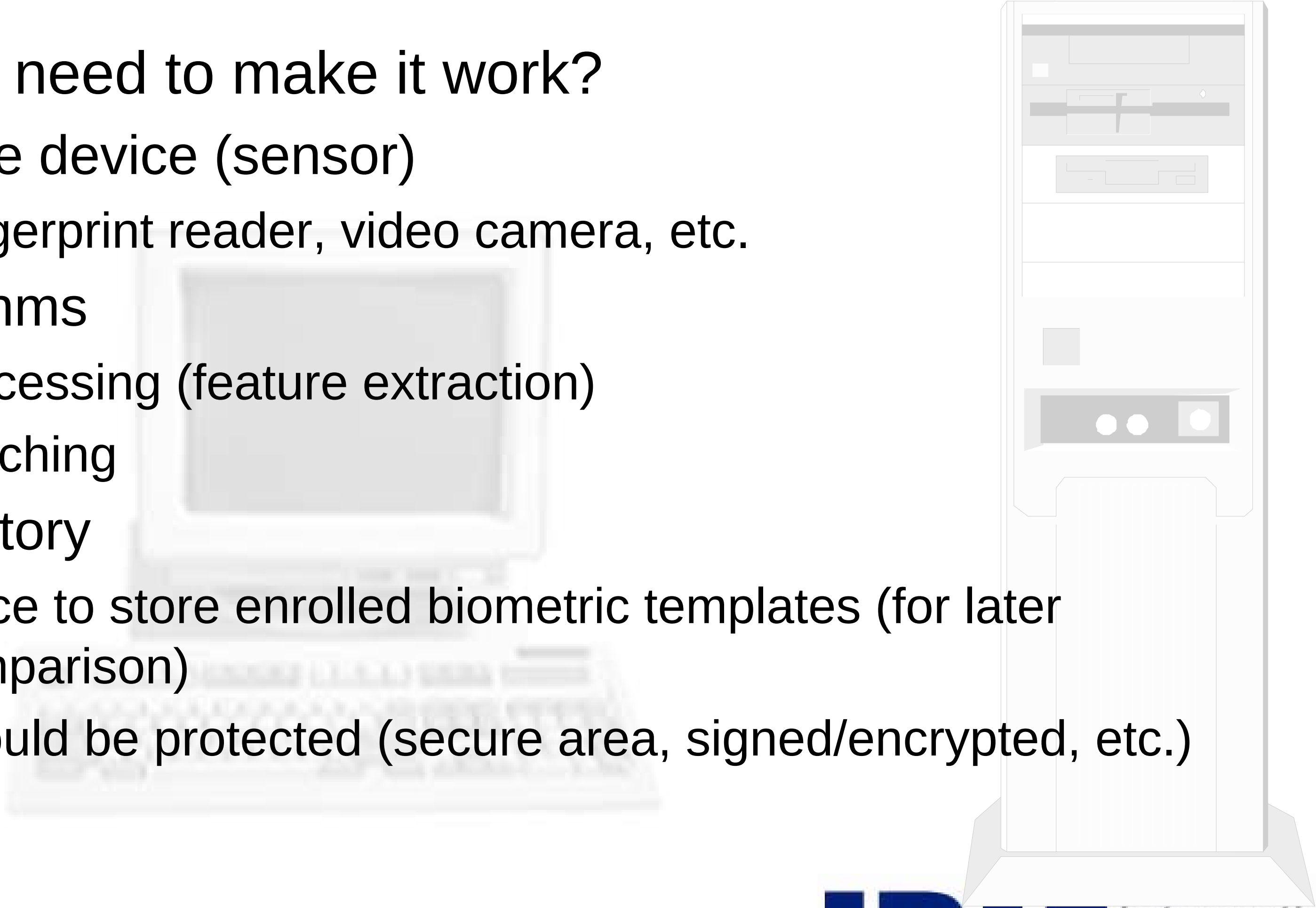
Benefits of biometrics

- Biometrics link an event to a particular individual - not just to a to a password or token
- Convenient – nothing to remember
- Can’t be guessed, stolen, shared, lost, or forgotten
- Prevents impersonation
  - Protects against identity theft
  - Higher degree of non-repudiation
- Enhances privacy
  - Protects against unauthorized access to personal information
- Complementary with other authentication mechanisms
  - Smart cards
  - Public Key Infrastructure

Example Uses of Biometrics

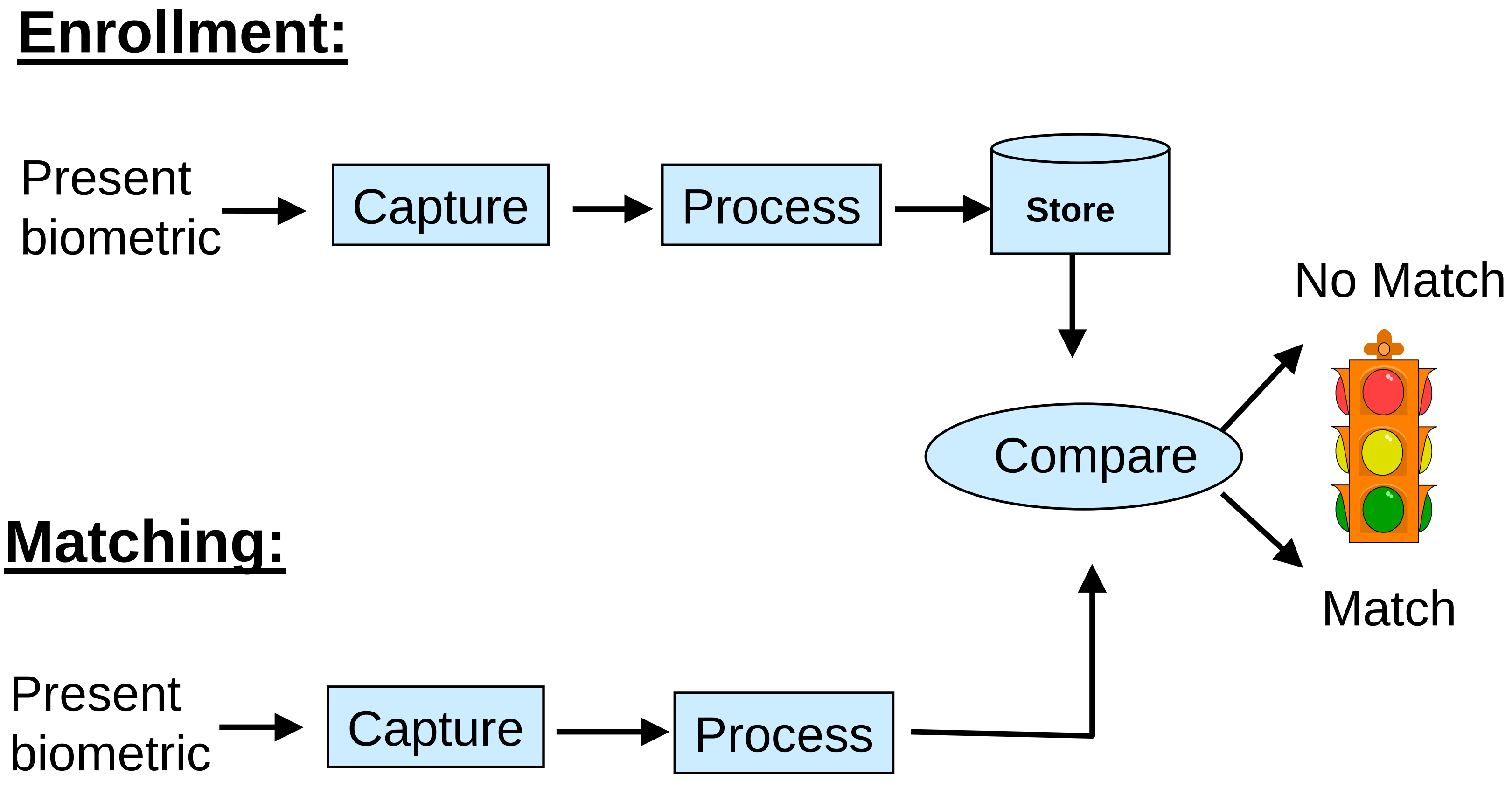
- Commercial
  - Access to facilities and information systems
  - Employee timekeeping
  - Retail point-of-sale transactions
- Law enforcement
  - Investigations
  - Forensic analysis
- Civil systems
  - Border and immigration control
  - Entitlement benefit eligibility screening and verification

Biometric system components



- What do I need to make it work?
  - Capture device (sensor)
    - Fingerprint reader, video camera, etc.
  - Algorithms
    - Processing (feature extraction)
    - Matching
  - Repository
    - Place to store enrolled biometric templates (for later comparison)
    - Should be protected (secure area, signed/encrypted, etc.)

How do biometrics work?



Enrollment:

Present biometric → Capture → Process → Store

Matching:

Present biometric → Capture → Process → Compare

Compare

No Match

Match

IBIA International Biometric Industry Association

Three Basic Functions

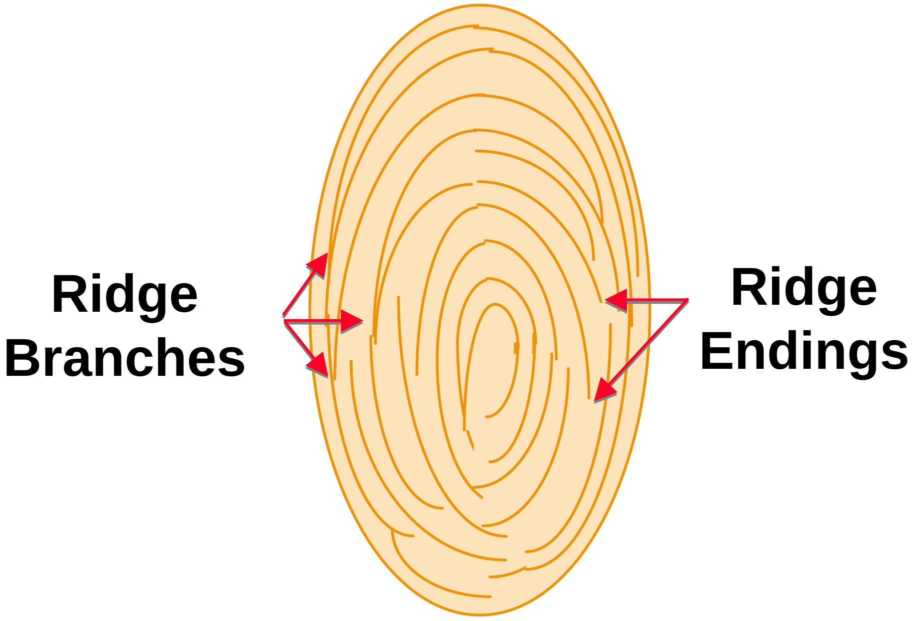
- Enrollment
  - Adding biometric information to a data file
    - Can include screening for duplicates in database
- Verification (one-to-one)
  - Matching against a single record
  - Answers “Is this person who they claim to be?”
- Identification (one-to-many)
  - Matching against all records in the database
  - Answers “Do we have a record of this person?”

Sub-Functions Common to Most Biometrics

- Capture
  - Measure biometric characteristic using a sensing device
  - Data may be a bitmapped image, audio stream, etc.
  - A series of samples may be captured
  - Sometimes includes a quality value
- Process
  - Converting the data into a numeric identifier (template)
  - Generally involves “feature extraction”, but can also include include other manipulations

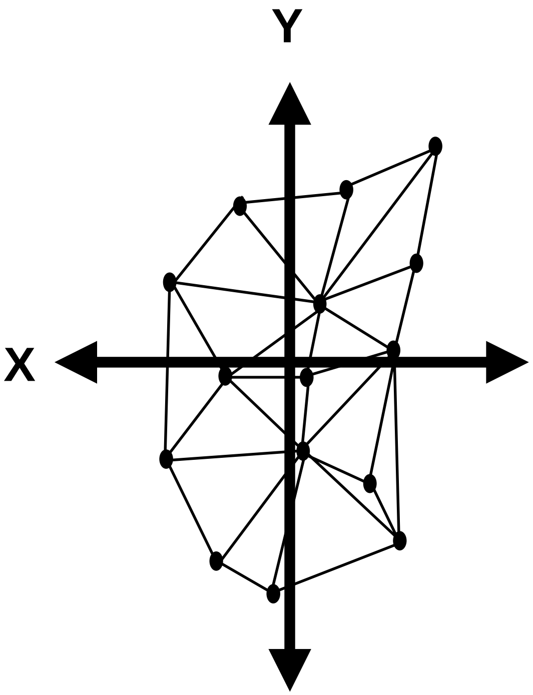
Example

Minutiae Based Fingerprint Algorithm


Ridge Branches

Ridge Endings

Image



Template

IBIA International Biometric Industry Association

Sub-Functions (cont’d)

- Match
  - Comparing a processed biometric template to a previously enrolled biometric template(s) to determine level of similarity
    - Many methods (types of algorithms) used
  - Output of match process is a score
    - Probability of match (i.e., belonging to the same subject)
- Decision
  - Determination of match results
  - Match results compared against a threshold score
    - Above threshold = Match
    - Below threshold = No-match

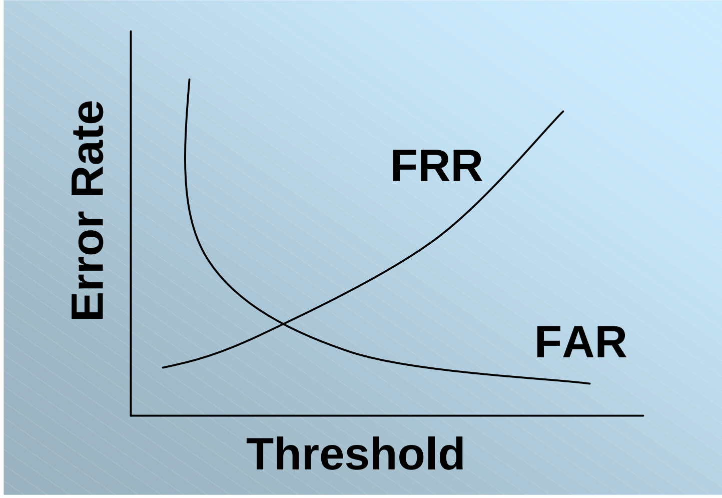
Accuracy

- Generally defined in terms of two parameters:
  - False Reject Rate (FRR):
    - Measures how often an authorized user, who should be granted access, is not recognized
    - FRR = Percentage of false rejections of the total number of of valid recognition attempts
    - Also called “False Non-Match Rate”
  - False Accept Rate (FAR):
    - Measures how often a non-authorized user, who should not not be granted access, is falsely recognized
    - FAR = Percentage of false acceptances of the total number number of imposter recognition attempts
    - Also called “False Match Rate”

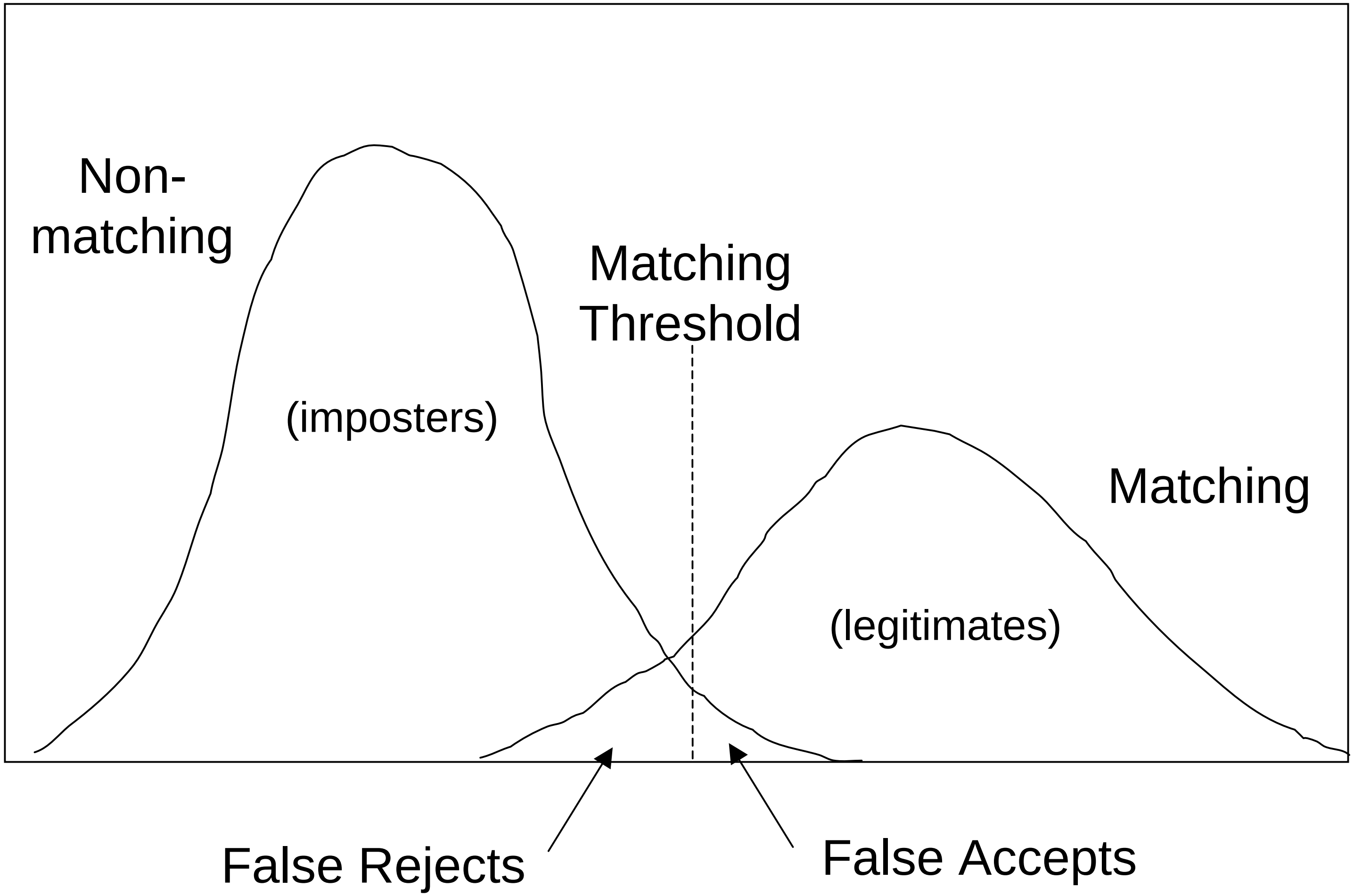
Accuracy (cont'd)

- Equal Error Rate (EER):
  - Point where FRR = FAR

- FAR/FRR are inversely related



Score distribution



Additional Performance Consideration

- Failure to Enroll Rate (FTER)
  - Measures how often users are unable to enroll a biometric biometric characteristic
    - Physical characteristic of user prevents creation of template template
      - Characteristic not present or obscured
    - User is not capable or willing to present biometric properly
- FTER = Percentage of failures to enroll of the total number of enrollment attempts

What Makes a Good Biometric?

- Unique
- Permanent
- Easy to use
- Fast
- Accurate
- Low cost
- Positive public perception

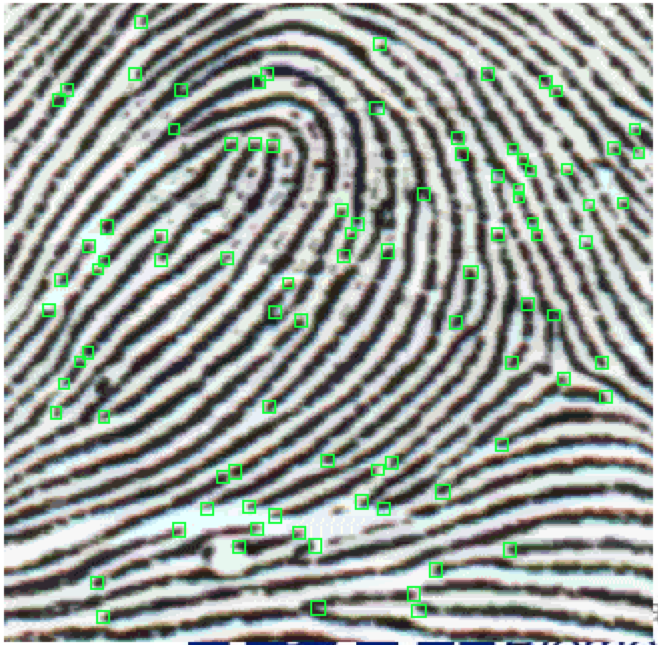
Biometric

Fingerprints

- Measures characteristics associated with the friction ridge ridge pattern on the fingertip
- One of the oldest and most widely used biometrics
- Capture techniques
  - Flat scan or swipe across
  - Rolled (“ten print”)
  - Slap (four flat fingers at a time)
- Sensor types
  - Optical
  - Silicon
  - Ultrasonic

Fingerprints (cont'd)

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



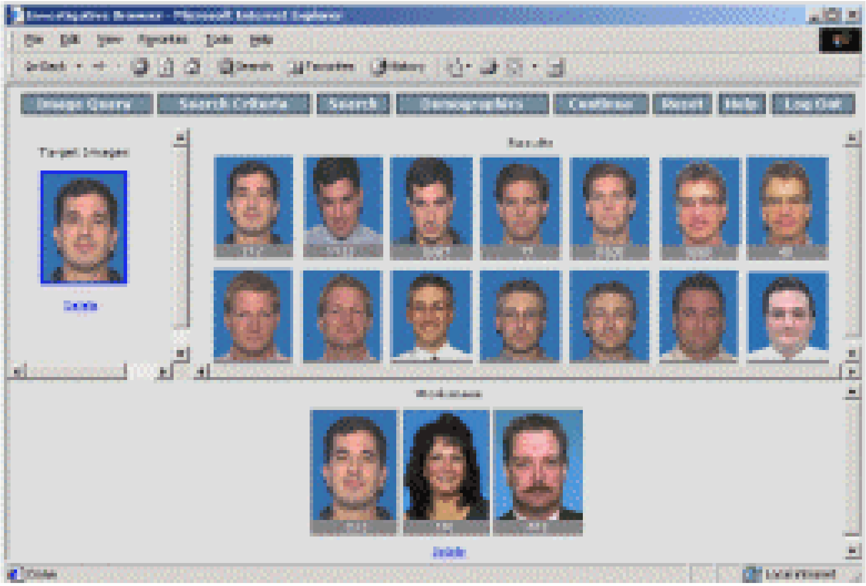
Fingerprints (cont’d)

- Features
  - Long time use - proven
  - High accuracy
  - General ease and speed of use use
  - Supports both 1:1 verification and 1:N identification applications
  - Numerous vendor selections

- Considerations
  - Small % of population have poor prints due to injury, age, disease, or occupation
  - Requires physical contact with with sensor
  - Historical association with law law enforcement

Facial recognition

- Analyzes geometry of the face or the relative distances between features (e.g., nose and mouth)
  - Can combine geometry features with skin texture
- Algorithm categories
  - Local feature analysis
  - Eigenfaces
  - Neural networks
  - Surface texture analysis (skin)
- Capture methods
  - Still camera
  - Video
  - Thermal imaging



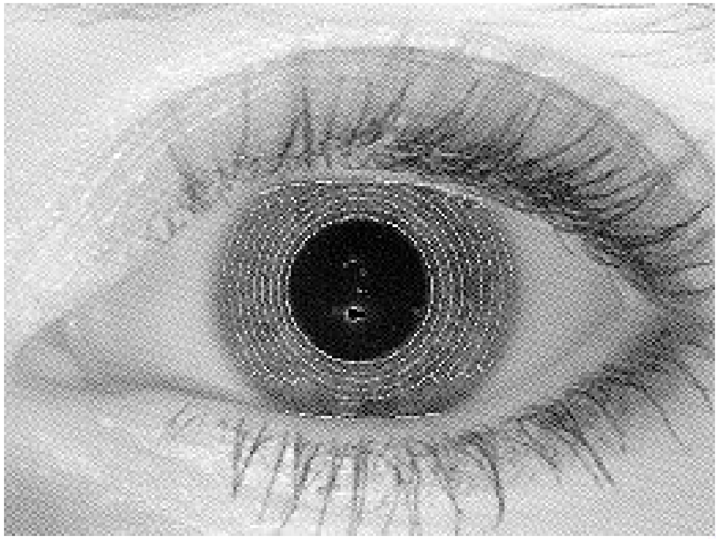
Facial recognition (cont’d)

- Features
  - Can use standard video cameras cameras
  - No physical contact required
  - Supports both 1:1 verification and and 1:N identification applications applications
  - Can be used with previously compiled photo databases
  - Can be fused with skin biometrics biometrics to enhance accuracy

- Considerations
  - Can be affected by lighting
  - Sometimes affected by eyeglasses, facial hair, or expression
  - Appearance can change over time

Iris recognition

- Measures features associated with the random texture of the the colored part of the eye
- Measures up to 266 unique features
- Uses near infrared sensor from a distance of 6 in. to 2 ft.
- Popular for facility access and transportation/border security



Iris recognition (cont'd)

- Features
  - Highly accurate
  - Very stable over lifetime
  - Works through glasses and contacts
  - No physical contact required
  - Not affected by common eye surgeries
  - Supports both 1:1 verification and 1:N identification applications

- Considerations
  - Can be affected by some eye eye diseases (cataracts)
  - Often confused with more invasive retinal scanning

IBIA International Biometric Industry Association

Hand geometry

- Measures dimensions of hand, including shape and length of fingers
- Used extensively for physical access control
  - High-traffic doors
  - All U.S. nuclear power plants
  - DoD
  - Airports
- Widely used for employee timekeeping
- Hand reader configuration
  - Typically lay hand flat
  - Pegs guide placement
  - Camera positioned above and to side

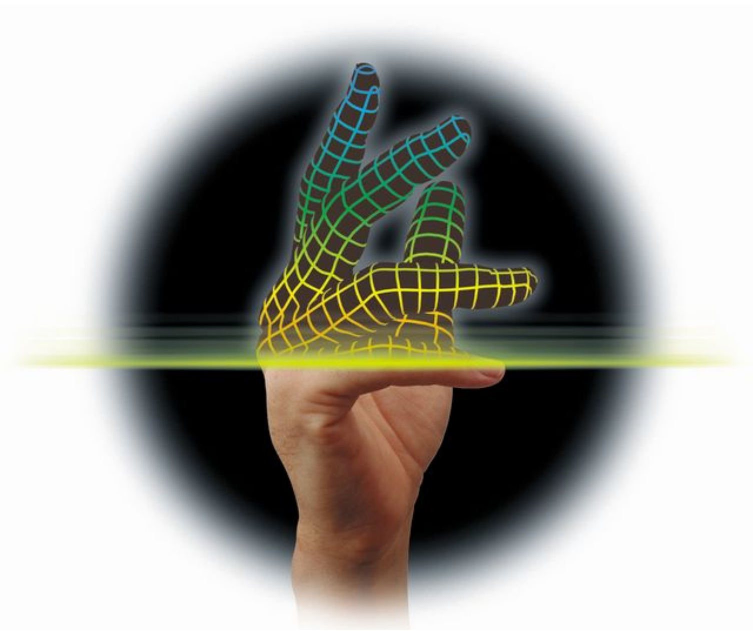
Access Control Terminal

IBIA International Biometric Industry Association

Hand geometry (cont'd)

- Features
  - Easy to use, fast
  - High public acceptance
  - Very low Failure to Enroll Rate
  - Proven over many years of use
  - Primary applications are physical access and time/attendance
  - Very small, adaptive template
    - Fits on any card media
  - Works well in outdoor environments
  - Rugged

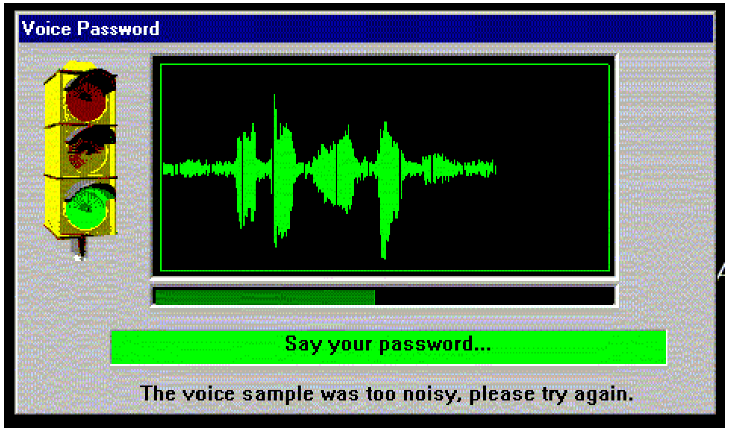
- Considerations
  - Best used in 1:1 contexts



IBIA International Biometric Industry Association

Speech verification

- Compares live speech with previously created speech model of of person’s voice
- Measures pitch, cadence and tone to create voice print
- Uniqueness based on vocal tract differences
  - Length, shape of mouth, nasal cavities, etc.
- Can be text dependent or independent
- Behavioral & physiological biometric
- Not speech recognition



Say your password...

The voice sample was too noisy, please try again.

Speech verification (cont'd)

- Features
  - Can use standard microphone or telephone handset
  - Can use existing audio channels, such as telephone lines
  - Can be combined with challenge/response techniques
  - Algorithms typically language independent

- Considerations
  - Background noise can interfere
  - Can be affected by illness or stress
  - Best when using similar instruments for enrollment and verification
  - Best used in 1:1 contexts

IBIA International Biometric Industry Association

Dynamic signature verification

- Measures characteristics of handwritten signatures
  - Shape, speed, pressure, pen angle, sequence, etc.
- Devices:
  - Signature or graphics tablets
  - Special pens
- Behavioral biometric
- Intended for point-of-sale applications

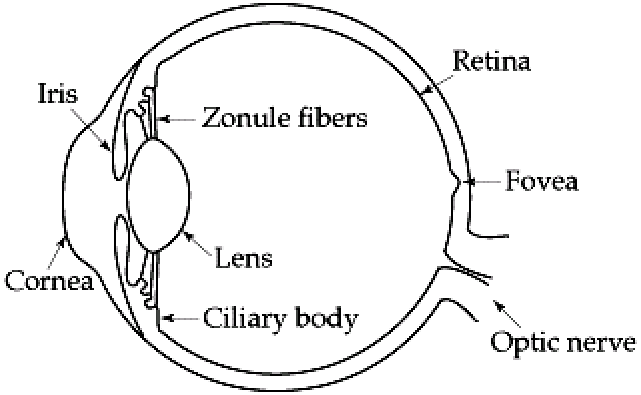
Dynamic Signature Verification (cont’d)

- Features
  - Works in conjunction with familiar signing process
  - Can be used with devices that have built-in graphics components - PDAs, PDAs, etc.

- Considerations
  - Can be affected by behavioral factors (stress, distractions, standing/sitting) standing/sitting)
  - Periodic update (adaptation) of templates may be necessary due to changes over time
  - Best used in 1:1 contexts

Retinal scanning

- Measures the blood vessel patterns at the back of the eye
- Light source is shone through the pupil to illuminate the retina retina
- Generally used for high-end security applications, primarily for for physical access control
- First commercial system available in 1984
- Not iris recognition



IBIA International Biometric Industry Association

Retinal scanning (cont'd)

- Features
  - High accuracy/stability
  - Clear contacts usually not a problem
  - Supports both 1:1 verification and 1:N 1:N identification applications

- Considerations
  - Generally considered intrusive; uncomfortable user interface
  - Requires removal of eyeglasses
  - Capture can take 10-15 seconds
  - Not commercially marketed

Keystroke dynamics

- Also known as “typing rhythm” or “typing pattern”
- Analyzes the way a person interacts with a computer keyboard keyboard
- Measures variables such as key depression time (duration), latency between keystrokes, inter-keystroke times, typing error error frequency, force keystrokes, etc.
- Generally used in conjunction with passwords/pass-phrases
- Behavioral biometric

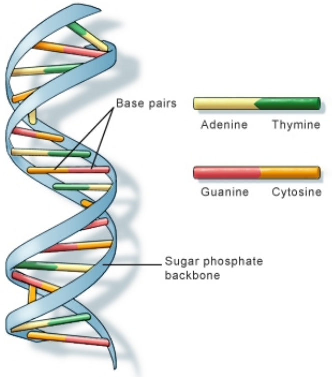
Keystroke dynamics (cont’d)

- Features
  - No special capture device required (low cost)
  - Leverages existing infrastructure (hardware and process)
  - Text dependent
  - Can be transparent to the user
  - Pass phrase text can be changed

- Considerations
  - Not suitable for non-touch typists typists (too inconsistent)
  - Pass phrase should be at least 8 8 characters long
  - Periodic update (adaptation) of templates may be necessary due due to changes over time
  - Enrollment process somewhat lengthy (15 captures)
  - Affected by “typos” and changes changes in typing patterns

DNA

- Deoxyribonucleic acid is the hereditary material in humans and almost all other organisms
- Chemical found in the nucleus of all cells
- Persistent throughout life and beyond
- Used primarily in criminal forensic investigations and in resolving questions of paternity/heredity
- Identification application uses consistent portion of DNA strand for measurement (CODIS system)
- DNA can be stored in a database



U.S. National Library of Medicine

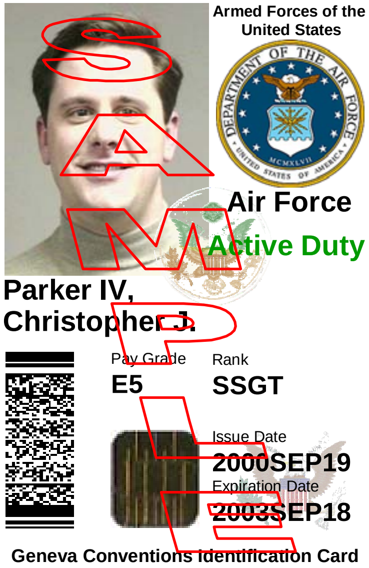
DNA (cont'd)

- Features
  - Highly accurate (one person in 6 billion billion accuracy)
  - Persistent (never changes)
  - Accepted by global justice system
  - Capable of 1:1 verification and 1:N identification applications

- Considerations
  - Requires collection of a DNA sample
  - Not instantaneous – currently takes 12 hours for match result result
  - Research being done to develop "instant" DNA
  - Identical twins share the same same DNA

Biometrics and Smart Cards

- Complementary technologies
- Smart card provides portable and personalized secure storage
  - Local security agent of the issuer
  - Ensures a strong chain of trust for the biometric credential



Armed Forces of the United States

Air Force

Active Duty

Parker IV,
Christopher J.

Pay Grade
E5

Rank
SSGT

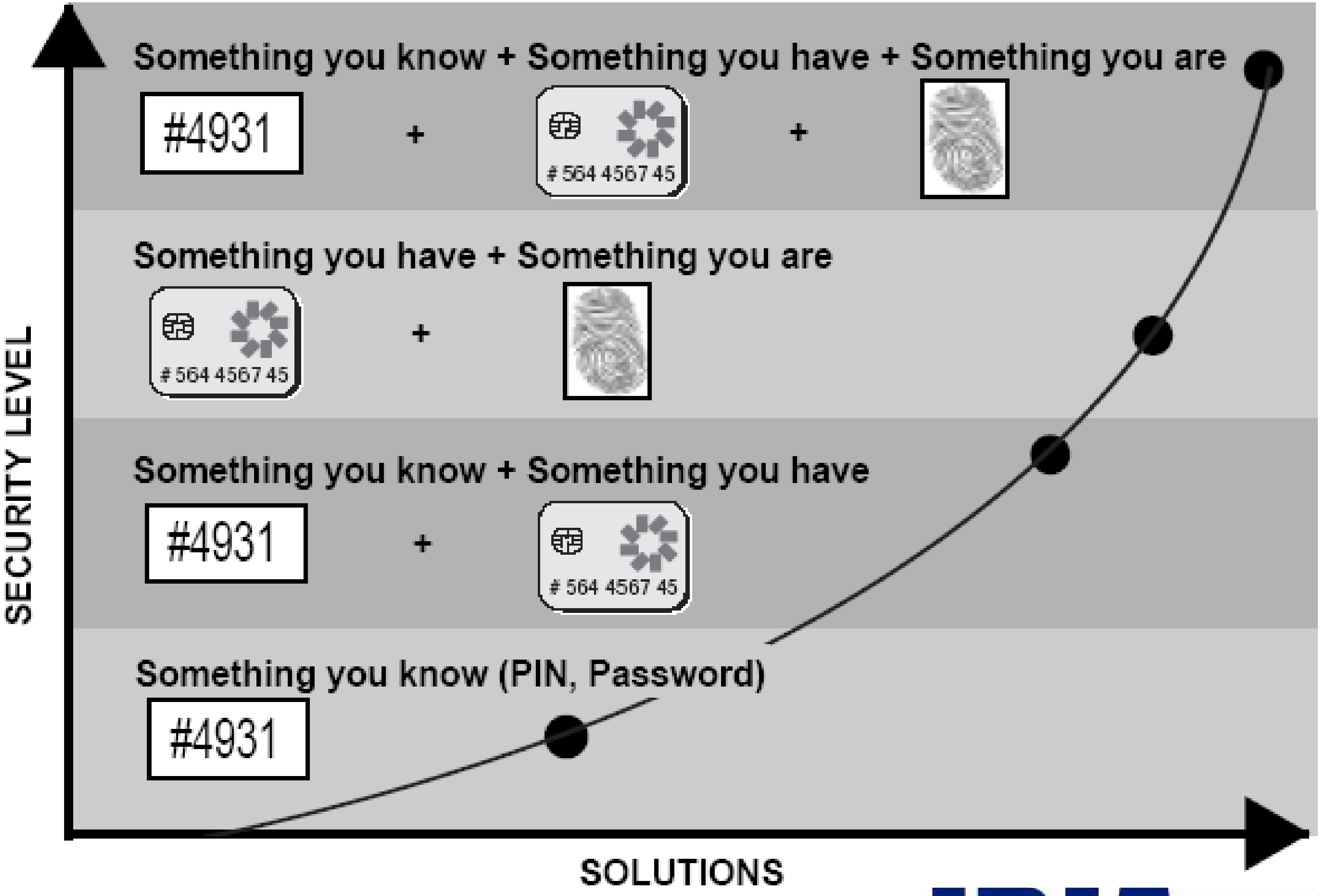
Issue Date
2000SEP19

Expiration Date
2003SEP18

Geneva Conventions Identification Card

IBIA International Biometric Industry Association

Multi-factor authentication


Something you know + Something you have + Something you are
#4931
+
# 564 4567 45
+
Something you have + Something you are
# 564 4567 45
+
Something you know + Something you have
#4931
+
# 564 4567 45
Something you know (PIN, Password)
#4931
SECURITY LEVEL
SOLUTIONS

Source: Smart Card Alliance

December 5, 2005

IBIA International Biometric Industry Association

Biometric Standards

- Biometric interoperability standards do exist and are evolving evolving
  - Application interface
  - Biometric data interchange formats
  - Application profiles (e.g., border security)
- Largely driven by government and industry working in partnership through accredited standards organizations
- Essential for industry growth and widespread adoption

The Future of Biometrics

- Smaller, cheaper, faster, more accurate
- Fusion of multiple biometrics (e.g., face and skin)
- Combination of biometrics with other authentication mechanisms
  - Smart cards and Public Key Infrastructure (PKI)
- Governments are sponsoring widespread adoption
- Public awareness and acceptance is growing
  - Technology will affect a growing percentage of the population population
- Existing standards being expanded and adopted
- Industry focus on privacy and securing biometric data
  - Biometric data protection
  - Device anti-spoofing

For More Information about IBIA

International Biometric Industry Association

The Homer Building
601 Thirteenth Street N.W.
Suite 370 South
Washington, D.C. 20005

Phone (202) 783-7272
Fax (202) 783-4345
www.ibia.org
ibia@ibia.org