An Overview of Biometrics

Dr. Charles C. Tappert

Seidenberg School of CSIS, Pace University

What are Biometrics?

- Biometrics refers to identification of humans by their characteristics or traits
  - Physical traits
    - Fingerprint, Face, Iris
  - Behavioral traits
    - Signature/handwriting, Voice
    - Keyboard and mouse input
  - Websites and videos
    - http://www.biometrics.gov/
    - Biometric Security

Technologies Used in Biometrics

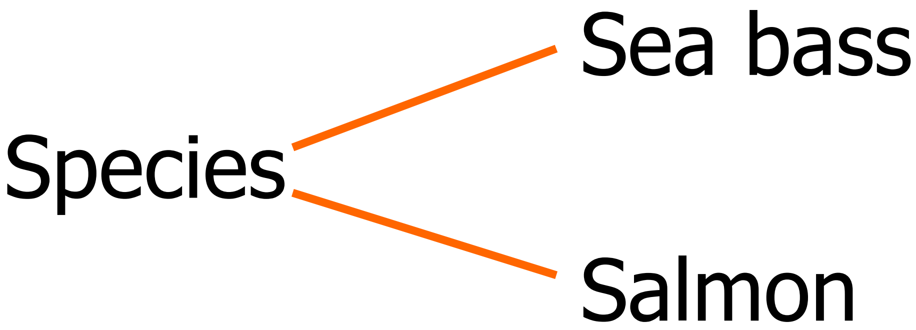
- Pattern Recognition
- Machine Learning
- Artificial Intelligence
- Data Mining
  - Beer and Diapers
  - Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Pattern Recognition
What is pattern recognition?

- The act of taking in raw data and taking an action based on the “category” of the pattern
- We gain an understanding and appreciation for pattern recognition in the real world – visual scenes, noises, etc.
    - Human senses: sight, hearing, taste, smell, touch
- Recognition not an exact match like a password

Pattern Recognition
An Introductory Example

- "Sorting incoming Fish on a conveyor according to species using optical sensing"



Species

Sea bass

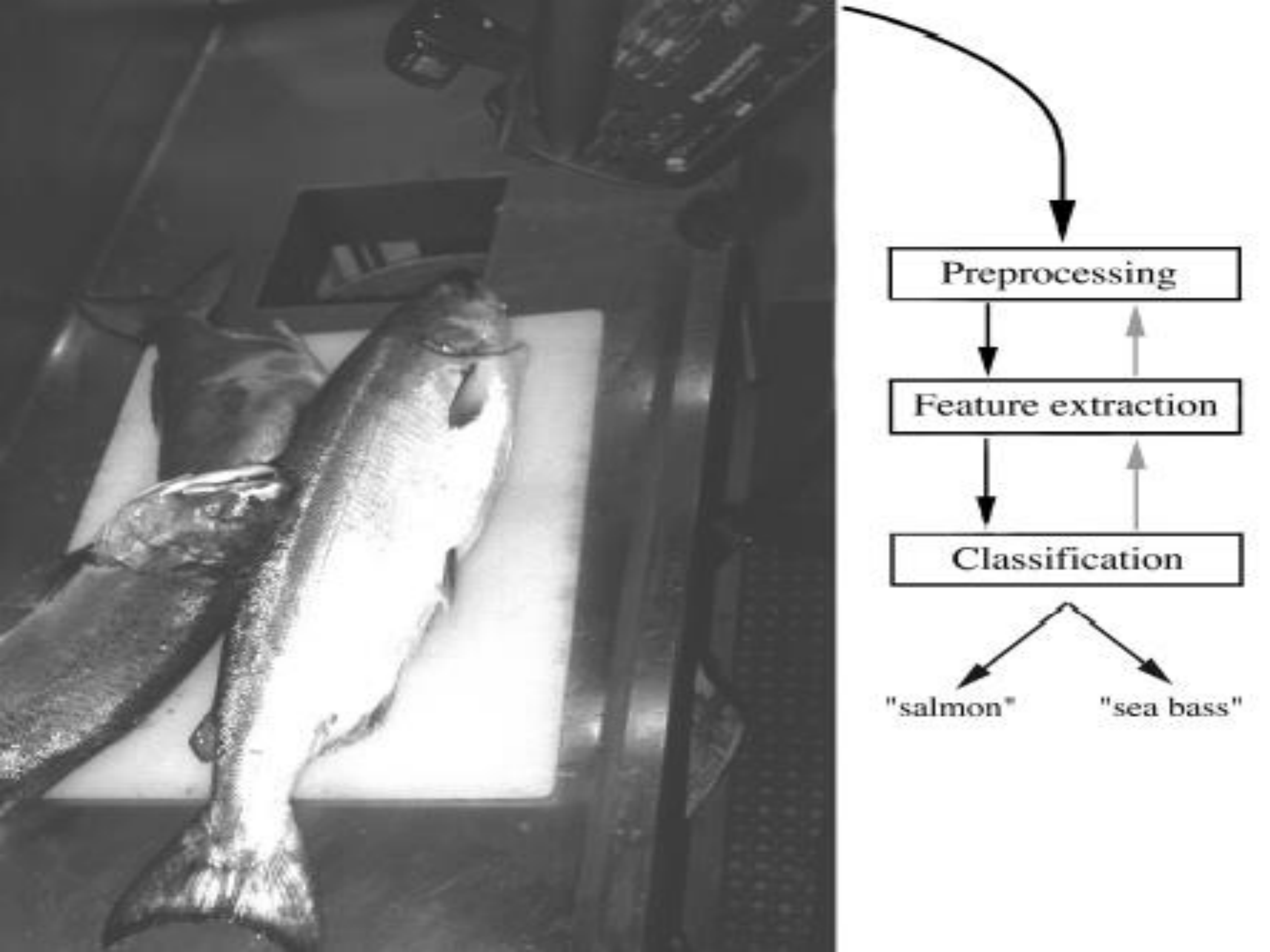
Salmon

Pattern Recognition Problem Analysis

- Set up a camera and take some sample images to extract features
  - Length
  - Lightness
  - Width
  - Number and shape of fins
  - Position of the mouth, etc…

Pattern Recognition
Pattern Classification System

- Preprocessing
  - Segment (isolate) fishes from one another and from the background
- Feature Extraction
  - Reduce the data by measuring certain features
- Classification
  - Divide the feature space into decision regions



Preprocessing

Feature extraction

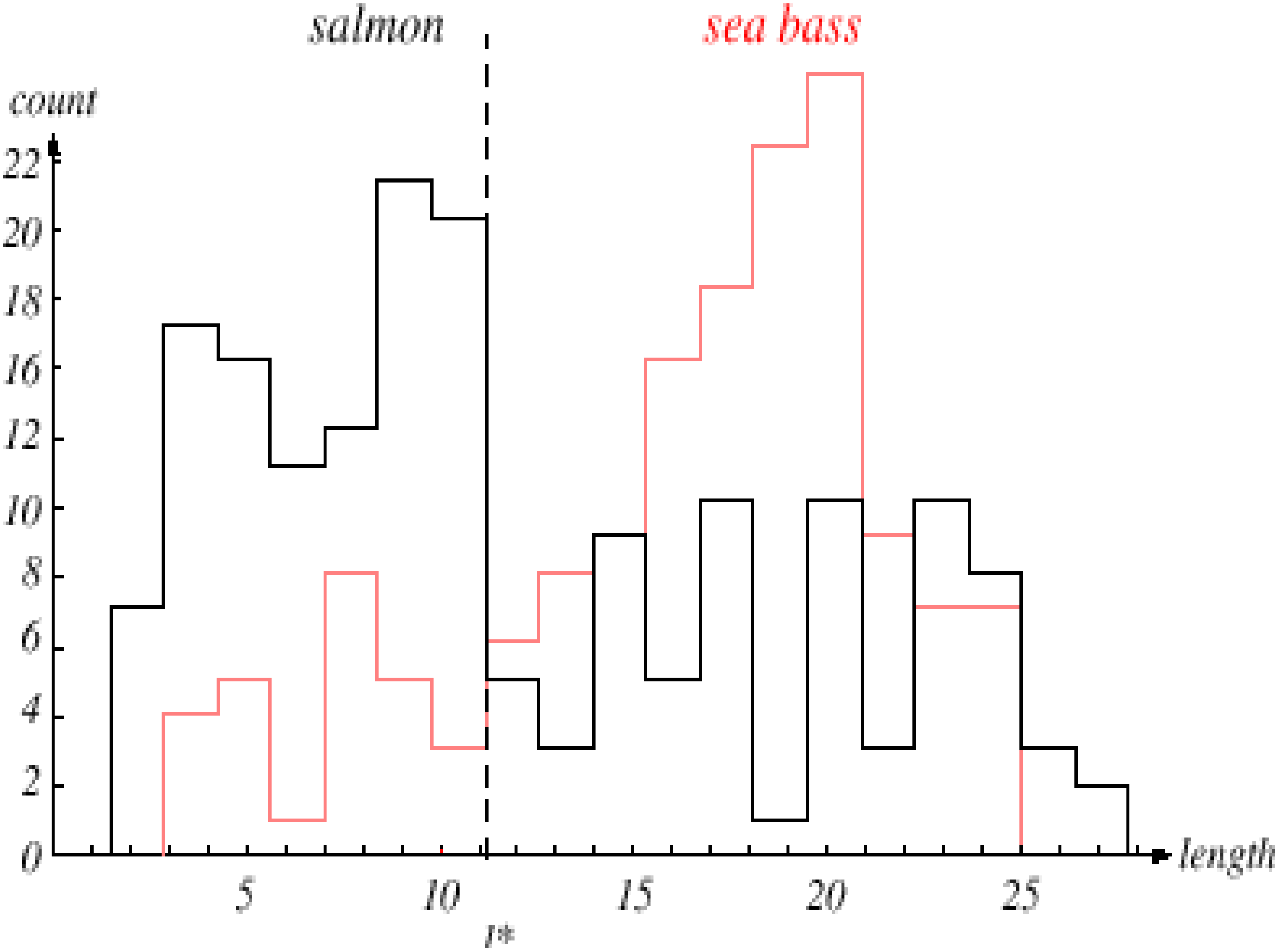
Classification

"salmon"

"sea bass"

Pattern Recognition Classification

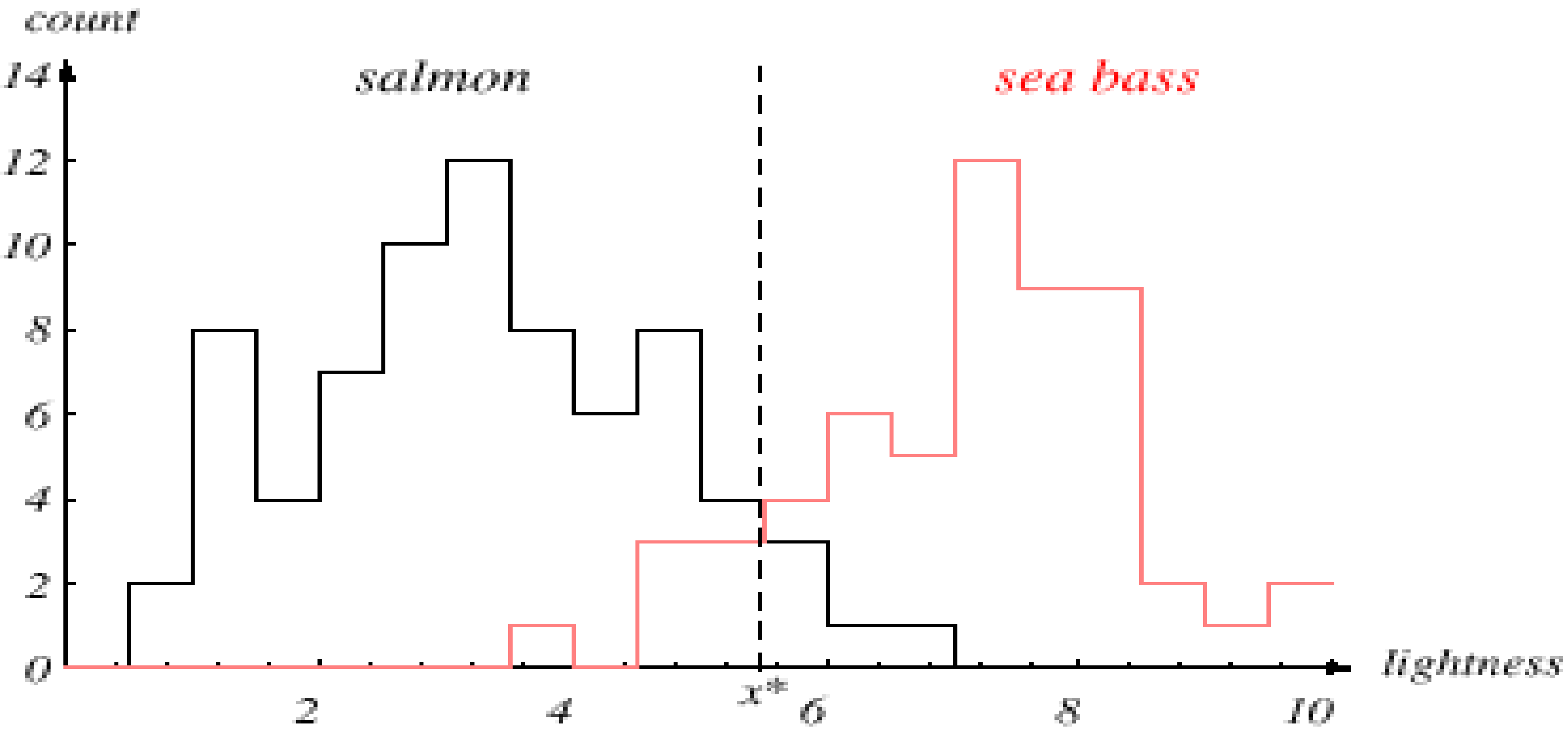
- Initially use the length of the fish as a possible feature for discrimination


salmon
sea bass
count
22
20
18
16
12
10
8
6
4
2
0
length
5
10
15
20
25
l*

Pattern Recognition
Feature Selection

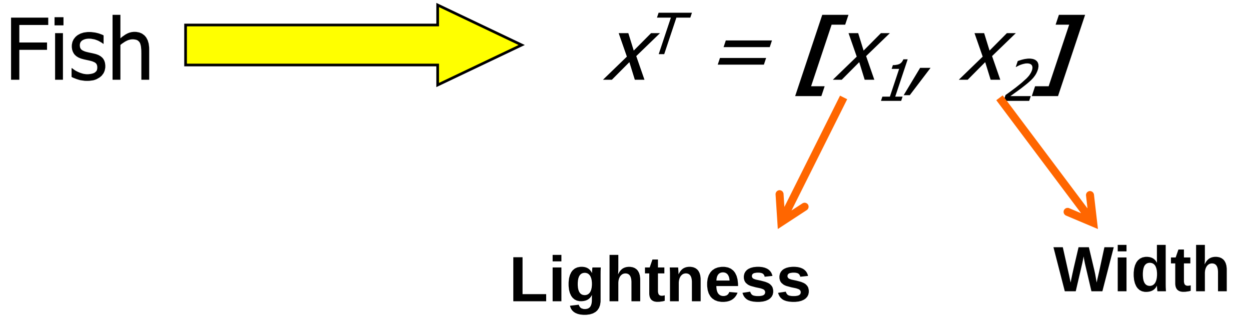
The length is a poor feature alone!

Select the lightness as a possible feature


count
14
12
10
8
6
4
2
0
salmon
sea bass
lightness
2
4
x*
6
8
10

Pattern Recognition
Feature Vector

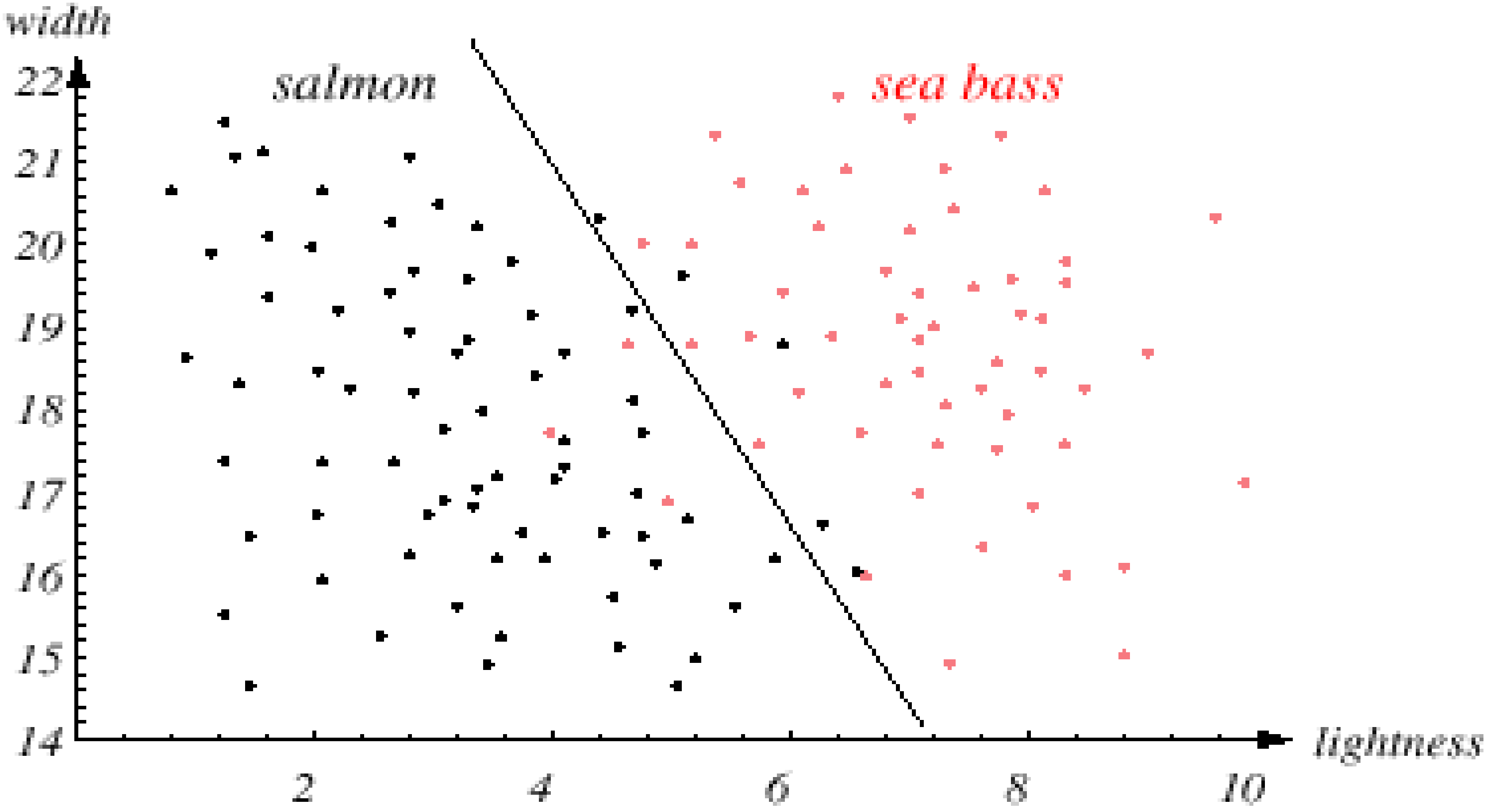
- Adopt the lightness and add the width of the fish to the feature vector



Fish

$x^T = [x_1, x_2]$

Pattern Recognition Straight line decision boundary



Pattern Recognition Stages

- Sensing
  - Use of a transducer (camera or microphone)
  - PR system depends on the bandwidth, the resolution sensitivity distortion of the transducer
  - What A Drone Can See From 17,000 Feet
- Preprocessing
  - Segmentation and grouping - patterns should be well separated and not overlap

Pattern Recognition Stages (cont)

- Feature extraction
  - Discriminative features
  - Ideally invariant wrt translation, rotation, scale
- Classification
  - Use the feature vector provided by a feature extractor to assign the object to a category
- Post Processing
  - Exploit context-dependent information to improve performance

Pattern Recognition
Post Processing – for example, OCR

- The following sentence has many spelling errors. Right click on a word to get suggested correct spelling choices.
- We cant allign teh wonds corektly in htis sentance.
- On right clicking, most of correct spellings of the words are listed as first choice.
- Now, type the sentence above with the spelling errors into Microsoft Word.
- Many of the misspelled words are almost instantaneously auto-corrected.

Back to Biometrics

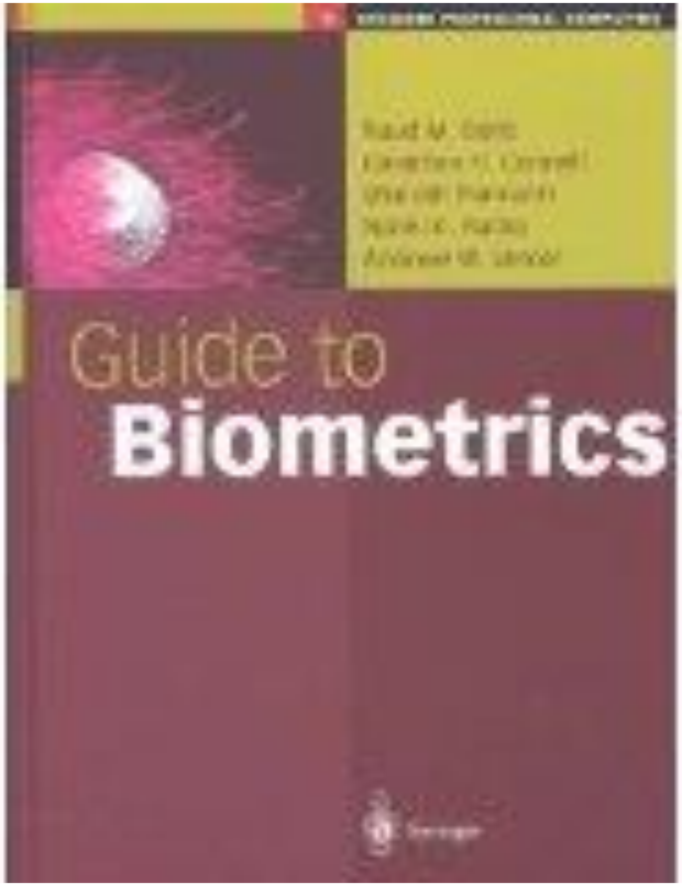
- Michigan State University
- Secret Lock

Biometrics Information Sources

The images and material contained here are from:

- *Guide to Biometrics*
  Bolle, Connell, Pankanti, Ratha, and Senior, Springer 2004

- and our conference/journal/book publications



What is Biometrics?

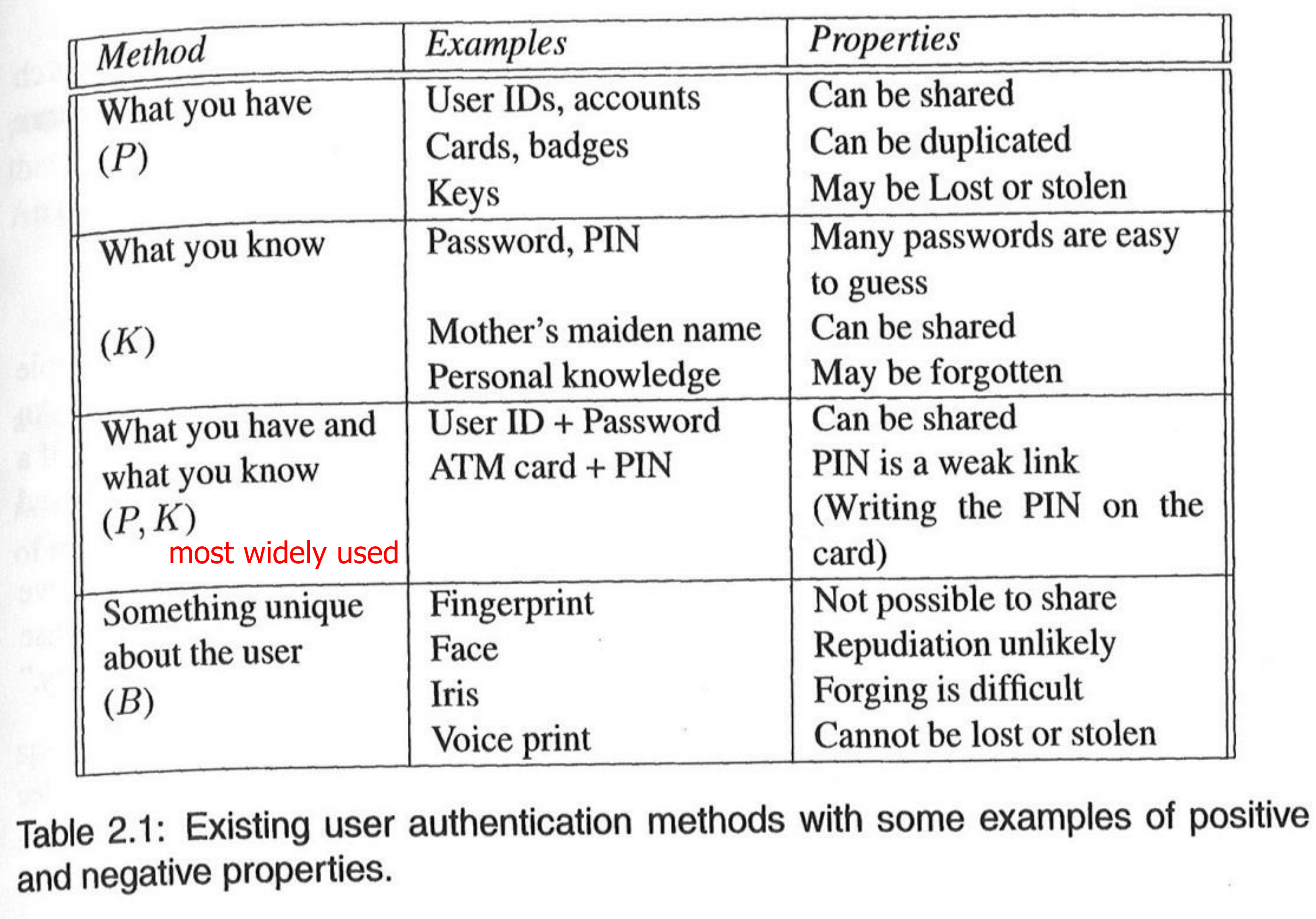
- Definition from Bolle, et al. – the science of identifying, or verifying the identity of, a person based on physiological or behavioral characteristics

- Note: biometric systems employ pattern recognition technology

Traditional Modes of Person Authentication

- Possessions – what you have
  - Keys, passports, smartcards, etc.
- Knowledge – what you know
  - Secret information: passwords, etc.
- Biometrics – what you are/do
  - Characteristics of the human body and human actions that differentiate people from each other

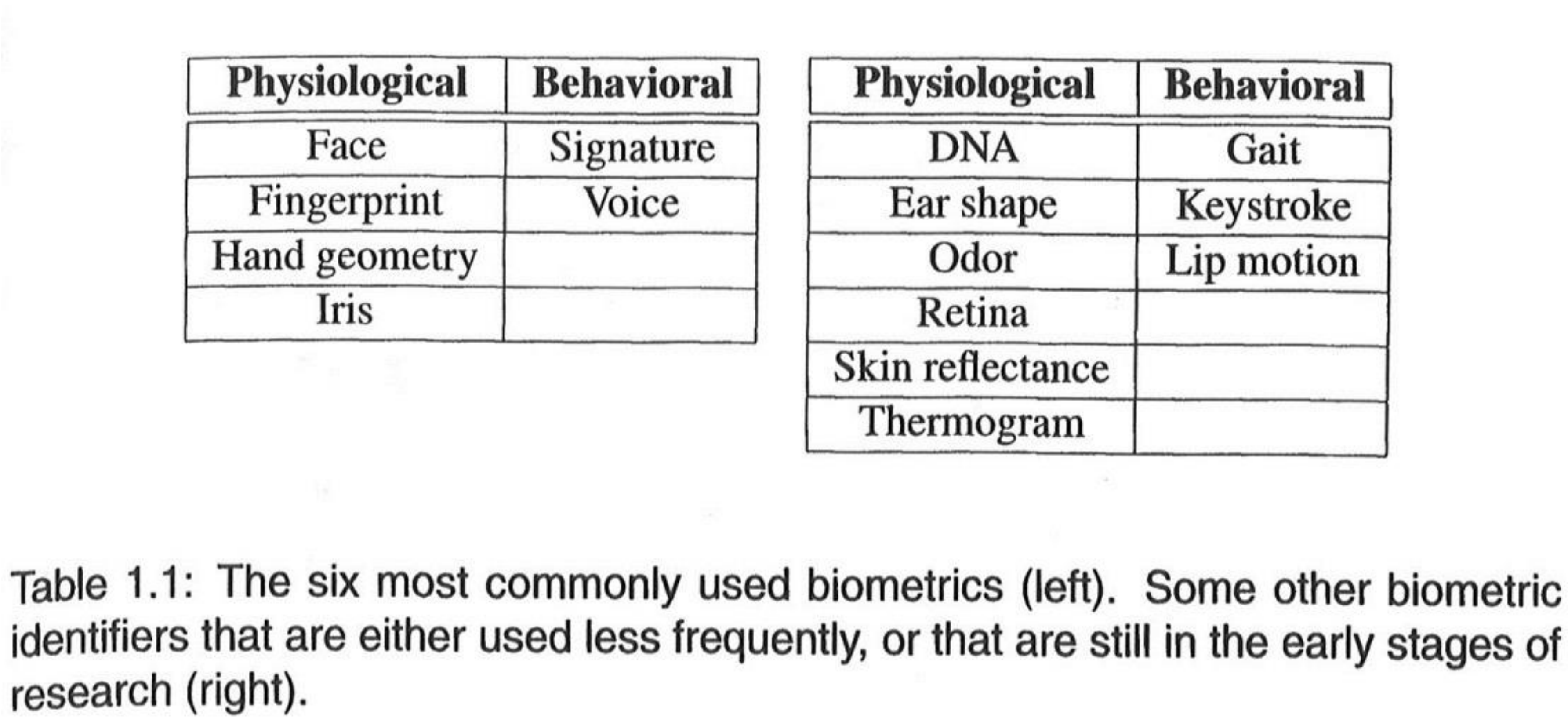
Authentication Methods: Examples and Properties



Method	*Examples*	*Properties*
What you have (P)	User IDs, accounts Cards, badges Keys	Can be shared Can be duplicated May be Lost or stolen
What you know (K)	Password, PIN Mother's maiden name Personal knowledge	Many passwords are easy to guess Can be shared May be forgotten
What you have and what you know (P, K) most widely used	User ID + Password ATM card + PIN	Can be shared PIN is a weak link (Writing the PIN on the card)
Something unique about the user (B)	Fingerprint Face Iris Voice print	Not possible to share Repudiation unlikely Forging is difficult Cannot be lost or stolen

Table 2.1: Existing user authentication methods with some examples of positive and negative properties.

Most Common & Other Biometrics



Physiological	Behavioral
Face	Signature
Fingerprint	Voice
Hand geometry	
Iris	

Physiological	Behavioral
DNA	Gait
Ear shape	Keystroke
Odor	Lip motion
Retina	
Skin reflectance	
Thermogram	

Table 1.1: The six most commonly used biometrics (left). Some other biometric identifiers that are either used less frequently, or that are still in the early stages of research (right).

Attributes Necessary to Make a Biometric Practical

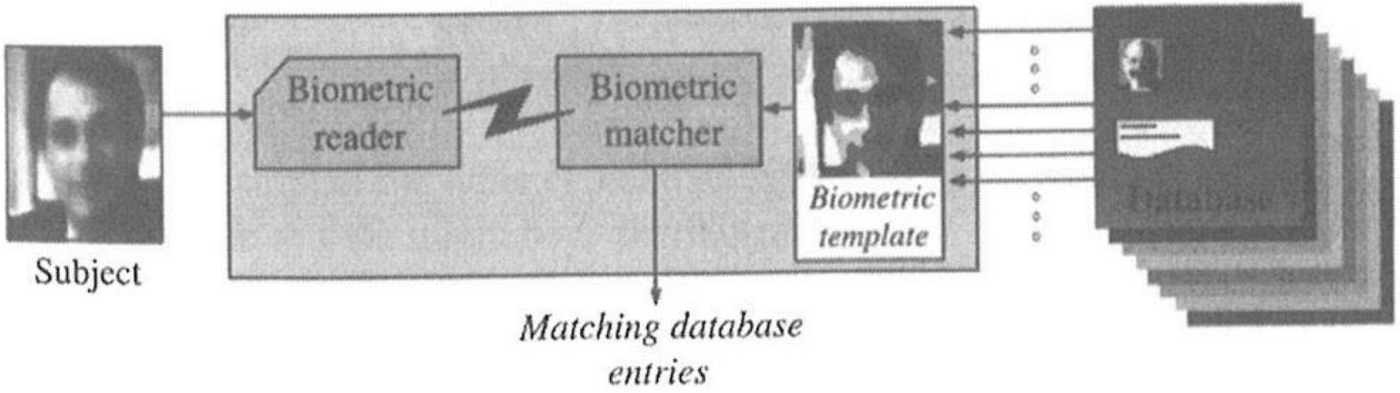
- Universality
  - every person has the biometric characteristic
- Uniqueness
  - no two persons have the same biometric characteristic
- Permanence
  - biometric characteristic invariant over time
- Collectability
  - measurable with a sensing device
- Acceptability
  - user population and public in general should have no strong objections to measuring/collecting the biometric

System Performance and Design Issues

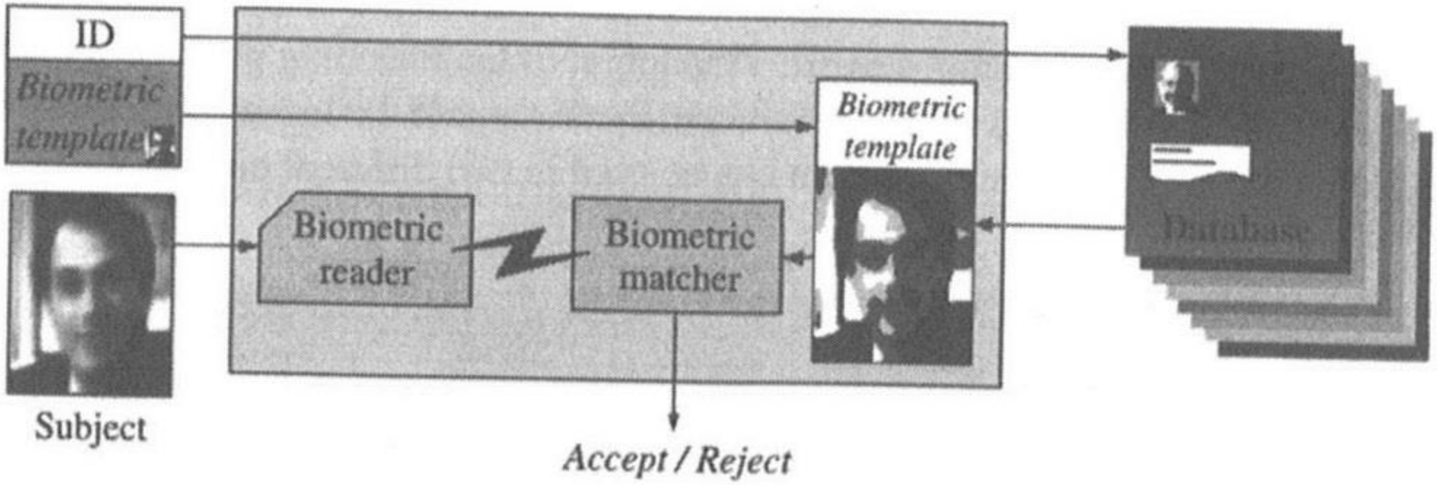
- System performance (accuracy)
- Computational speed (DNA slow)
- Exception handling (difficult to predict)
- System cost (high for DNA)
- Security (can system be compromised?)
- Privacy (data confidentiality)

Identification versus Verification

Identification
1-of-n

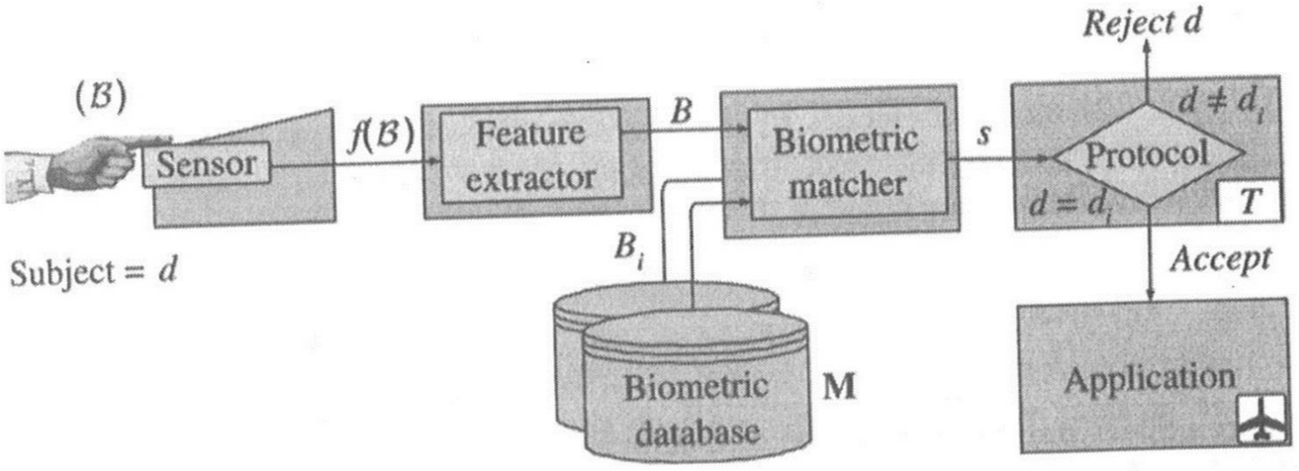


Verification
accept/reject

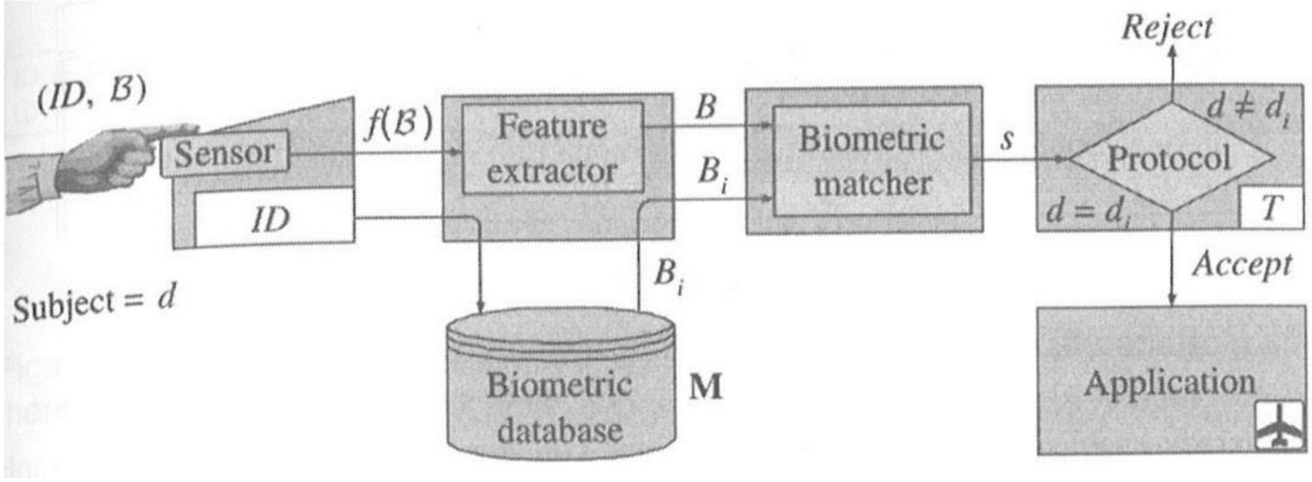


Identification versus Verification

Identification
1-of-n



Verification
accept/reject

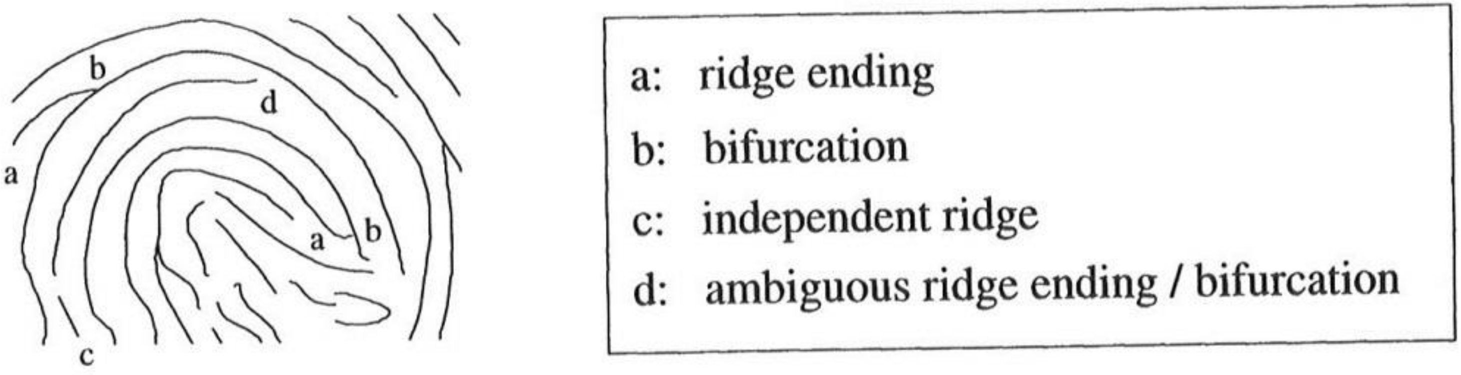


Face Biometric

- Acquisition
  - Single 2D image
  - Video sequence
  - 3D image via stereo imaging, etc.
- Michigan State University – Anil Jain
  - http://biometrics.cse.msu.edu/Presentations/AnilJain_FaceRecognition_KU10.pdf

Fingerprint Biometric

- Acquisition
  - Inked finger impressions, scanners, etc.
- Problem – elastic distortion
- Features



a: ridge ending

b: bifurcation

c: independent ridge

d: ambiguous ridge ending / bifurcation

Figure 3.3: Ridge patterns of individual fingers have minute details, known as minutiae, that distinguish one print from another.

Signature Biometric

- Acquisition
  - Offline (static information) – scanned images
  - Online (static and dynamic info) – digitizers
- Categories of forger sophistication
  - Zero-effort, home-improved, over-the-shoulder, professional

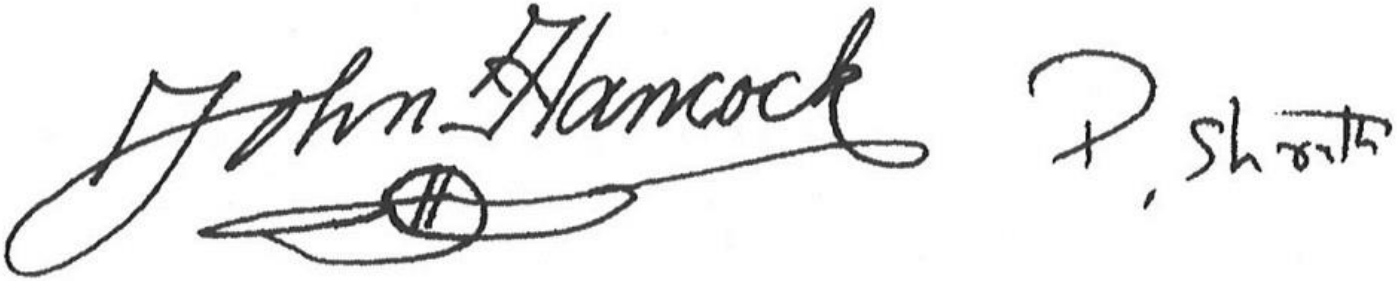
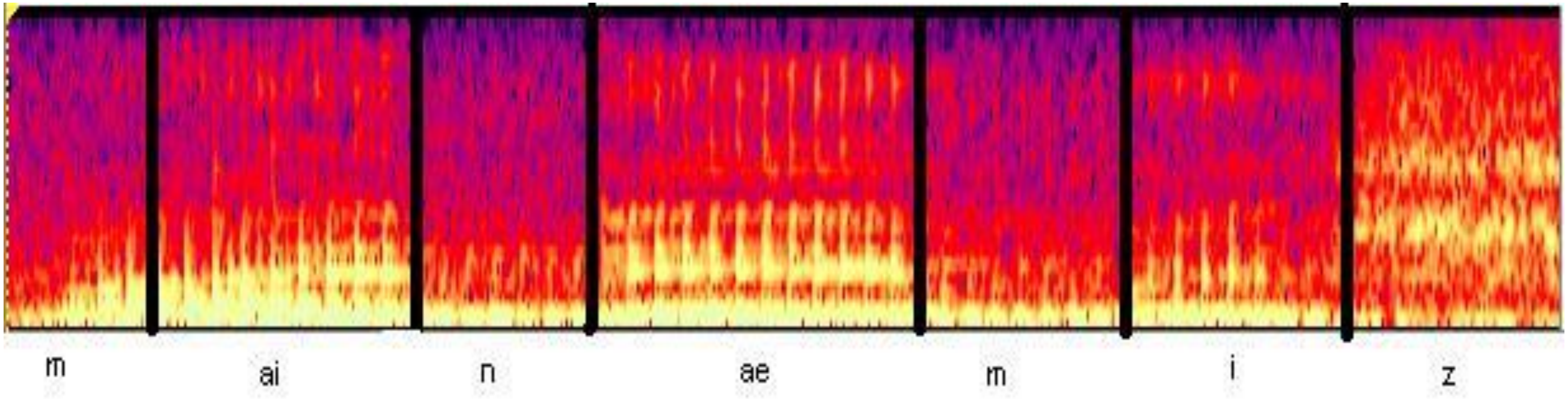


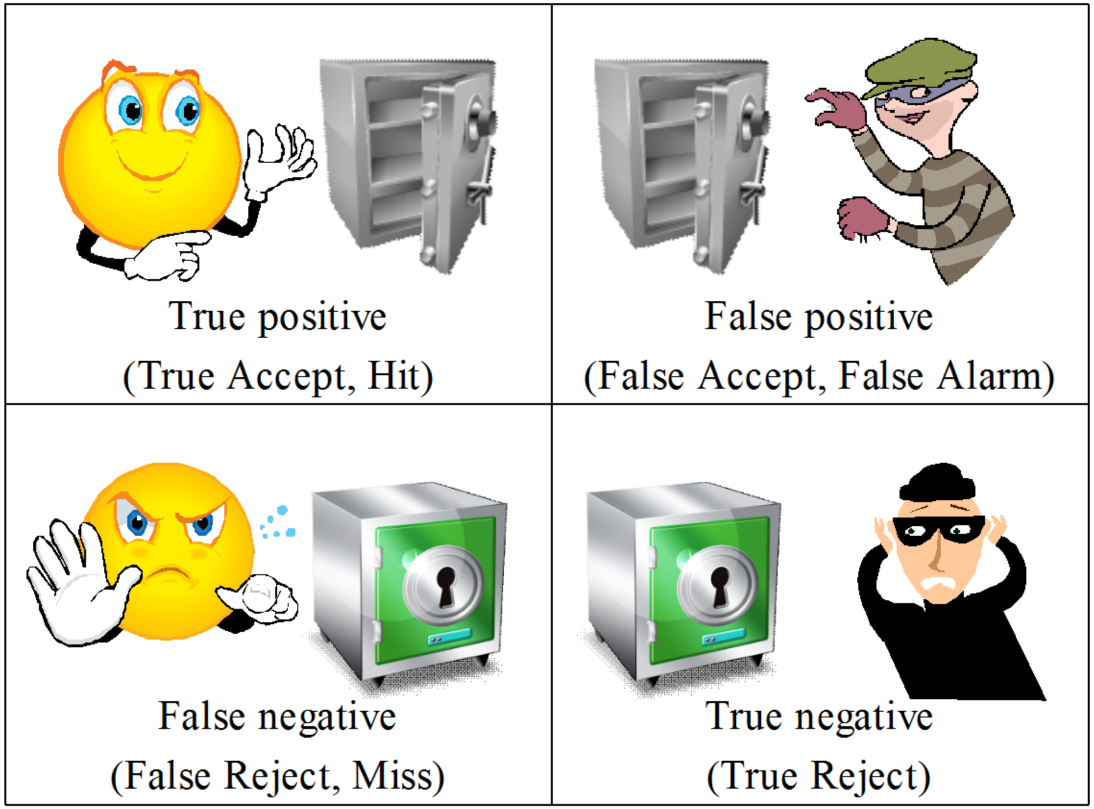
Figure 3.10: Signatures come in a many forms.

Speech Biometric – Voiceprint

- Acquisition
  - Microphone – inexpensive, ubiquitous
- Features from segmented “My name is”



Basic Authentication System Matching Errors

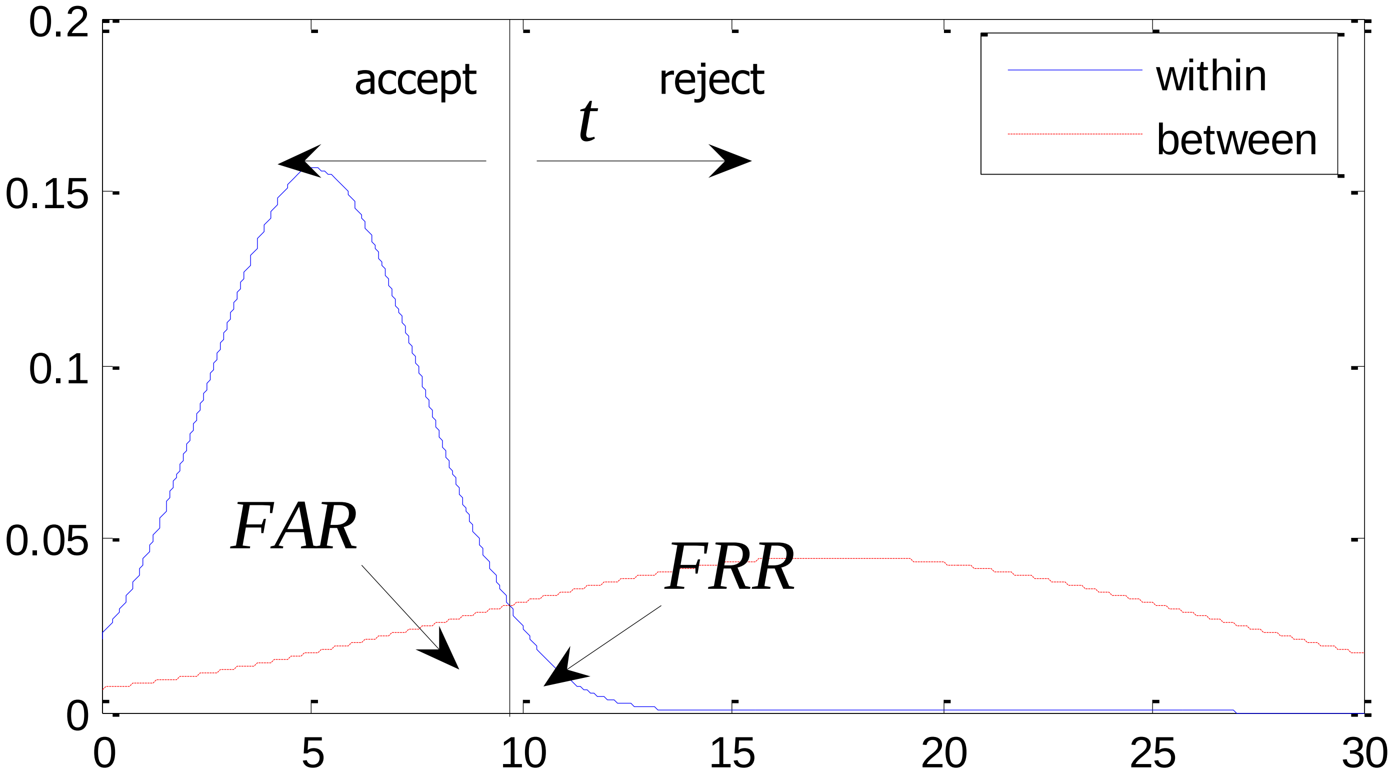


		Actual		
		w	*b*	
Predicted	*w*	True positive (True Accept, Hit)	False positive (False Accept, False Alarm)	FAR
	b	False negative (False Reject, Miss)	True negative (True Reject)	

FRR

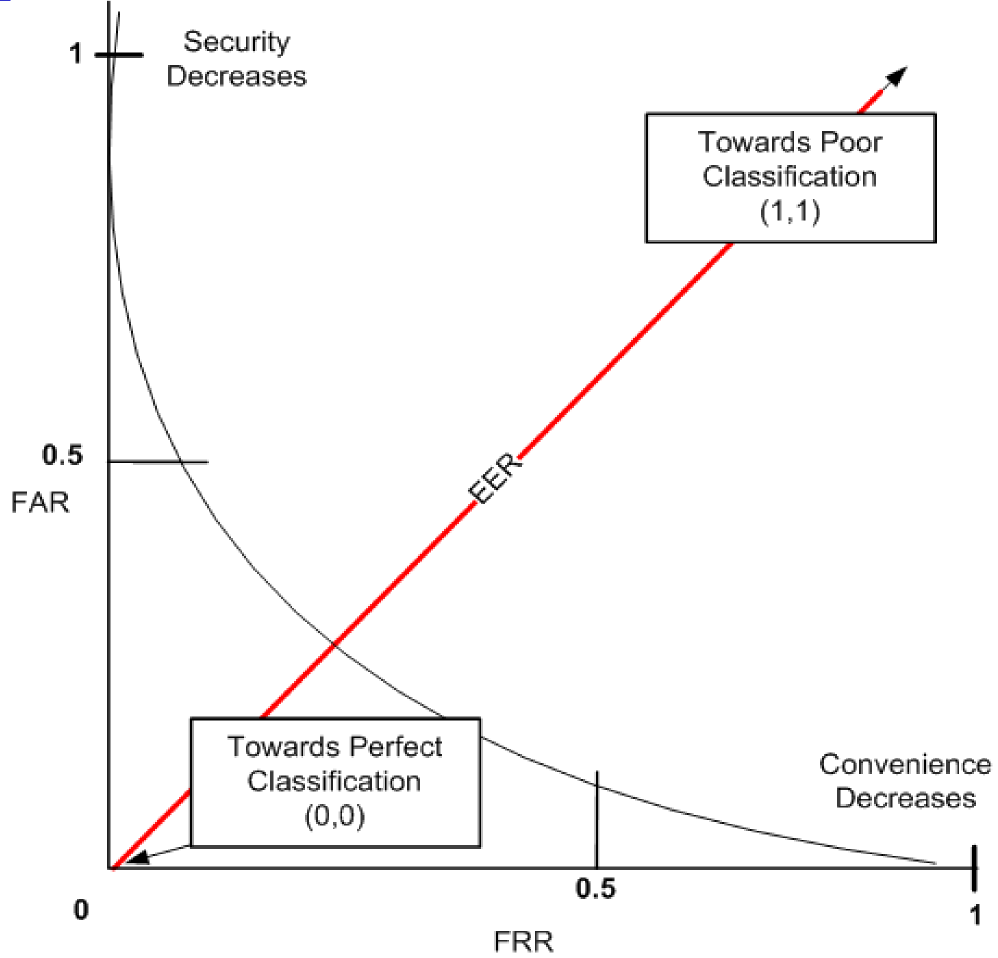
***w* = within class (same person), *b* = between class (different people)**

Basic Authentication System Matching Errors



FAR = False Accept Rate,   FRR = False Reject Rate

Receiver Operating Characteristic (ROC) Curve

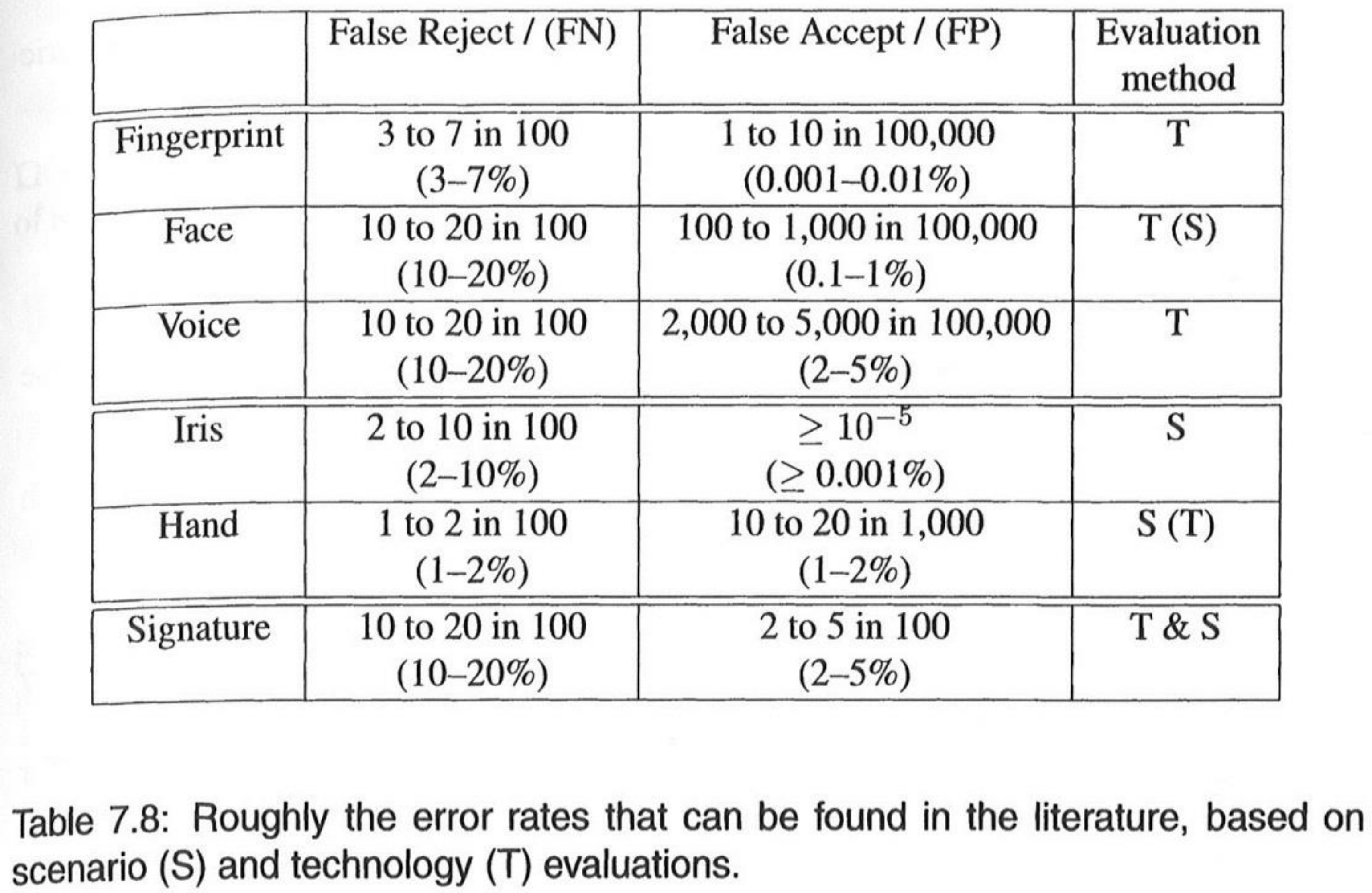


- Low Security/High Convenience (liberal) can be too open
- Low Convenience/High Security (conservative) can be too restrictive
- FAR = False Accept Rate
  - Requires imposter testing
- FRR = False Reject Rate
- EER = Equal Error Rate

Biometric System Evaluation Types

- Technical Evaluation
  - Simulation tests – usual for academic studies
- Scenario Evaluation
  - Testing facility that simulates the actual installation
- Operational Evaluation
  - Actual installation testing – most realistic

Typical Error Rates



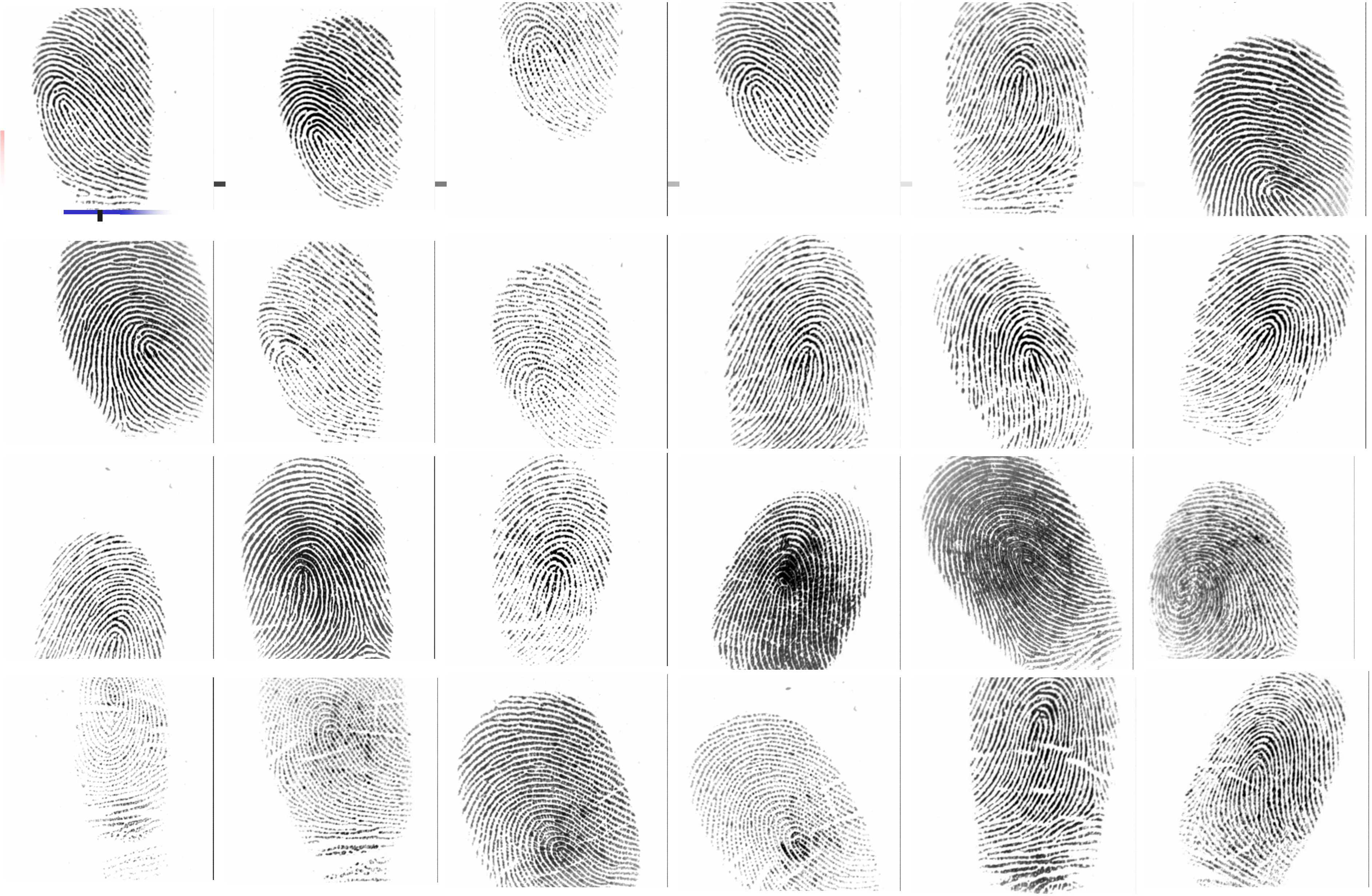
	False Reject / (FN)	False Accept / (FP)	Evaluation method
Fingerprint	3 to 7 in 100 (3–7%)	1 to 10 in 100,000 (0.001–0.01%)	T
Face	10 to 20 in 100 (10–20%)	100 to 1,000 in 100,000 (0.1–1%)	T (S)
Voice	10 to 20 in 100 (10–20%)	2,000 to 5,000 in 100,000 (2–5%)	T
Iris	2 to 10 in 100 (2–10%)	$\geq 10^{-5}$ ($\geq$ 0.001%)	S
Hand	1 to 2 in 100 (1–2%)	10 to 20 in 1,000 (1–2%)	S (T)
Signature	10 to 20 in 100 (10–20%)	2 to 5 in 100 (2–5%)	T & S

Table 7.8: Roughly the error rates that can be found in the literature, based on scenario (S) and technology (T) evaluations.

Biometric Zoo

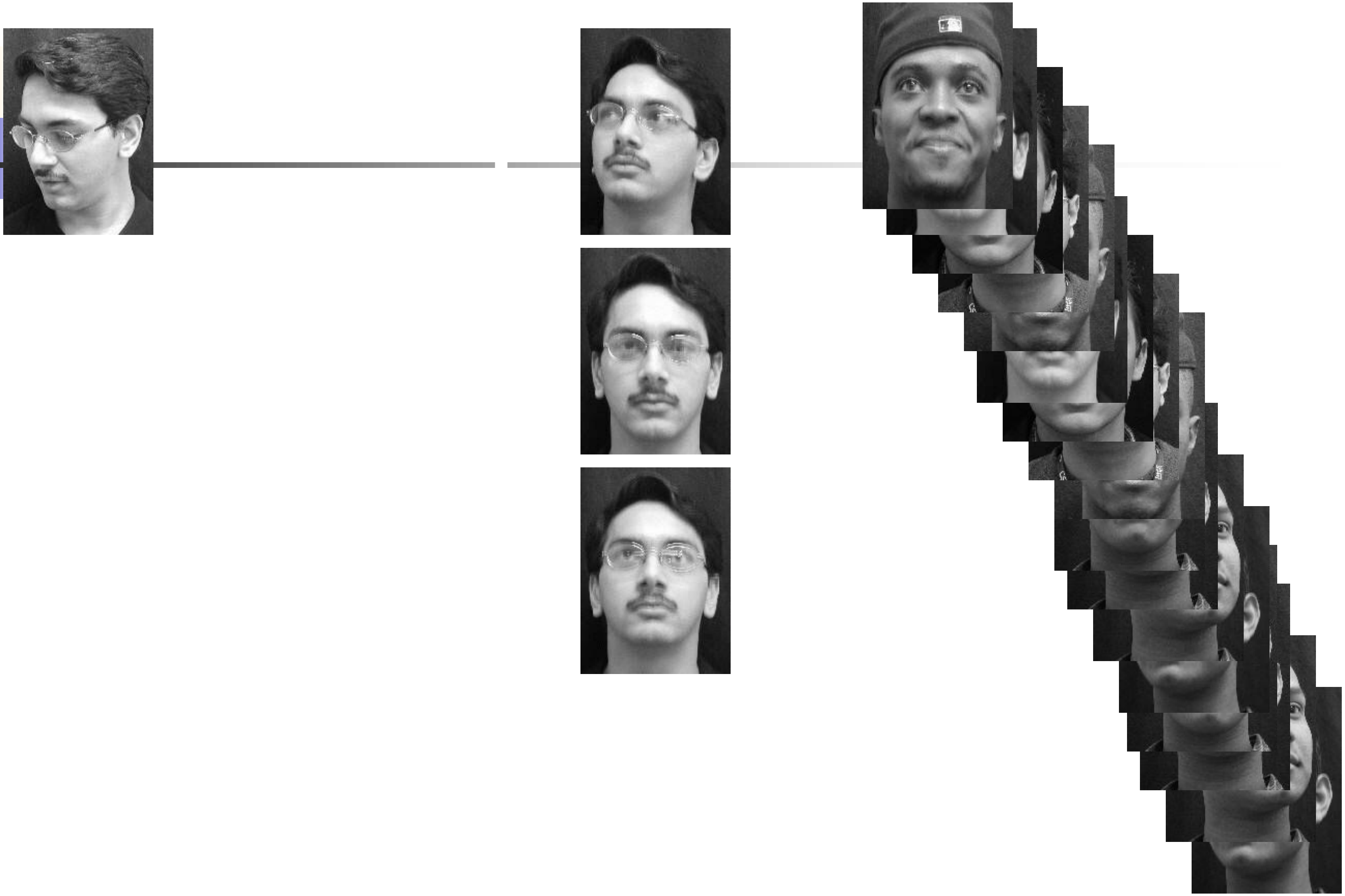
- Sheep
  - Dominant group, systems perform well for them
- Goats
  - Weak distinctive traits, produce many False Rejects
- Lambs
  - Easy to imitate, cause “passive” False Accepts
- Wolves
  - Good at imitating, cause “active” False Accepts
- Chameleons
  - Easy to imitate and good at imitating others

Fingerprint Verification



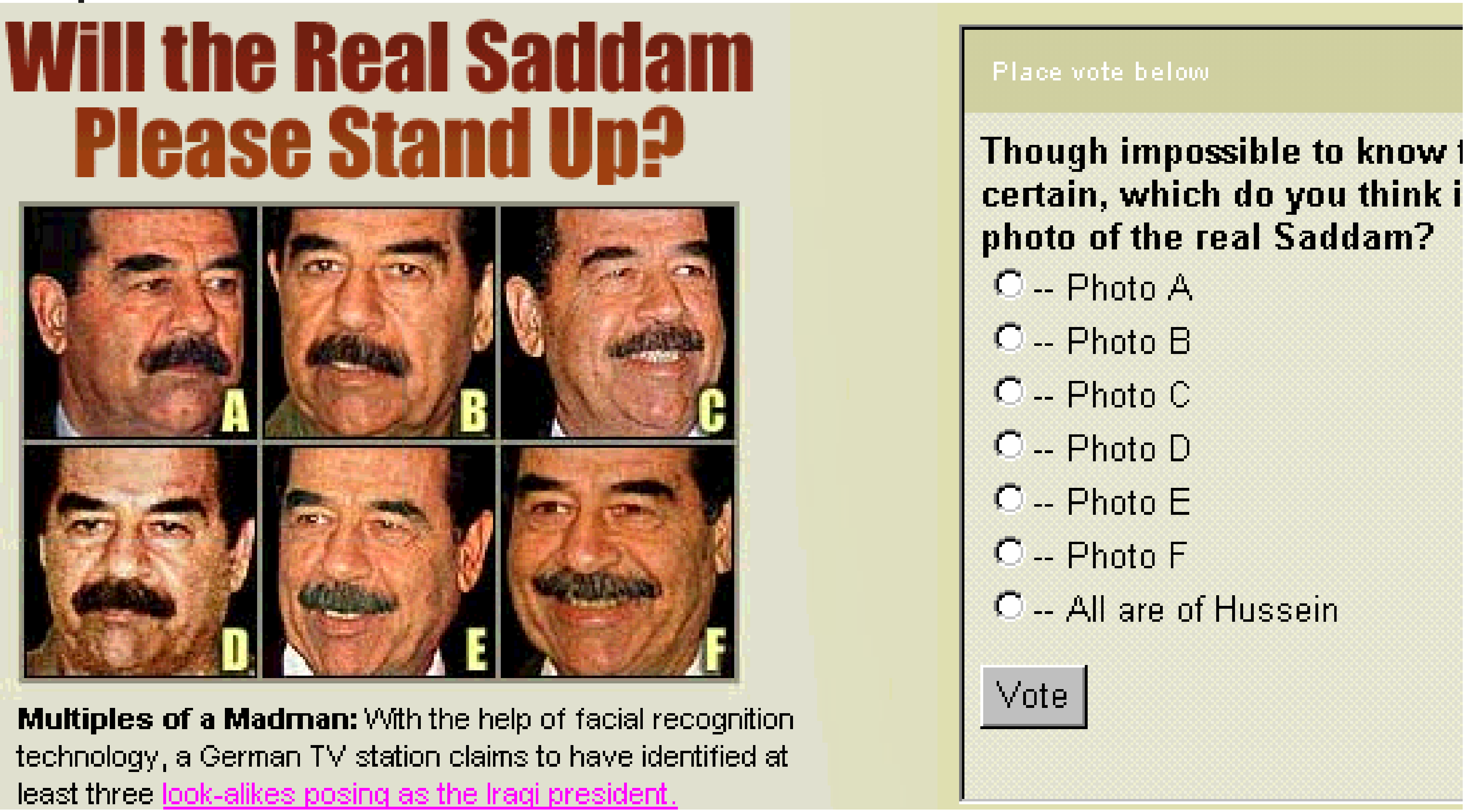
Face Recognition

Face Recognition: System



Inspirational Portrait of Individuality

Face Recognition: National Security



Will the Real Saddam Please Stand Up?

Multiples of a Madman: With the help of facial recognition technology, a German TV station claims to have identified at least three look-alikes posing as the Iraqi president.

Place vote below

Though impossible to know f certain, which do you think i photo of the real Saddam?

○ -- Photo A

○ -- Photo B

○ -- Photo C

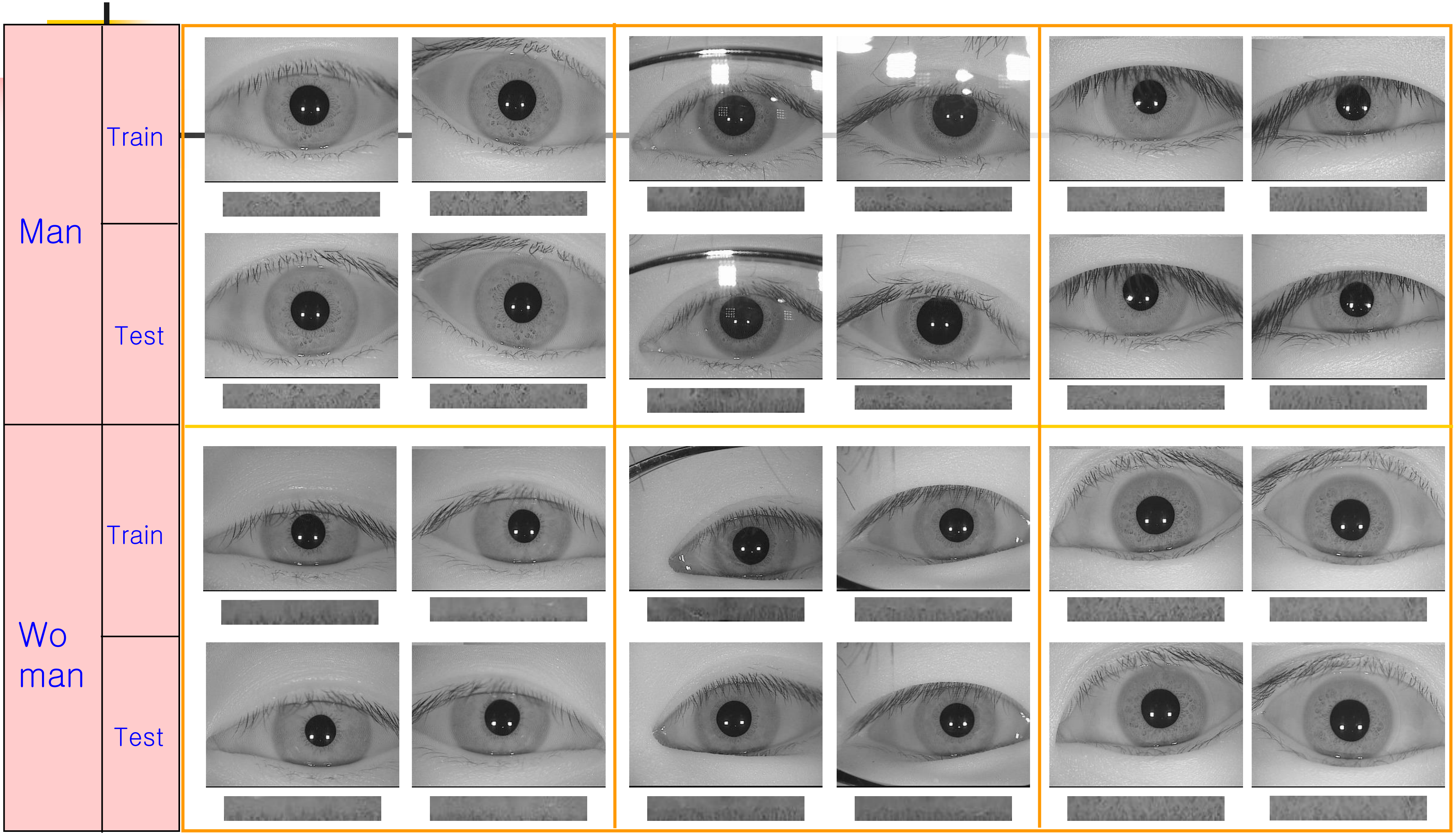
○ -- Photo D

○ -- Photo E

○ -- Photo F

○ -- All are of Hussein

Iris Authentication: Data



Man

Train

Test

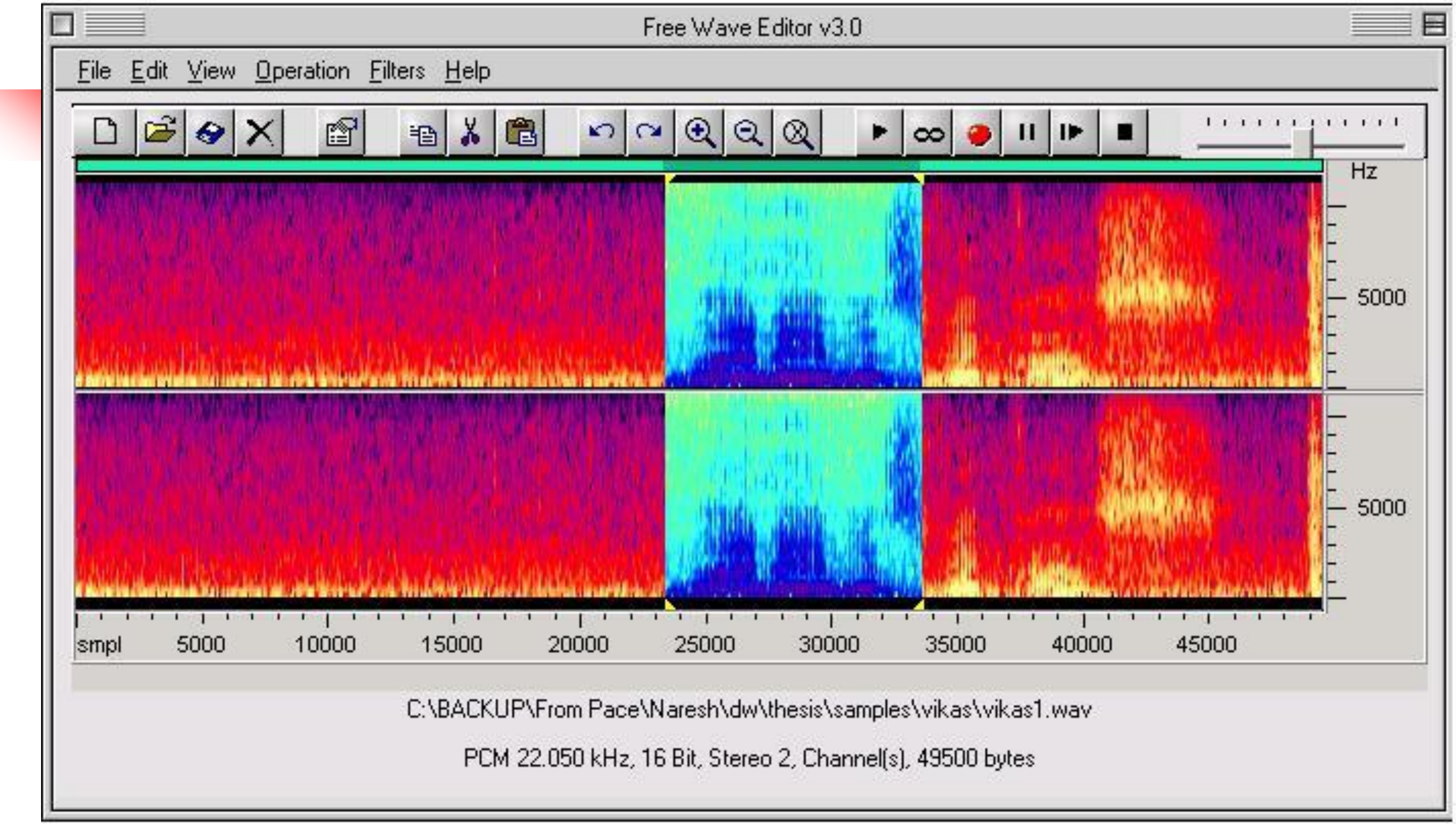
Wo
man

Train

Test

Biometric Authentication

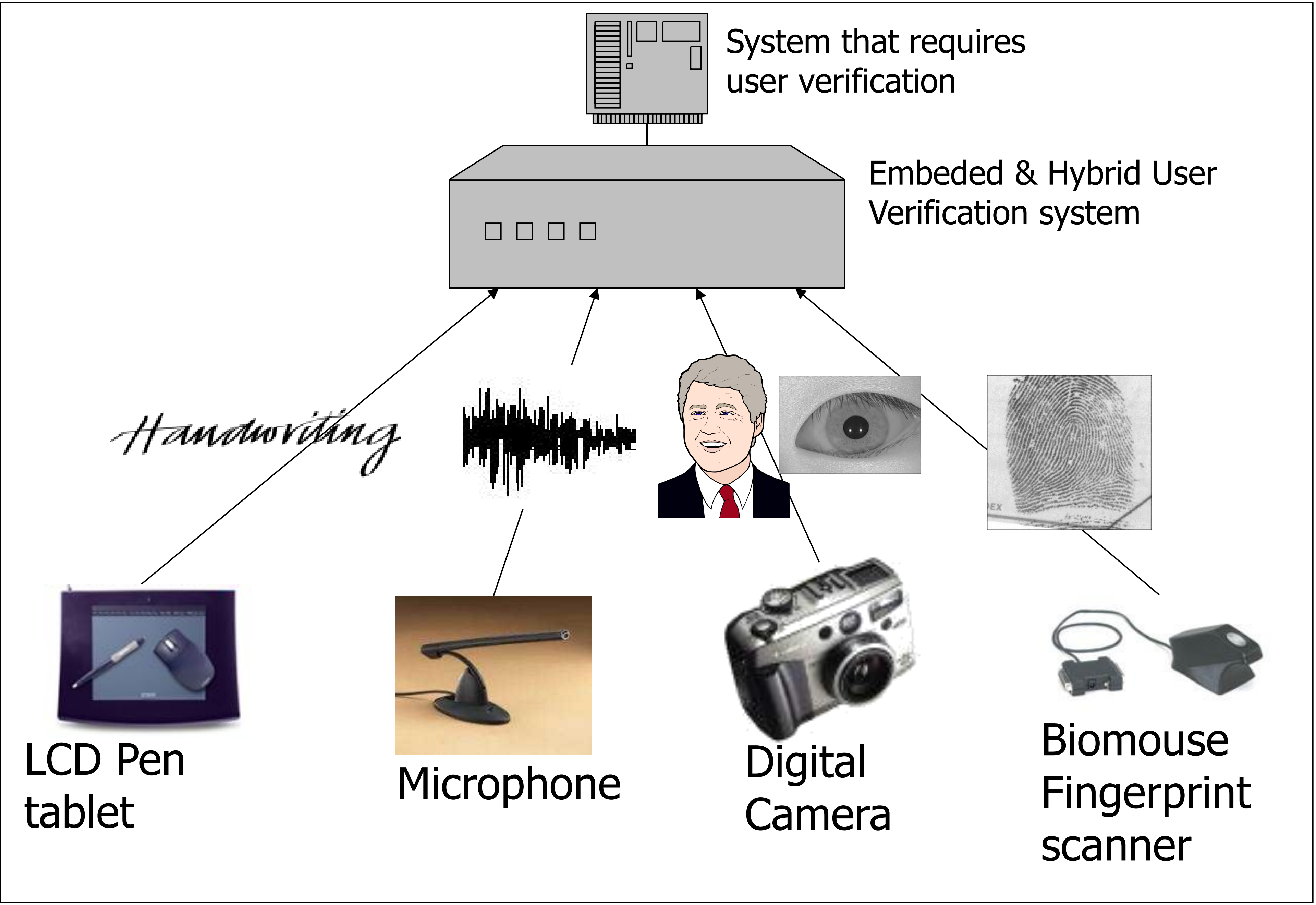
Speaker Individuality: “My name is ...”



C:\BACKUP\From Pace\Naresh\dw\thesis\samples\vikas\vikas1.wav

PCM 22.050 kHz, 16 Bit, Stereo 2, Channel(s), 49500 bytes

Multi-modality Biometric Authentication



System that requires
user verification

Embeded & Hybrid User
Verification system

LCD Pen
tablet

Microphone

Digital
Camera

Biomouse
Fingerprint
scanner

Keystroke Biometrics

- Based on idea that generated patterns are unique to individuals and difficult to duplicate
- Appeal of keystroke over other biometrics
    - Not intrusive, inexpensive, continual user verification
- The keystroke biometric is one of the less-studied behavioral biometrics

Earlier Keystroke Biometric Studies

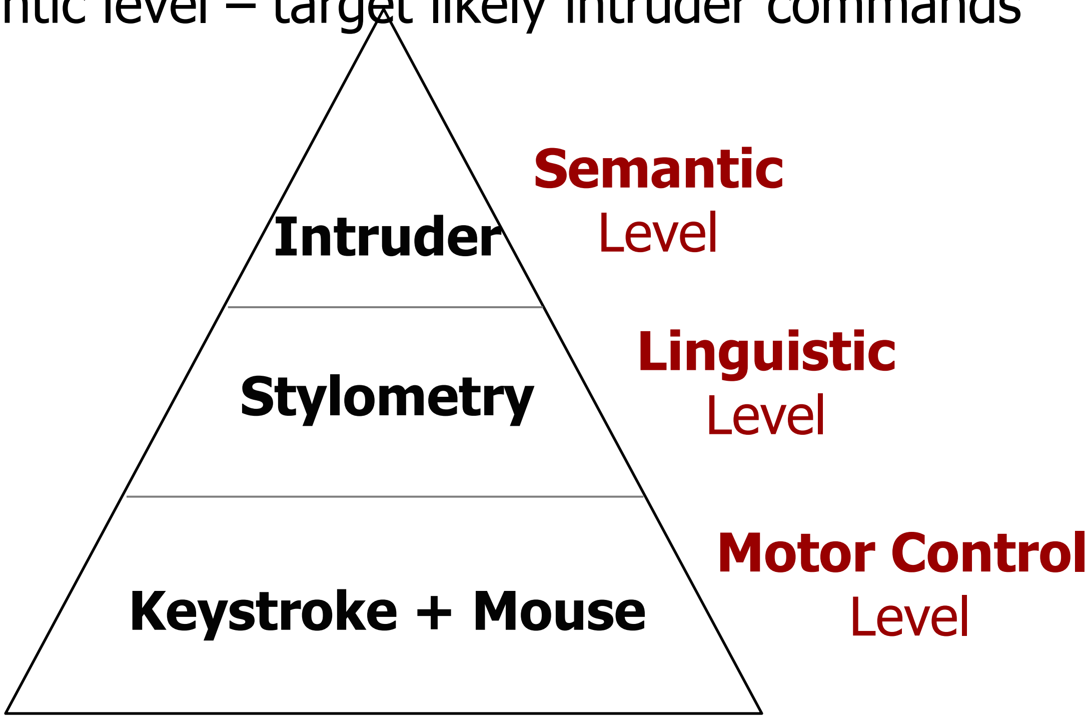
- Most external studies have been on short input of a few seconds
  - Commercial products on hardening passwords
- Most Pace University studies have been on long text input of several minutes
- This study is unique: soft touch-screen keyboards capture more info than mechanical keyboards
  - Location region of press on individual keys
  - Area of finger press on individual keys

Importance of Keystroke & Mouse Biometrics Continual Authentication of Computer Users

- U.S. DoD wants to continually authenticate all government computer users, both military and non-military
  - U.S. DARPA 2010 and 2012 Requests for Proposals
  - Requirement – detect intruder within minutes
- Authentication of students taking online tests
  - U.S. Higher Education Opportunity Act of 2008

Possible Broader Intrusion Detection Plan Multi-biometric System

- Motor control level – keystroke + mouse movement
- Linguistic level – stylometry (char, word, syntax)
- Semantic level – target likely intruder commands


Intruder
Semantic Level
Stylometry
Linguistic Level
Keystroke + Mouse
Motor Control Level