Introduction-cont
Pattern classification

Biometrics
CSE 190-a
Lecture 2

How are people identified?

- People are identified by three basic means:
  – Something they **have** (identity document or token)
  – Something they **know** (password, PIN)
  – Something they **are** (human body)

Problems with Possession- or Knowledge-based Approaches

- Card may be lost, stolen or forgotten
  – Password or PIN may be forgotten or guessed by the imposters
- –25% of people seem to write their PIN on their ATM card
- Estimates of annual identity fraud damages:
  – $56.6 billion in credit card transactions in U.S. alone in 2005*
    - 0.25% of internet transactions revenues, 0.08% of off-line revenues
  – $1 billion in fraudulent cellular phone use
  – $3 billion in ATM withdrawals
- The traditional approaches are unable to differentiate between an authorized person and an impostor

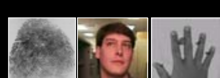
* Spectrum July, 2006

Requirements for an Ideal Biometric Identifier

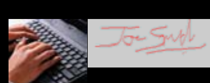
1. Universality
   – Every person should have the biometric characteristic
2. Uniqueness
   – No two persons should be the same in terms of the biometric characteristic
3. Permanence
   – The biometric characteristic should be invariant over time
4. Collectability
   – The biometric characteristic should be measurable with some (practical) sensing device
5. Acceptability
   – One would want to minimize the objections of the users to the measuring/collection of the biometric

Behavioral vs Physical Traits

- Physical Characteristics
  - Iris
  - Retina
  - Vein Pattern
  - Hand Geometry
  - Face
  - Fingerprint
  - Ear shape



- Behavioral Characteristics
  - Keystroke dynamics
  - Signature dynamics
  - Walking Gait
  - Voice



About this Class

- See Syllabus
- Special thanks to
  – Peter Belhumeur
  – Anil Jain

Applications

Forensic	Government	Commercial
Corpse Identification,	National ID card,	Computer Network Logon,
Criminal Investigation,	Correctional Facility,	Electronic Data Security,
Terrorist Identification,	Driver's License,	E-Commerce,
Parenthood Determination,	Social Security,	Internet Access,
Missing Children, etc.	Welfare Disbursement,	ATM, Credit Card,
	Border Control,	Physical Access Control,
	Passport Control, etc.	Cellular Phones,
		Personal Digital Assistant,
		Medical Records Management
		Distance Learning, etc.

* There are ~500 million border crossings/year in the U.S.

UCSD Biometric Soda Machine

Face
Fingerprint

US-VISIT
www.dhs.gov/us-visit
Homeland Security

*As part of the enhanced procedures, most visitors traveling on visas will have two fingerprints scanned by an inkless device and a digital photograph taken. All of the data and information is then used to assist the border inspector in determining whether or not to admit the traveler. These enhanced procedures will add only seconds to the visitor's overall processing time.

The electronic fingerprint scanner allows inspectors to check identities of visitors against those on terrorist watch lists.

By Stephen J. Boitano, AP

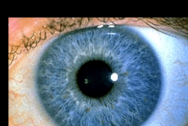
From the DHS US-VISIT web-site

Access Control

http://www.livegrip.com

http://www.livegrip.com

Using Iris Scans to Unlock Hotel Rooms



The Nine Zero hotel in Boston just installed a new system which uses digital photos of the irises of employees, vendors and VIP guests to admit them to certain areas, the same system used in high-security areas at airports such as New York's JFK.

USA TODAY 7/22/2004

Biometrics for Personalization

- Automatic personalization of vehicle settings:
  - Seat position
  - Steering wheel position
  - Mirror positions
  - Lighting
  - Radio station preferences
  - Climate control settings
- URLs at your fingertips

http://www.visteon.com

What makes using biometrics difficult?

Why is Biometric Recognition Difficult?

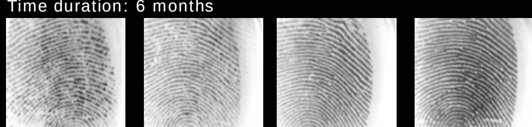
- Large number of classes (e.g., millions of faces)
- Intra-class variability and inter-class similarity
- Segmentation
- Noisy and distorted images
- Population coverage & scalability
- System performance (error rate, speed, ,throughput, cost)
- Attacks on the biometric system
- Template ageing
- Non-uniqueness of biometric characteristics
- Addressing privacy concerns

Intra-class variability

Inter-class Similarity

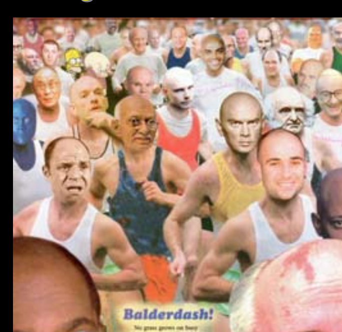
Temporal Variations

Time duration: 6 months



Time duration: 2 years

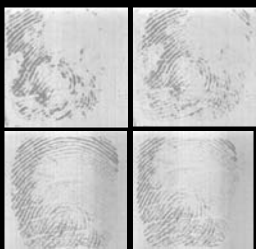
Locating Faces in a Crowd



Games Magazine, September 2001

Noisy Images

- ~ 3% of the population has poor quality fingerprint images



Four impressions of a user's fingerprint

Jan 2, 2004

Faded fingerprints cost former welder a job

Associated Press

DECATUR — The years Chuck Strickler spent as a welder provided him with the experience he needed as a welding inspector at power plants across the nation.

But the welding also has left Strickler, 60, of Decatur, lacking a full set of intact fingerprints required under new, stepped-up security regulations at nuclear plants. Since the U.S. Department of Homeland Security issued the new rules in the wake of Sept. 11, the reams of documents Strickler has attesting to his identity no longer are sufficient.

"I first ran into a problem with it three or four years ago," Strickler said. "They said my fingerprints weren't valid. But at the time they accepted a picture ID as proof of identity."

Earlier this year, when he tried to get a job inspecting the D.C. Cook Nuclear Power Station near Bridgman, where he had worked before, his application was turned down because of the worn-down ridges on his fingertips.

"I passed everything except for the fingerprints," Strickler said adding that the application process included a comprehensive psychological examination and criminal background check.

"The plant sent the fingerprints to the FBI, and they said it's outside the realm of the Homeland Security's guidelines (for what is needed). It was a little frustrating."

Strickler

A person has about 100 identification marks on his or her fingerprints, and most adults have about 80 that can be used to identify them.

But because of his welding work, Strickler has only about 30 of the identification points.

Strickler is free to work at non-nuclear plants. But he says he prefers to have the option of working for the nuclear facilities.

"This cuts my income in half," he said.

Attacks on Biometric Systems

- Spoofing a biometric trait

Dummy finger created from a lifted impression

Artificial skin/fingers (http://www.livingskin.com/)

Sensor Interoperability

- Sensors used during enrollment and verification may be different

Sensor Interoperability

A rolled inked fingerprint

Digital Biometrics optical sensor (508x480)

Veridicom capacitive sensor (300x300)

Fidelica pressure sensor (256x256)

Sensors used during enrollment and verification may be different

How good are Biometric Systems?
i.e., Evaluation

Performance Evaluation

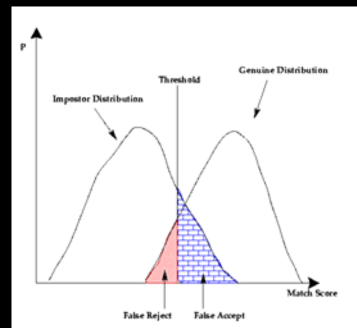
- The overall performance of a biometric system is assessed in terms of its universality, accuracy, speed, and storage
- Factors like cost and ease of use also affect performance
- Biometric systems are not perfect, and can mistakenly accept an impostor as a valid user (a false match) or conversely, reject a valid individual (a false non-match)

Best Practices: www.cesg.gov.uk/technology/biometrics
FRVT2002:www.frvt.org/
FVC 2004: bias.csr.unibo.it/fvc2004
NIST SV: www.nist.gov/speech/tests/spk

Performance Characterization

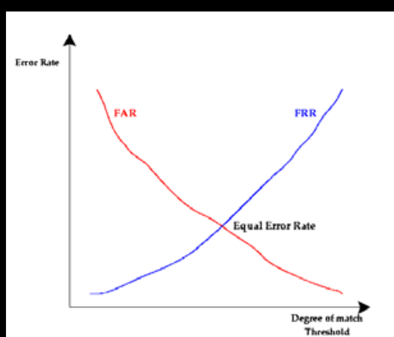
- Impostor Distribution
- Genuine Distribution
- Threshold
- False Accept Rate (FAR) or False Match Rate
- False Reject Rate (FRR) or False Non-match Rate
- Receiver Operating Characteristic (ROC) curve
- Equal Error Rate or Crossover Rate
- Failure to Enroll (FTE)
- Failure to Acquire (FTA) or Failure to Capture

Error Rates



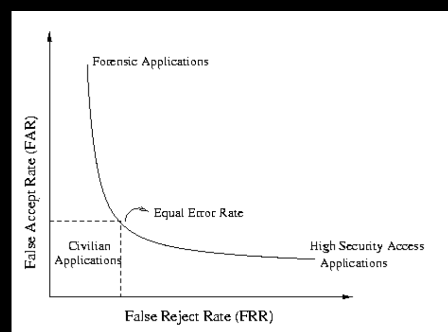
False Match (False Accept): Mistaking biometric measurements from two different persons to be from the same person; **False Non-match (False reject):** Mistaking two biometric measurements from the same person to be from two different persons

Error vs Threshold



FAR: False accept rate
FRR: False reject rate

ROC Curve



Accuracy requirements of a biometric system are application dependent

Evaluation Protocol

- Define a protocol to test the system, select the data and measure the performance; performance depends on the test set
- Evaluations should be conducted by an independent organization (that is not involved in the design of the system)
- Test on biometric data previously unseen by the system
- Size of the data-set and representative examples of the data set should be provided for tuning algorithmic parameters
- Face, Fingerprint and Voice systems have undergone the most study and testing

"State-of-the-art" Error Rates

	Test	Test Parameter	False Reject Rate	False Accept Rate
Fingerprint	FVC [2002]	20 years (average age)	0.2%	0.2%
	FVC [2004]	Deliberate perturbations	2.07%	2.07%
Face	FRVT [2002]	Varied lighting, outdoor/indoor	10%	1%
Voice	NIST [2000]	Text Independent	10-20%	2-5%

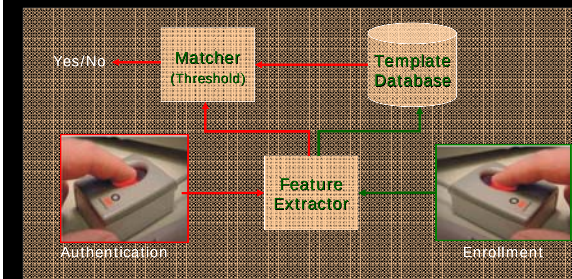
At NY airports, an average of ~ 300,000 passengers pass through daily. If all of these used biometric-authenticated smart cards for identification, there would be 600 falsely rejected (and inconvenienced) passengers per day for fingerprints, 30,000 for face and 45,000 for voice. Similar numbers can be computed for false accepts.

Reading List

Performance Metrics and Evaluation

1. Fingerprint Verification Competition (FVC 2000, 2002, 2004): http://bias.csr.unibo.it/fvc2004/
2. Fingerprint Vendor Technology Evaluation (FpVTE 2003): http://fpvte.nist.gov/
3. Face Recognition Vendor Tests (FRVT 2000, 2002): http://www.frvt.org/
4. Face Verification Contest on the BANCA dataset (2004): http://www.ee.surrey.ac.uk/banca/icpr2004/
5. NIST - Speaker Recognition Evaluations (1996 – 2004): http://www.nist.gov/speech/tests/spk/
6. Signature Verification Competition (SVC 2004): http://www.cs.ust.hk/svc2004/

Biometrics: A Pattern Recognition System



- False accept rate (FAR): Proportion of imposters accepted
- False reject rate (FRR): Proportion of genuine users rejected
- Failure to enroll rate (FTE): portion of population that cannot be enrolled
- Failure to acquire rate (FTA): portion of population that cannot be verified

Chapter 1: Introduction to Pattern Recognition (Sections 1.1-1.6)

- Machine Perception
- An Example
- Pattern Recognition Systems
- The Design Cycle
- Learning and Adaptation

An Example

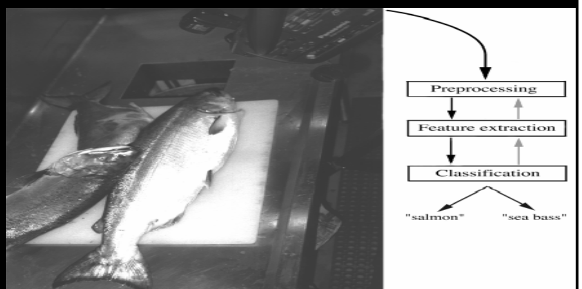
- "Sorting incoming Fish on a conveyor according to species using optical sensing"

Species — Sea bass / Salmon

- 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…
    - This is the set of all suggested features to explore for use in our classifier!

- Preprocessing
  - Use a segmentation operation to isolate fishes from one another and from the background
- Information from a single fish is sent to a feature extractor whose purpose is to reduce the data by measuring certain features
- The features are passed to a classifier

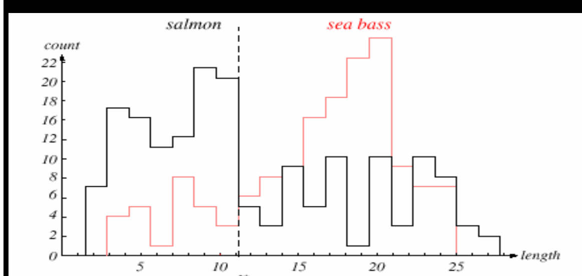
37



38

- Classification
  - Select the length of the fish as a possible feature for discrimination

39

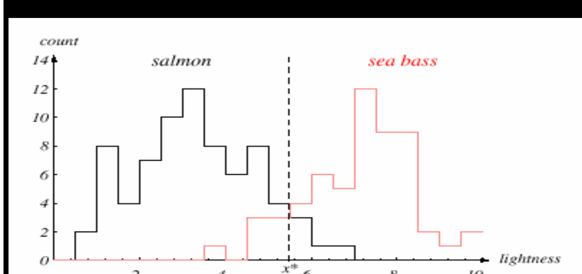


40

The length is a poor feature alone!

Select the lightness as a possible feature.

41



42

- Threshold decision boundary and cost relationship
  - Move our decision boundary toward smaller values of lightness in order to minimize the cost (reduce the number of sea bass that are classified salmon!)

Task of decision theory

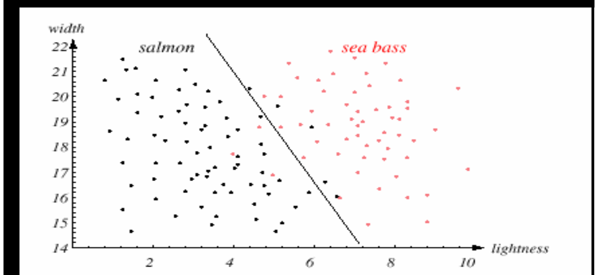
43

- Adopt the lightness and add the width of the fish

Fish ⟶ $x^T = [x_1, x_2]$

Lightness   Width

44

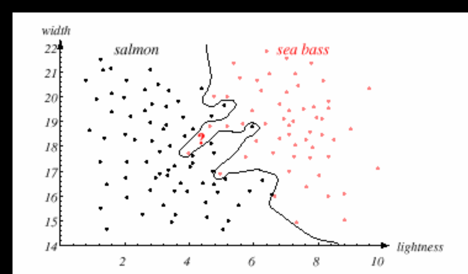


45

- We might add other features that are not correlated with the ones we already have. A precaution should be taken not to reduce the performance by adding such “noisy features”

- Ideally, the best decision boundary should be the one which provides an optimal performance such as in the following figure:

46



47

- However, our satisfaction is premature because the central aim of designing a classifier is to correctly classify novel input

Issue of generalization!

48