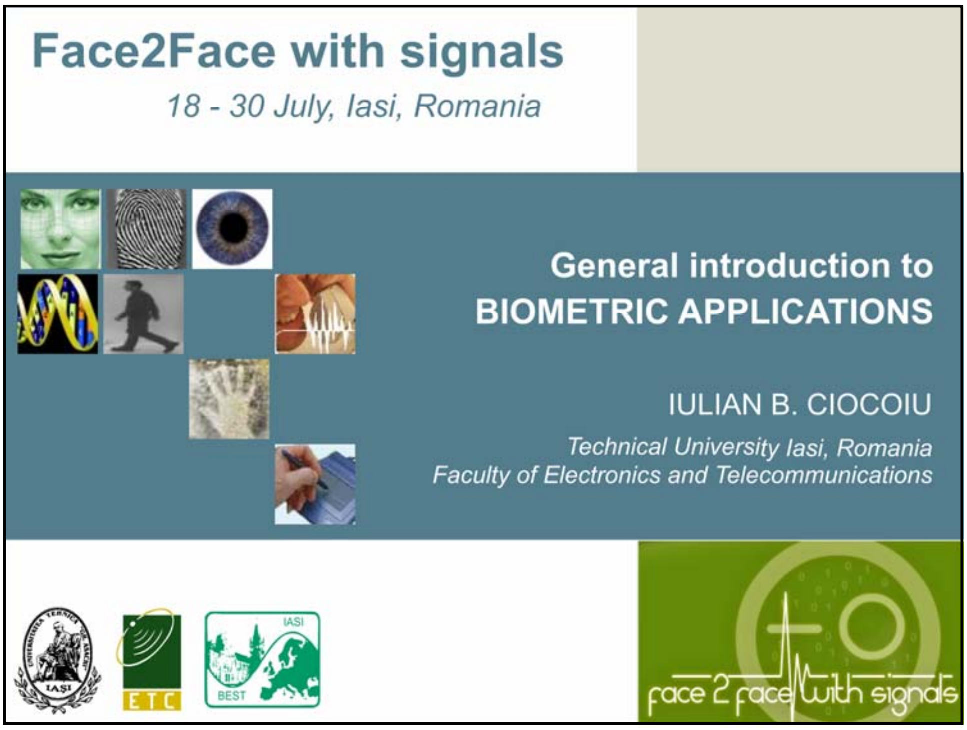


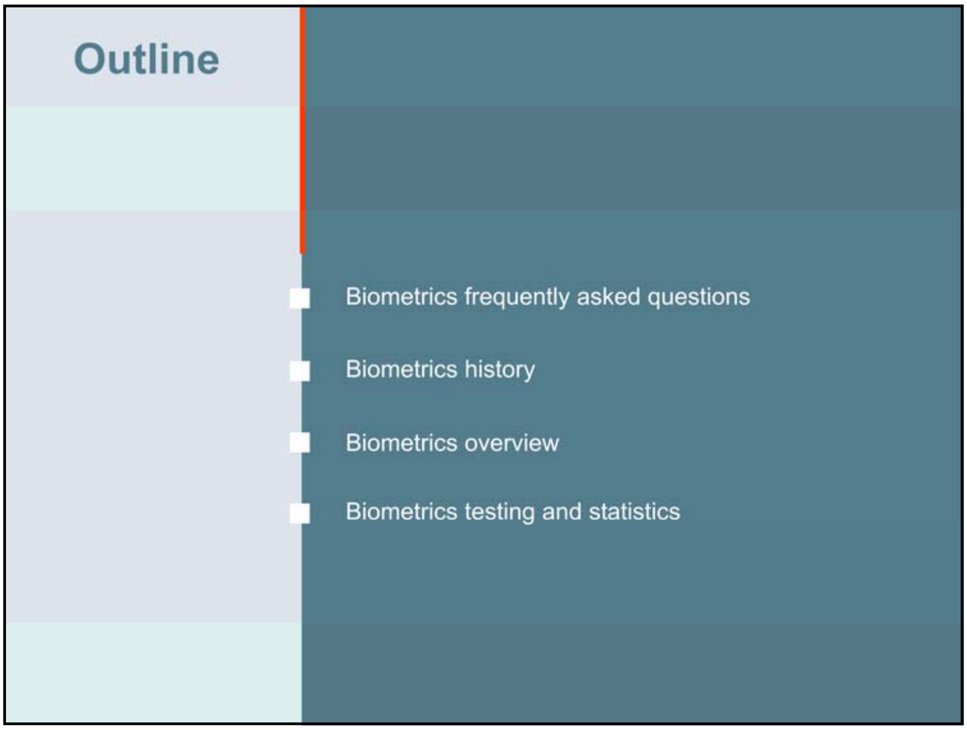
Face2Face with signals

18 - 30 July, Iasi, Romania

General introduction to BIOMETRIC APPLICATIONS

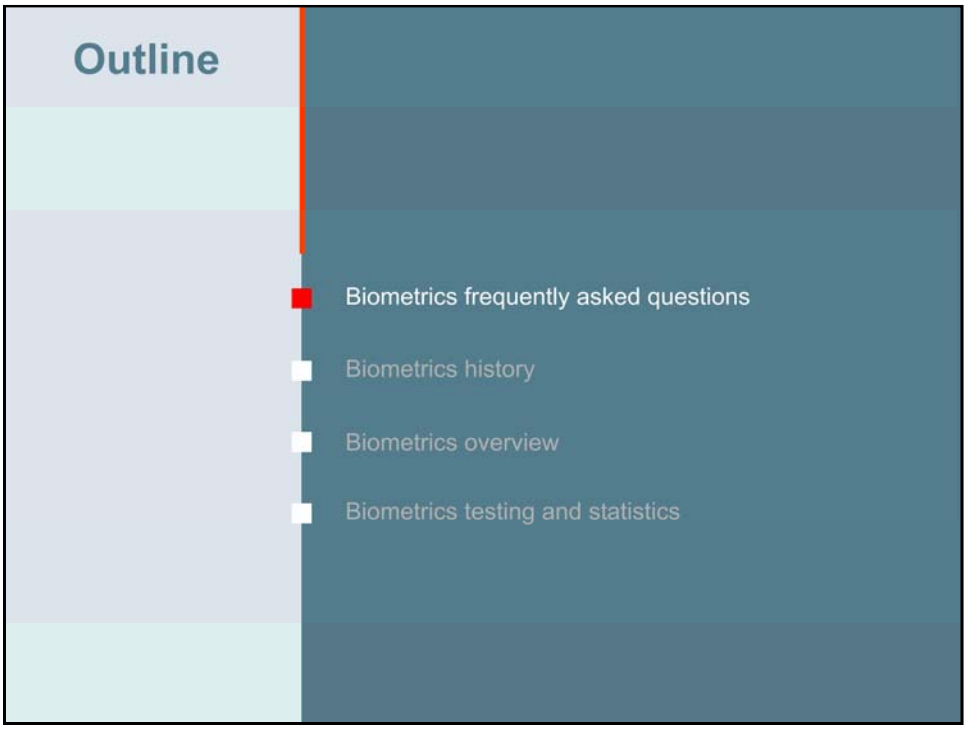
IULIAN B. CIOCOIU

Technical University Iasi, Romania
Faculty of Electronics and Telecommunications



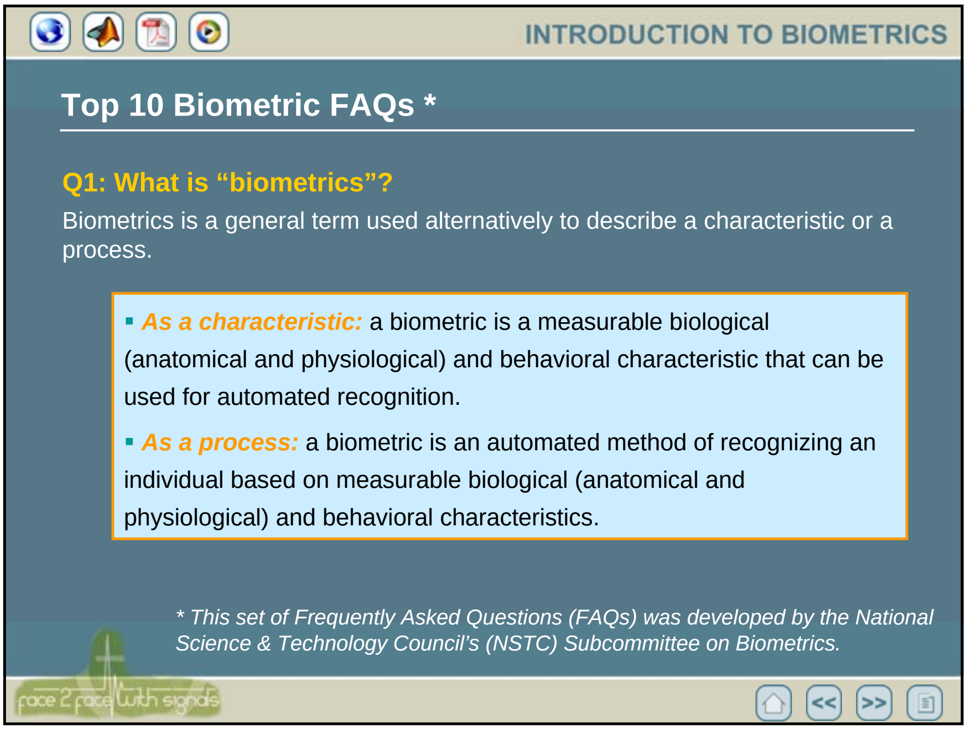
Outline

- Biometrics frequently asked questions
- Biometrics history
- Biometrics overview
- Biometrics testing and statistics



Outline

- Biometrics frequently asked questions
- Biometrics history
- Biometrics overview
- Biometrics testing and statistics



INTRODUCTION TO BIOMETRICS

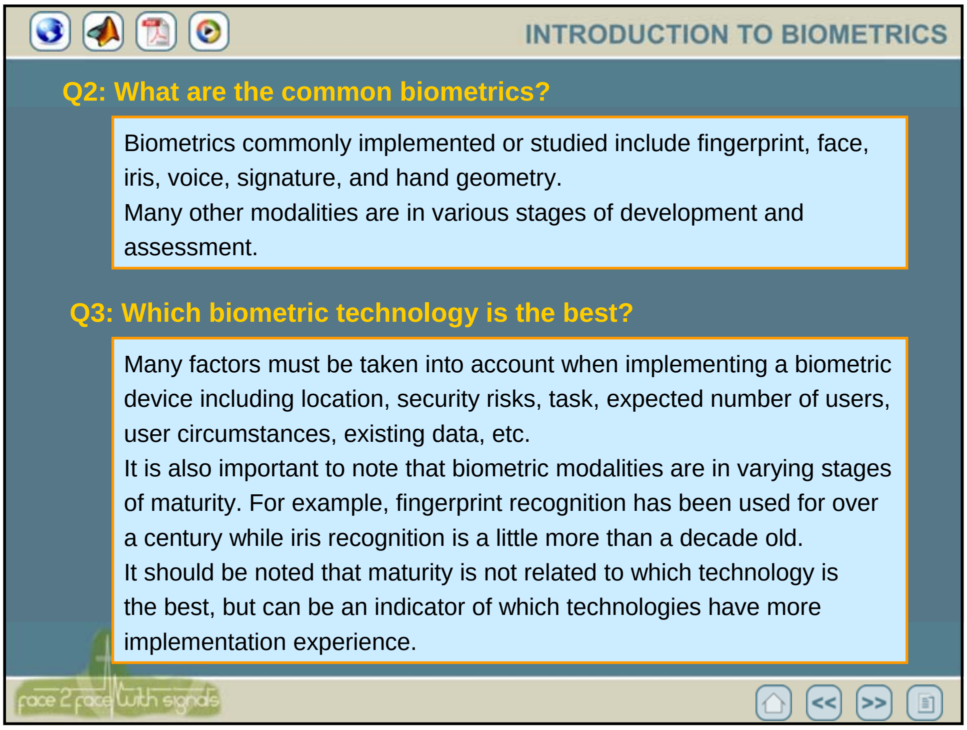
Top 10 Biometric FAQs *

Q1: What is “biometrics”?

Biometrics is a general term used alternatively to describe a characteristic or a process.

- ***As a characteristic:*** a biometric is a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition.
- ***As a process:*** a biometric is an automated method of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

** This set of Frequently Asked Questions (FAQs) was developed by the National Science & Technology Council’s (NSTC) Subcommittee on Biometrics.*



INTRODUCTION TO BIOMETRICS

Q2: What are the common biometrics?

Biometrics commonly implemented or studied include fingerprint, face, iris, voice, signature, and hand geometry.

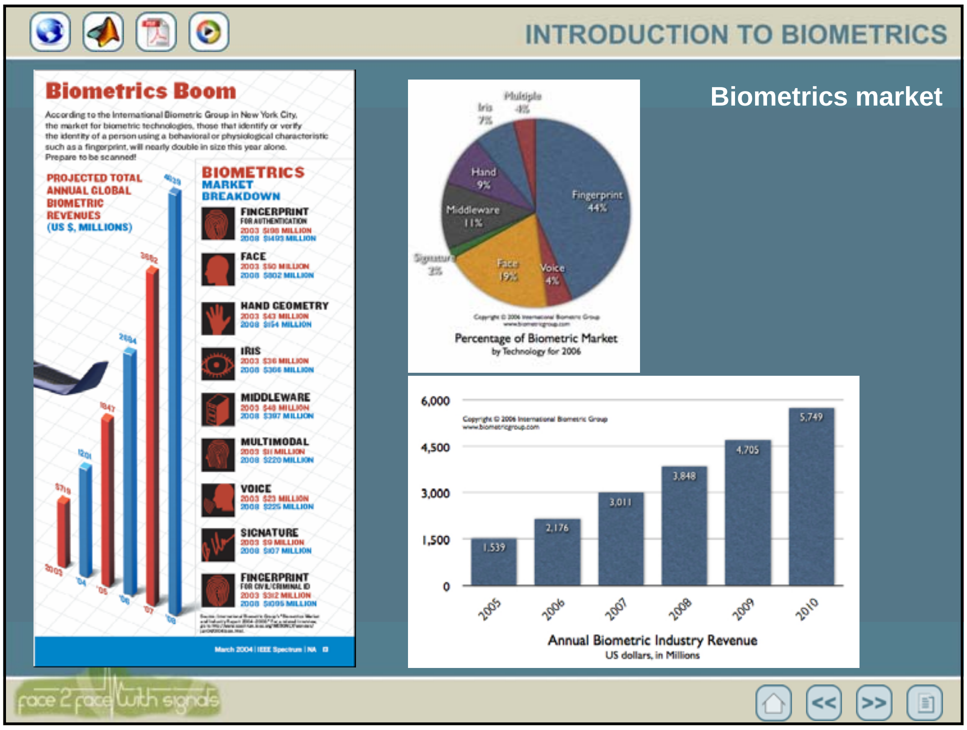
Many other modalities are in various stages of development and assessment.

Q3: Which biometric technology is the best?

Many factors must be taken into account when implementing a biometric device including location, security risks, task, expected number of users, user circumstances, existing data, etc.

It is also important to note that biometric modalities are in varying stages of maturity. For example, fingerprint recognition has been used for over a century while iris recognition is a little more than a decade old.

It should be noted that maturity is not related to which technology is the best, but can be an indicator of which technologies have more implementation experience.



INTRODUCTION TO BIOMETRICS

Biometrics market

Biometrics Boom

According to the International Biometric Group in New York City, the market for biometric technologies, those that identify or verify the identity of a person using a behavioral or physiological characteristic such as a fingerprint, will nearly double in size this year alone. Prepare to be scanned!

PROJECTED TOTAL ANNUAL GLOBAL BIOMETRIC REVENUES (US $, MILLIONS)
$719
1201
1847
2684
3682
4639
2003
'04
'05
'06
'07
'08

BIOMETRICS MARKET BREAKDOWN

FINGERPRINT FOR AUTHENTICATION
2003 $198 MILLION
2008 $1493 MILLION

FACE
2003 $50 MILLION
2008 $802 MILLION

HAND GEOMETRY
2003 $43 MILLION
2008 $154 MILLION

IRIS
2003 $36 MILLION
2008 $366 MILLION

MIDDLEWARE
2003 $48 MILLION
2008 $397 MILLION

MULTIMODAL
2003 $11 MILLION
2008 $220 MILLION

VOICE
2003 $23 MILLION
2008 $225 MILLION

SIGNATURE
2003 $9 MILLION
2008 $107 MILLION

FINGERPRINT FOR CIVIL/CRIMINAL ID
2003 $312 MILLION
2008 $1095 MILLION

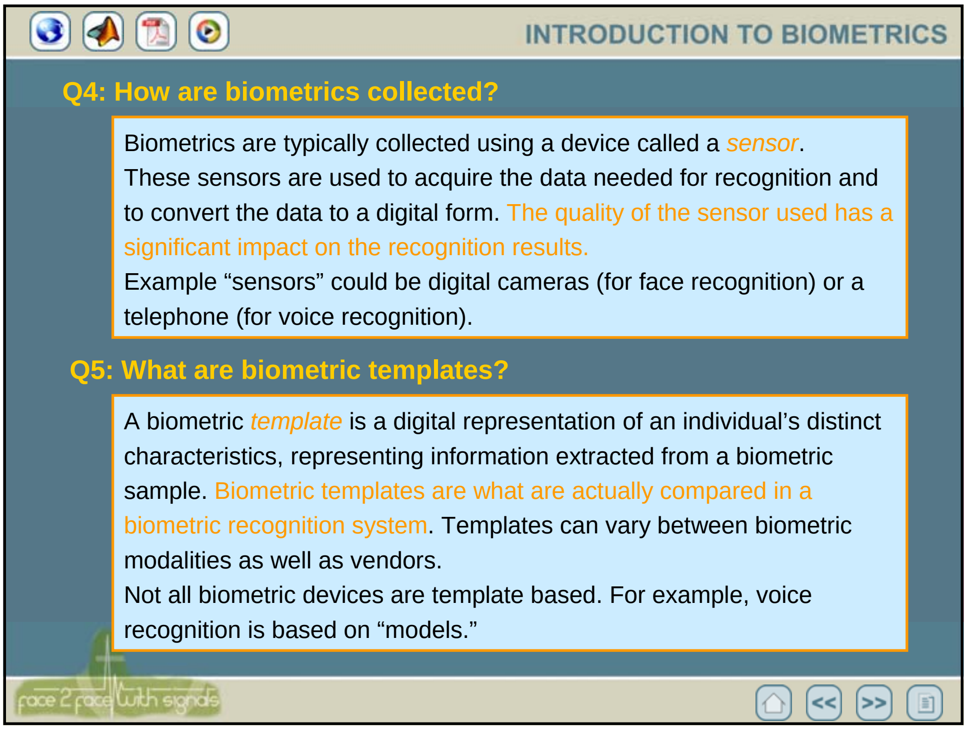
March 2004 | IEEE Spectrum | NA

Copyright © 2006 International Biometric Group www.biometricgroup.com

Percentage of Biometric Market by Technology for 2006

Copyright © 2006 International Biometric Group www.biometricgroup.com

Annual Biometric Industry Revenue
US dollars, in Millions



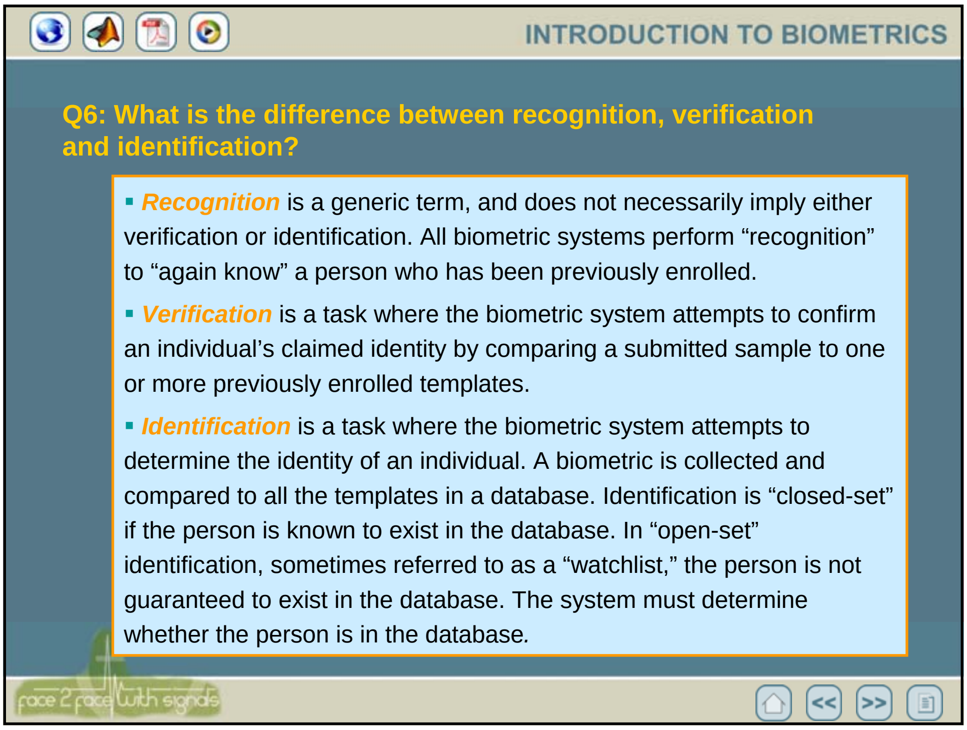
INTRODUCTION TO BIOMETRICS

Q4: How are biometrics collected?

Biometrics are typically collected using a device called a *sensor*. These sensors are used to acquire the data needed for recognition and to convert the data to a digital form. The quality of the sensor used has a significant impact on the recognition results.
Example “sensors” could be digital cameras (for face recognition) or a telephone (for voice recognition).

Q5: What are biometric templates?

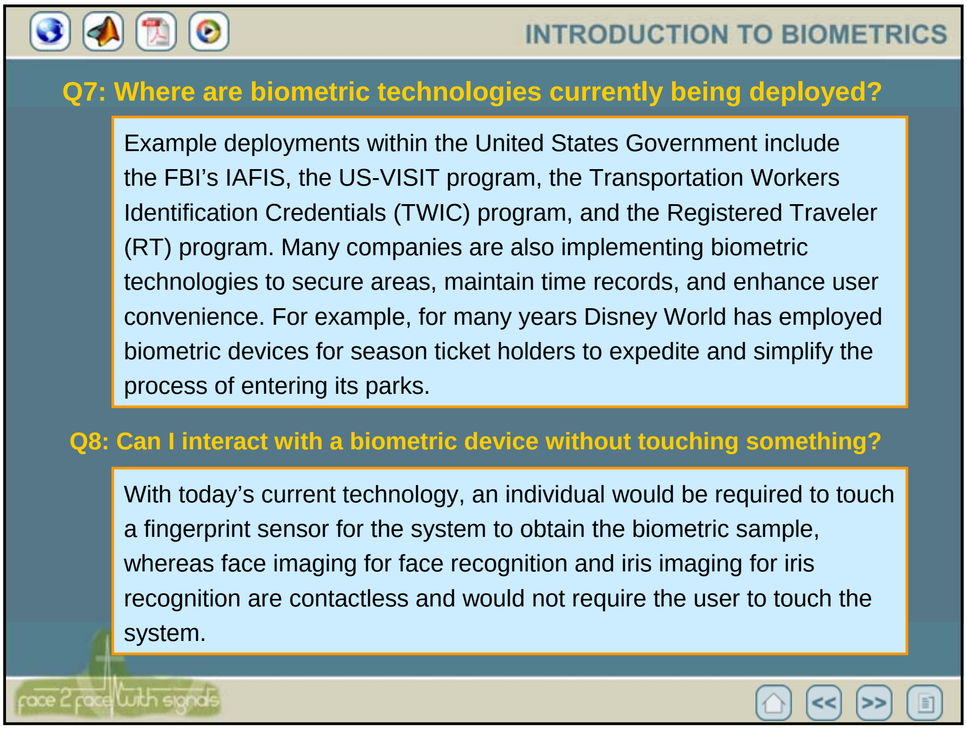
A biometric *template* is a digital representation of an individual’s distinct characteristics, representing information extracted from a biometric sample. Biometric templates are what are actually compared in a biometric recognition system. Templates can vary between biometric modalities as well as vendors.
Not all biometric devices are template based. For example, voice recognition is based on “models.”



INTRODUCTION TO BIOMETRICS

Q6: What is the difference between recognition, verification and identification?

- ***Recognition*** is a generic term, and does not necessarily imply either verification or identification. All biometric systems perform “recognition” to “again know” a person who has been previously enrolled.
- ***Verification*** is a task where the biometric system attempts to confirm an individual’s claimed identity by comparing a submitted sample to one or more previously enrolled templates.
- ***Identification*** is a task where the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database. Identification is “closed-set” if the person is known to exist in the database. In “open-set” identification, sometimes referred to as a “watchlist,” the person is not guaranteed to exist in the database. The system must determine whether the person is in the database.


face 2 face with signals
<<
>>

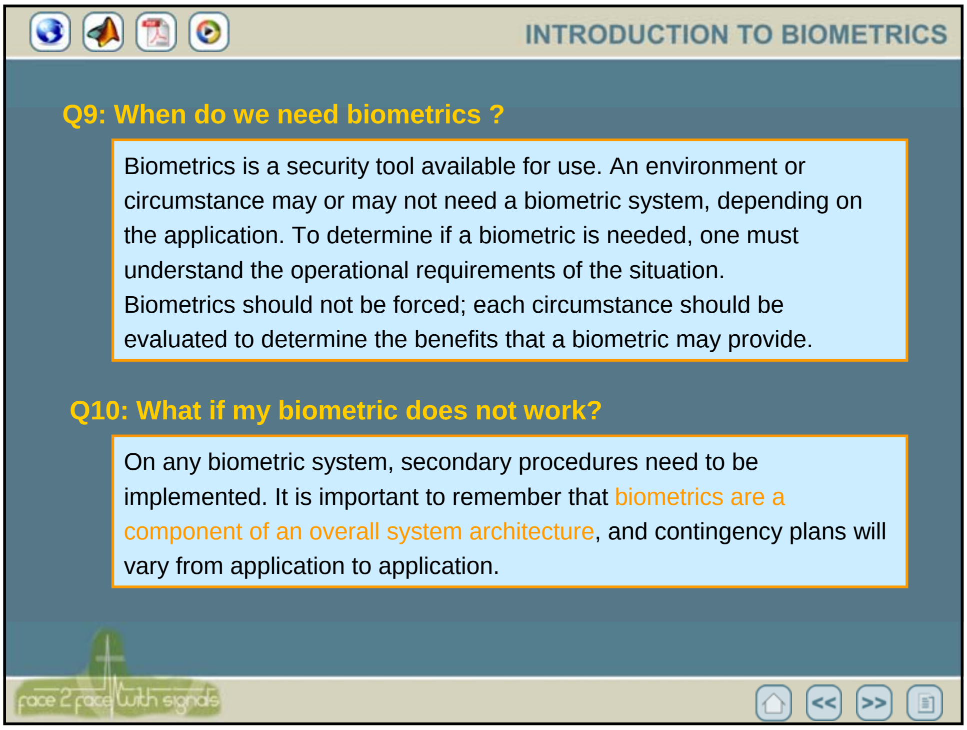
INTRODUCTION TO BIOMETRICS

Q7: Where are biometric technologies currently being deployed?

Example deployments within the United States Government include the FBI's IAFIS, the US-VISIT program, the Transportation Workers Identification Credentials (TWIC) program, and the Registered Traveler (RT) program. Many companies are also implementing biometric technologies to secure areas, maintain time records, and enhance user convenience. For example, for many years Disney World has employed biometric devices for season ticket holders to expedite and simplify the process of entering its parks.

Q8: Can I interact with a biometric device without touching something?

With today's current technology, an individual would be required to touch a fingerprint sensor for the system to obtain the biometric sample, whereas face imaging for face recognition and iris imaging for iris recognition are contactless and would not require the user to touch the system.


face 2 face with signals
<<
>>

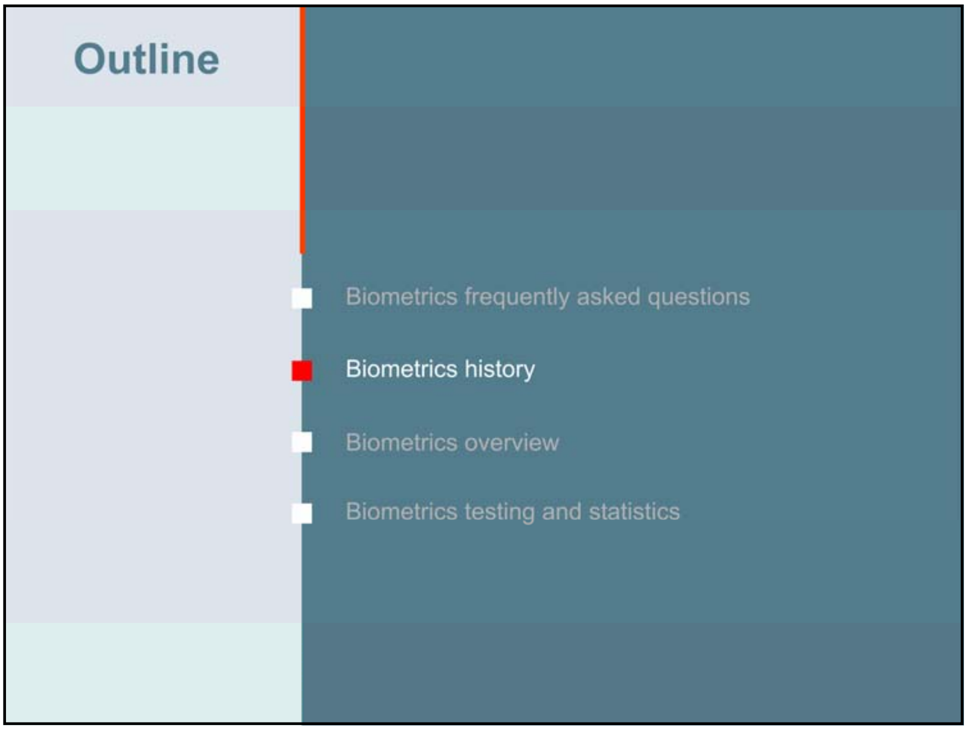
INTRODUCTION TO BIOMETRICS

Q9: When do we need biometrics ?

Biometrics is a security tool available for use. An environment or circumstance may or may not need a biometric system, depending on the application. To determine if a biometric is needed, one must understand the operational requirements of the situation. Biometrics should not be forced; each circumstance should be evaluated to determine the benefits that a biometric may provide.

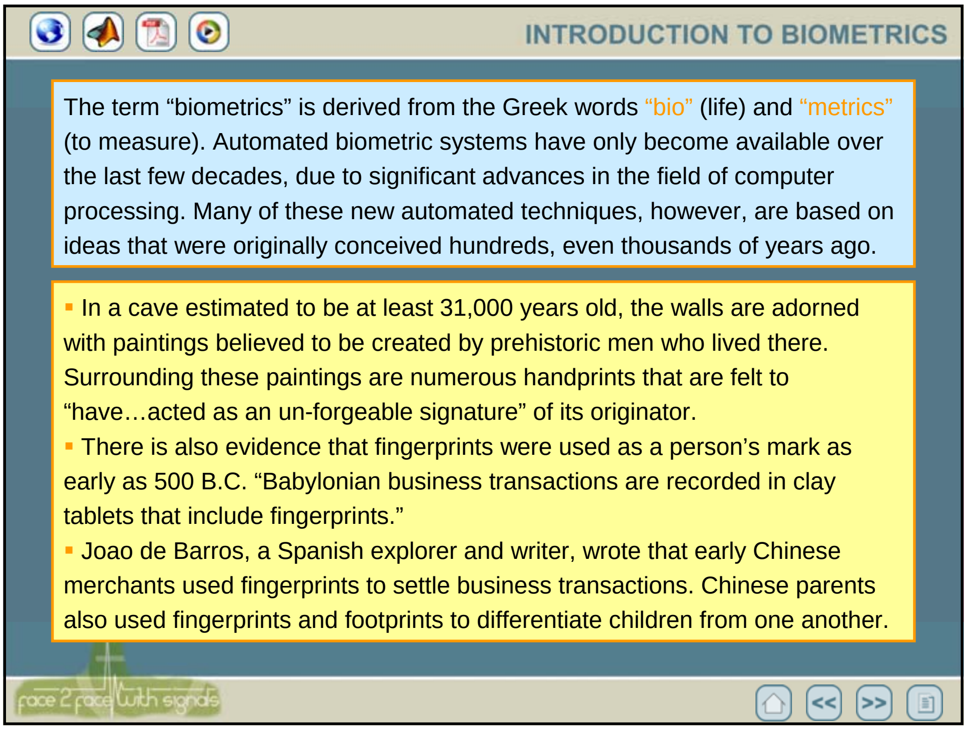
Q10: What if my biometric does not work?

On any biometric system, secondary procedures need to be implemented. It is important to remember that biometrics are a component of an overall system architecture, and contingency plans will vary from application to application.



Outline

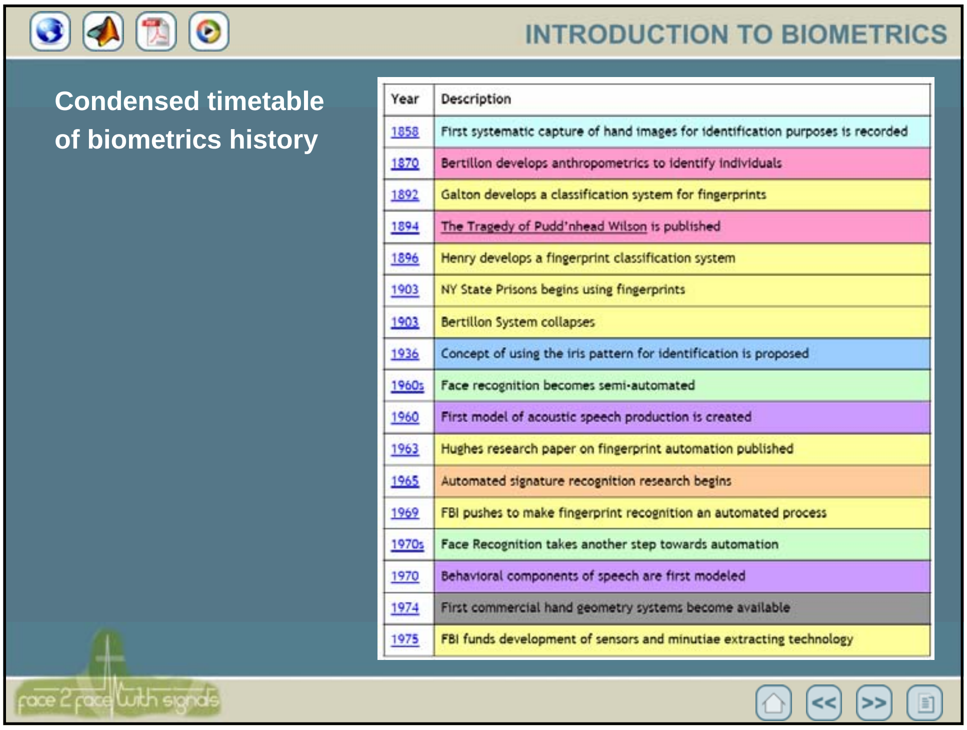
- Biometrics frequently asked questions
- Biometrics history
- Biometrics overview
- Biometrics testing and statistics



INTRODUCTION TO BIOMETRICS

The term “biometrics” is derived from the Greek words “bio” (life) and “metrics” (to measure). Automated biometric systems have only become available over the last few decades, due to significant advances in the field of computer processing. Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago.

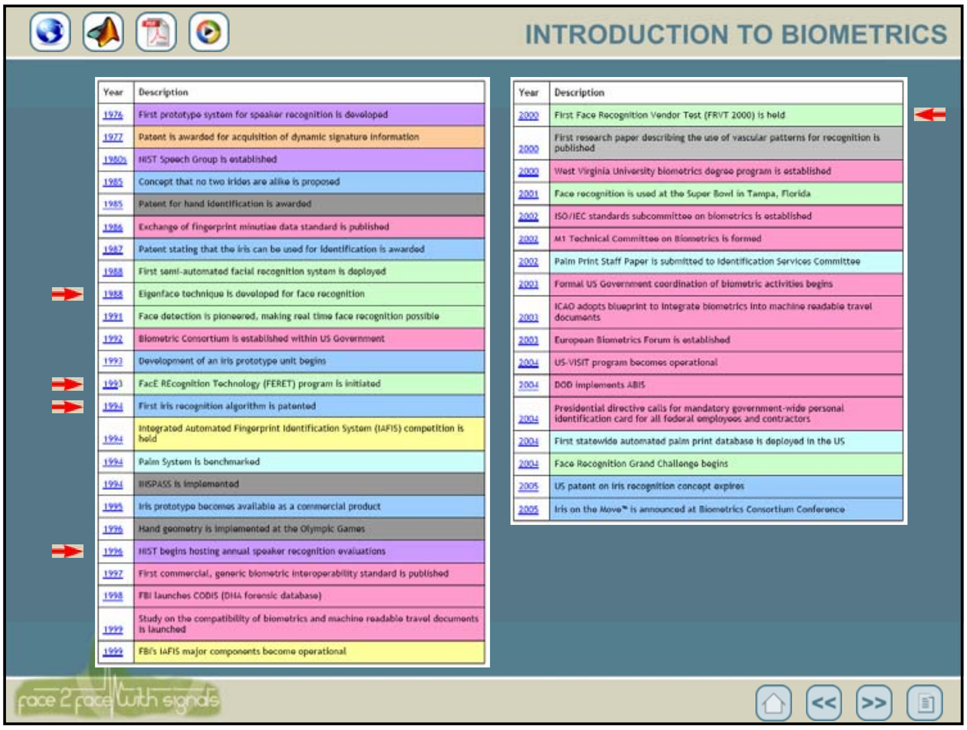
- In a cave estimated to be at least 31,000 years old, the walls are adorned with paintings believed to be created by prehistoric men who lived there. Surrounding these paintings are numerous handprints that are felt to “have…acted as an un-forgeable signature” of its originator.
- There is also evidence that fingerprints were used as a person’s mark as early as 500 B.C. “Babylonian business transactions are recorded in clay tablets that include fingerprints.”
- Joao de Barros, a Spanish explorer and writer, wrote that early Chinese merchants used fingerprints to settle business transactions. Chinese parents also used fingerprints and footprints to differentiate children from one another.



INTRODUCTION TO BIOMETRICS

Condensed timetable of biometrics history

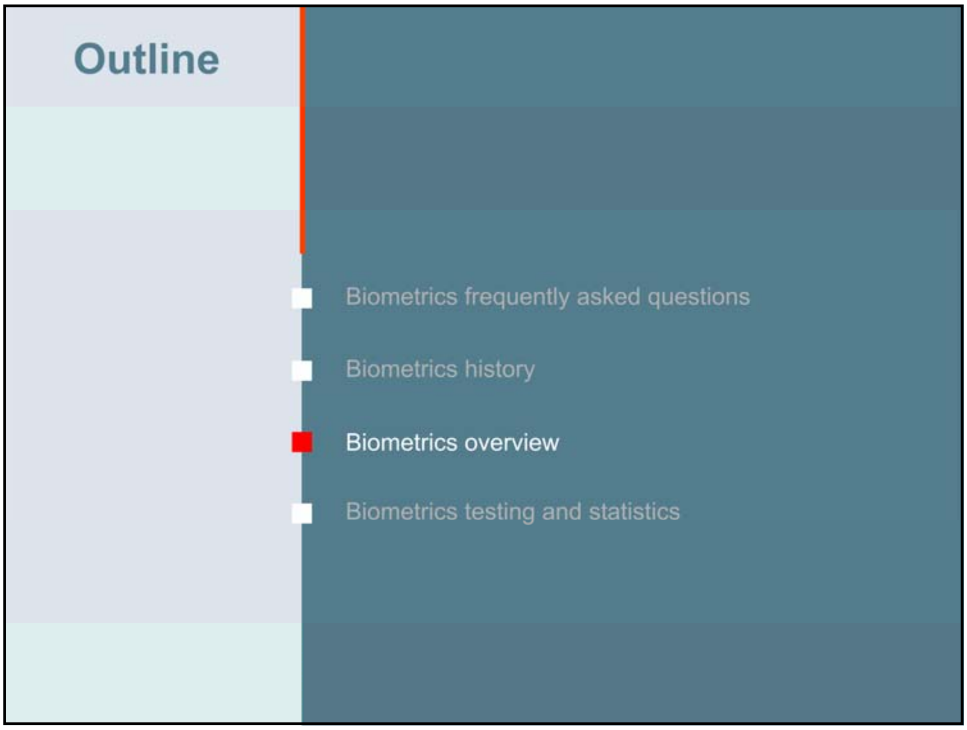
Year	Description
1858	First systematic capture of hand images for identification purposes is recorded
1870	Bertillon develops anthropometrics to identify individuals
1892	Galton develops a classification system for fingerprints
1894	The Tragedy of Pudd'nhead Wilson is published
1896	Henry develops a fingerprint classification system
1903	NY State Prisons begins using fingerprints
1903	Bertillon System collapses
1936	Concept of using the iris pattern for identification is proposed
1960s	Face recognition becomes semi-automated
1960	First model of acoustic speech production is created
1963	Hughes research paper on fingerprint automation published
1965	Automated signature recognition research begins
1969	FBI pushes to make fingerprint recognition an automated process
1970s	Face Recognition takes another step towards automation
1970	Behavioral components of speech are first modeled
1974	First commercial hand geometry systems become available
1975	FBI funds development of sensors and minutiae extracting technology



INTRODUCTION TO BIOMETRICS

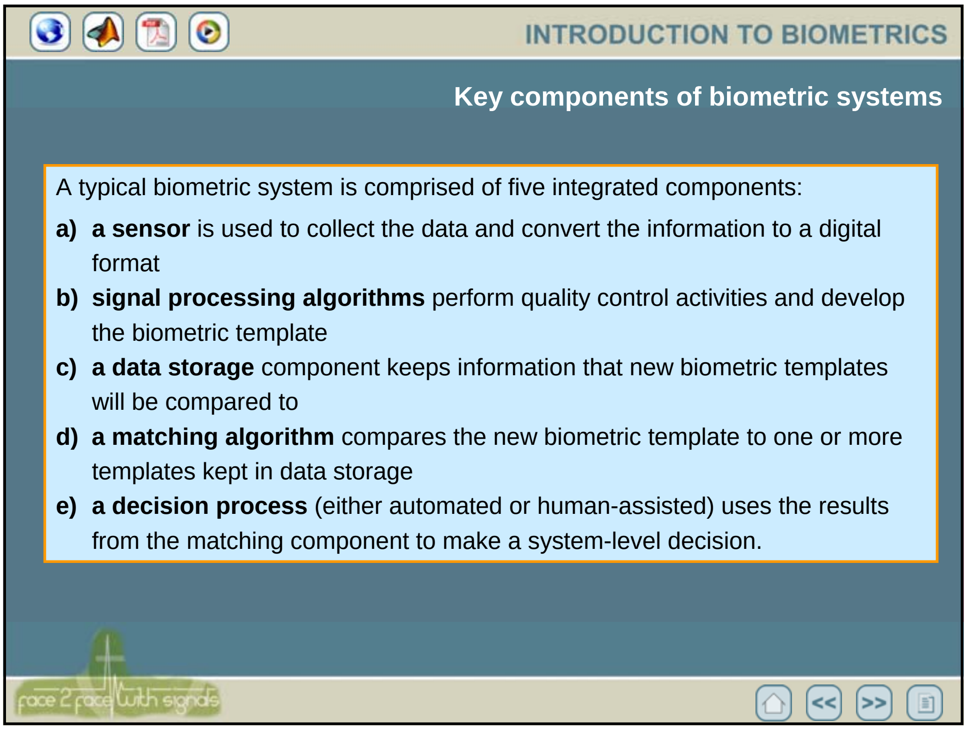
Year	Description
1976	First prototype system for speaker recognition is developed
1977	Patent is awarded for acquisition of dynamic signature information
1980s	NIST Speech Group is established
1985	Concept that no two irides are alike is proposed
1985	Patent for hand identification is awarded
1986	Exchange of fingerprint minutiae data standard is published
1987	Patent stating that the iris can be used for identification is awarded
1988	First semi-automated facial recognition system is deployed
1988	Eigenface technique is developed for face recognition
1991	Face detection is pioneered, making real time face recognition possible
1992	Biometric Consortium is established within US Government
1993	Development of an iris prototype unit begins
1993	FacE REcognition Technology (FERET) program is initiated
1994	First iris recognition algorithm is patented
1994	Integrated Automated Fingerprint Identification System (IAFIS) competition is held
1994	Palm System is benchmarked
1994	INSPASS is implemented
1995	Iris prototype becomes available as a commercial product
1996	Hand geometry is implemented at the Olympic Games
1996	NIST begins hosting annual speaker recognition evaluations
1997	First commercial, generic biometric interoperability standard is published
1998	FBI launches CODIS (DNA forensic database)
1999	Study on the compatibility of biometrics and machine readable travel documents is launched
1999	FBI's IAFIS major components become operational

Year	Description
2000	First Face Recognition Vendor Test (FRVT 2000) is held
2000	First research paper describing the use of vascular patterns for recognition is published
2000	West Virginia University biometrics degree program is established
2001	Face recognition is used at the Super Bowl in Tampa, Florida
2002	ISO/IEC standards subcommittee on biometrics is established
2002	M1 Technical Committee on Biometrics is formed
2002	Palm Print Staff Paper is submitted to Identification Services Committee
2003	Formal US Government coordination of biometric activities begins
2003	ICAO adopts blueprint to integrate biometrics into machine readable travel documents
2003	European Biometrics Forum is established
2004	US-VISIT program becomes operational
2004	DOD implements ABIS
2004	Presidential directive calls for mandatory government-wide personal identification card for all federal employees and contractors
2004	First statewide automated palm print database is deployed in the US
2004	Face Recognition Grand Challenge begins
2005	US patent on iris recognition concept expires
2005	Iris on the Move™ is announced at Biometrics Consortium Conference



Outline

- ■ Biometrics frequently asked questions
- ■ Biometrics history
- ■ Biometrics overview
- ■ Biometrics testing and statistics



INTRODUCTION TO BIOMETRICS

Key components of biometric systems

A typical biometric system is comprised of five integrated components:

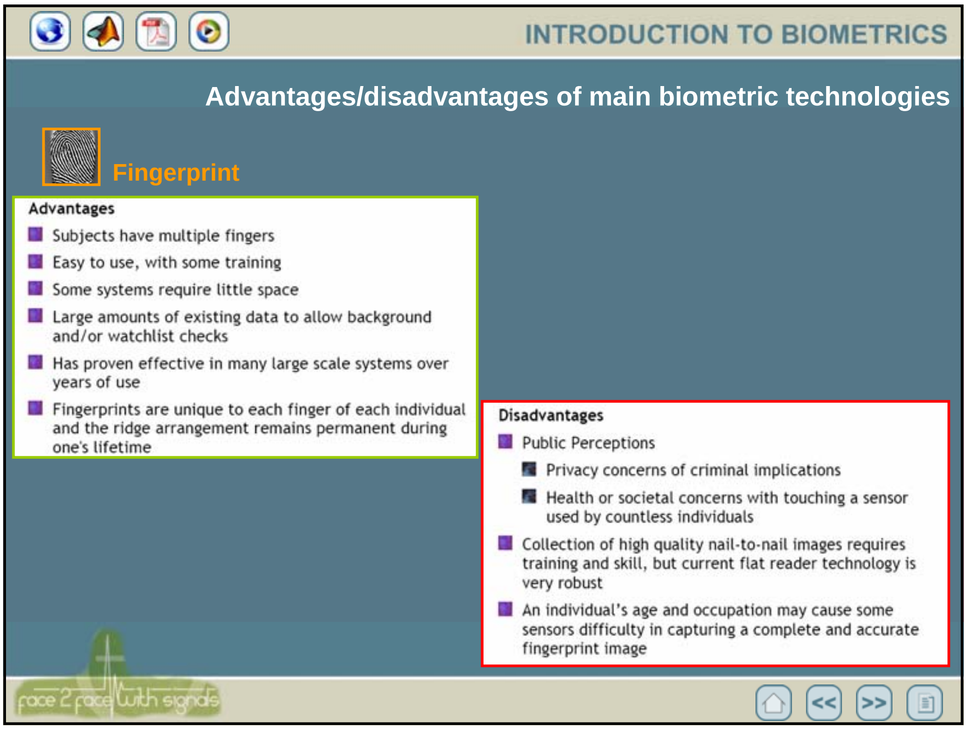
a) **a sensor** is used to collect the data and convert the information to a digital format

b) **signal processing algorithms** perform quality control activities and develop the biometric template

c) **a data storage** component keeps information that new biometric templates will be compared to

d) **a matching algorithm** compares the new biometric template to one or more templates kept in data storage

e) **a decision process** (either automated or human-assisted) uses the results from the matching component to make a system-level decision.



INTRODUCTION TO BIOMETRICS

Advantages/disadvantages of main biometric technologies

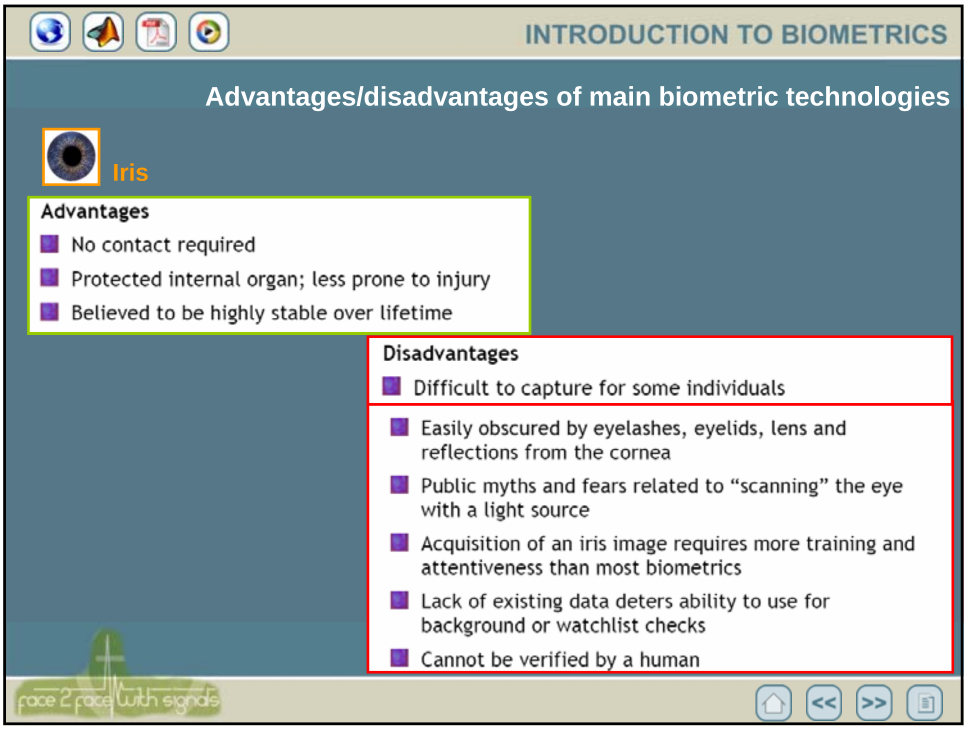
Fingerprint

Advantages

- Subjects have multiple fingers
- Easy to use, with some training
- Some systems require little space
- Large amounts of existing data to allow background and/or watchlist checks
- Has proven effective in many large scale systems over years of use
- Fingerprints are unique to each finger of each individual and the ridge arrangement remains permanent during one's lifetime

Disadvantages

- Public Perceptions
  - Privacy concerns of criminal implications
  - Health or societal concerns with touching a sensor used by countless individuals
- Collection of high quality nail-to-nail images requires training and skill, but current flat reader technology is very robust
- An individual's age and occupation may cause some sensors difficulty in capturing a complete and accurate fingerprint image



INTRODUCTION TO BIOMETRICS

Advantages/disadvantages of main biometric technologies

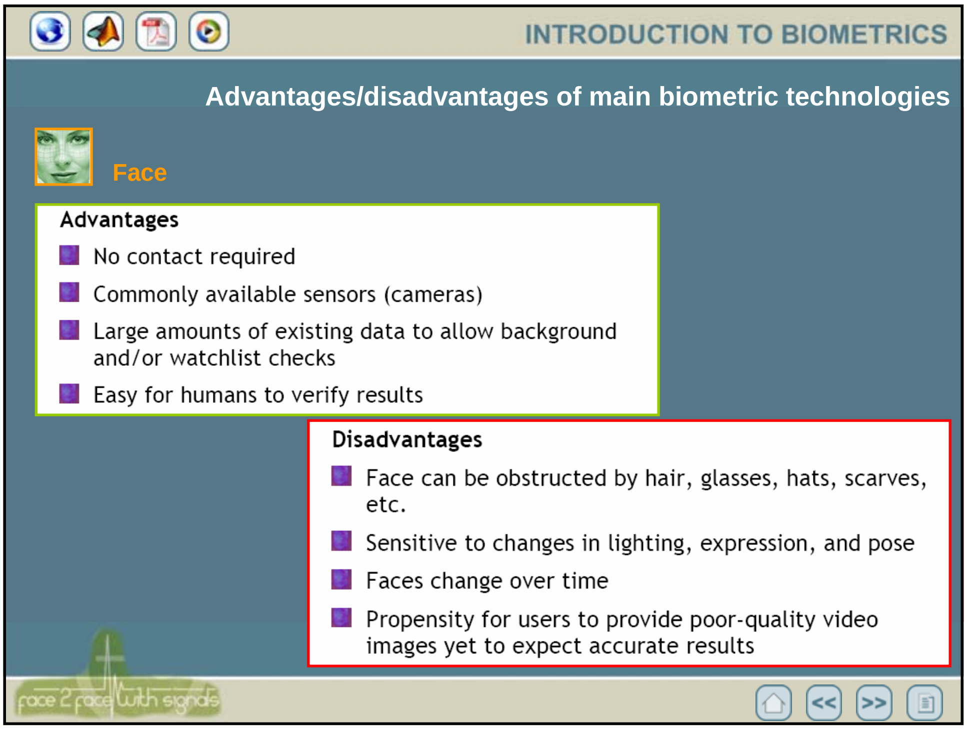
Iris

Advantages

- No contact required
- Protected internal organ; less prone to injury
- Believed to be highly stable over lifetime

Disadvantages

- Difficult to capture for some individuals
- Easily obscured by eyelashes, eyelids, lens and reflections from the cornea
- Public myths and fears related to "scanning" the eye with a light source
- Acquisition of an iris image requires more training and attentiveness than most biometrics
- Lack of existing data deters ability to use for background or watchlist checks
- Cannot be verified by a human



INTRODUCTION TO BIOMETRICS

Advantages/disadvantages of main biometric technologies

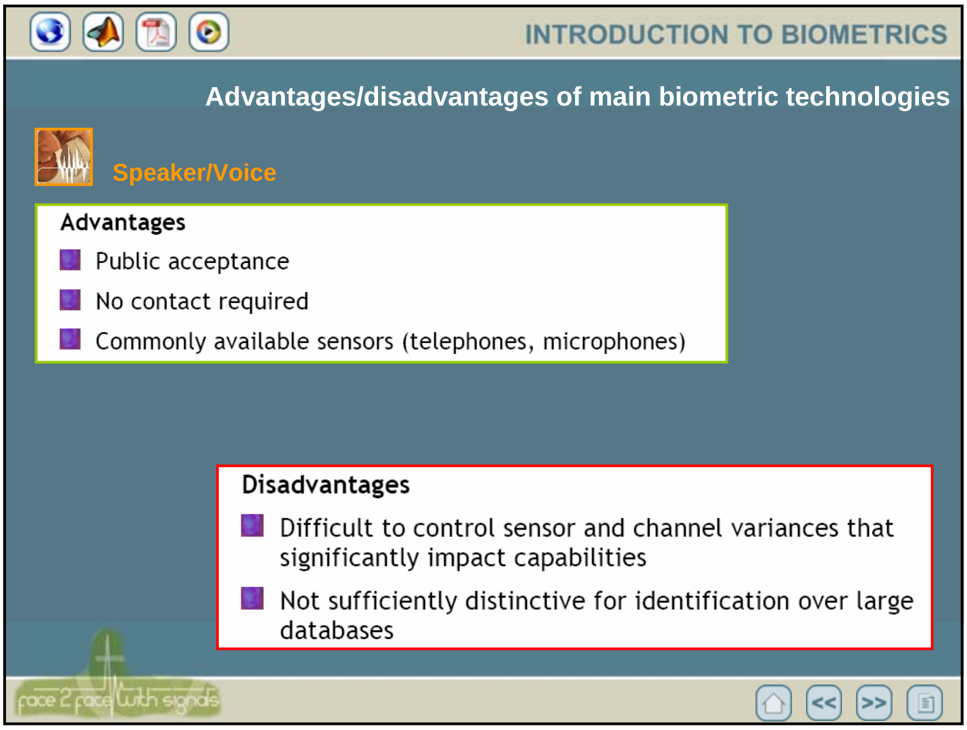
Face

Advantages

- No contact required
- Commonly available sensors (cameras)
- Large amounts of existing data to allow background and/or watchlist checks
- Easy for humans to verify results

Disadvantages

- Face can be obstructed by hair, glasses, hats, scarves, etc.
- Sensitive to changes in lighting, expression, and pose
- Faces change over time
- Propensity for users to provide poor-quality video images yet to expect accurate results



INTRODUCTION TO BIOMETRICS

Advantages/disadvantages of main biometric technologies

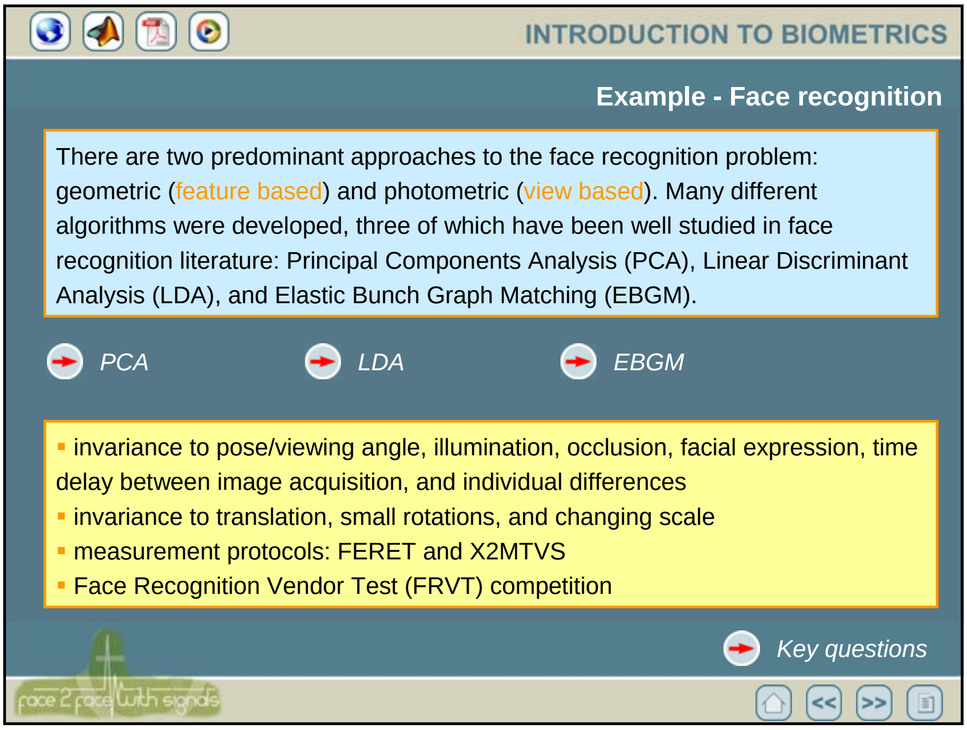
Speaker/Voice

Advantages

- Public acceptance
- No contact required
- Commonly available sensors (telephones, microphones)

Disadvantages

- Difficult to control sensor and channel variances that significantly impact capabilities
- Not sufficiently distinctive for identification over large databases



INTRODUCTION TO BIOMETRICS

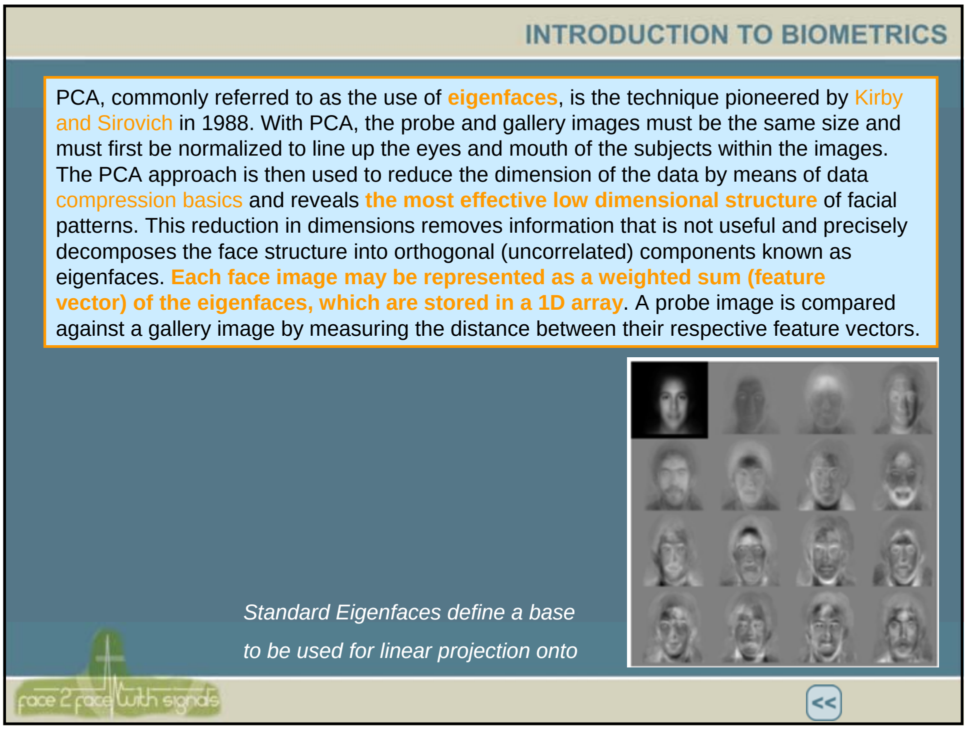
Example - Face recognition

There are two predominant approaches to the face recognition problem: geometric (feature based) and photometric (view based). Many different algorithms were developed, three of which have been well studied in face recognition literature: Principal Components Analysis (PCA), Linear Discriminant Analysis (LDA), and Elastic Bunch Graph Matching (EBGM).

➔ *PCA* ➔ *LDA* ➔ *EBGM*

- invariance to pose/viewing angle, illumination, occlusion, facial expression, time delay between image acquisition, and individual differences
- invariance to translation, small rotations, and changing scale
- measurement protocols: FERET and X2MTVS
- Face Recognition Vendor Test (FRVT) competition

➔ *Key questions*



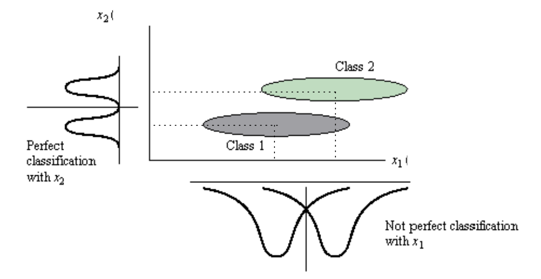
INTRODUCTION TO BIOMETRICS

PCA, commonly referred to as the use of **eigenfaces**, is the technique pioneered by Kirby and Sirovich in 1988. With PCA, the probe and gallery images must be the same size and must first be normalized to line up the eyes and mouth of the subjects within the images. The PCA approach is then used to reduce the dimension of the data by means of data compression basics and reveals **the most effective low dimensional structure** of facial patterns. This reduction in dimensions removes information that is not useful and precisely decomposes the face structure into orthogonal (uncorrelated) components known as eigenfaces. **Each face image may be represented as a weighted sum (feature vector) of the eigenfaces, which are stored in a 1D array**. A probe image is compared against a gallery image by measuring the distance between their respective feature vectors.

Standard Eigenfaces define a base to be used for linear projection onto

INTRODUCTION TO BIOMETRICS

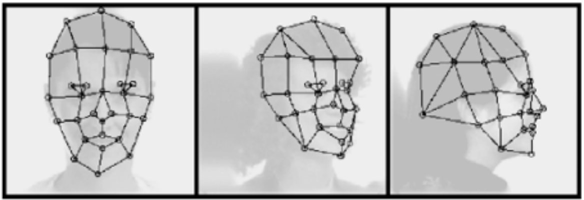
LDA is a statistical approach for classifying samples of unknown classes based on training samples with known classes. This technique aims to maximize between-class (i.e., across users) variance and minimize within-class (i.e., within user) variance. When dealing with high dimensional face data, this technique faces the small sample size problem that arises where there are a small number of available training samples compared to the dimensionality of the sample space.


x_2
Class 2
Class 1
x_1
Perfect classification with x_2
Not perfect classification with x_1

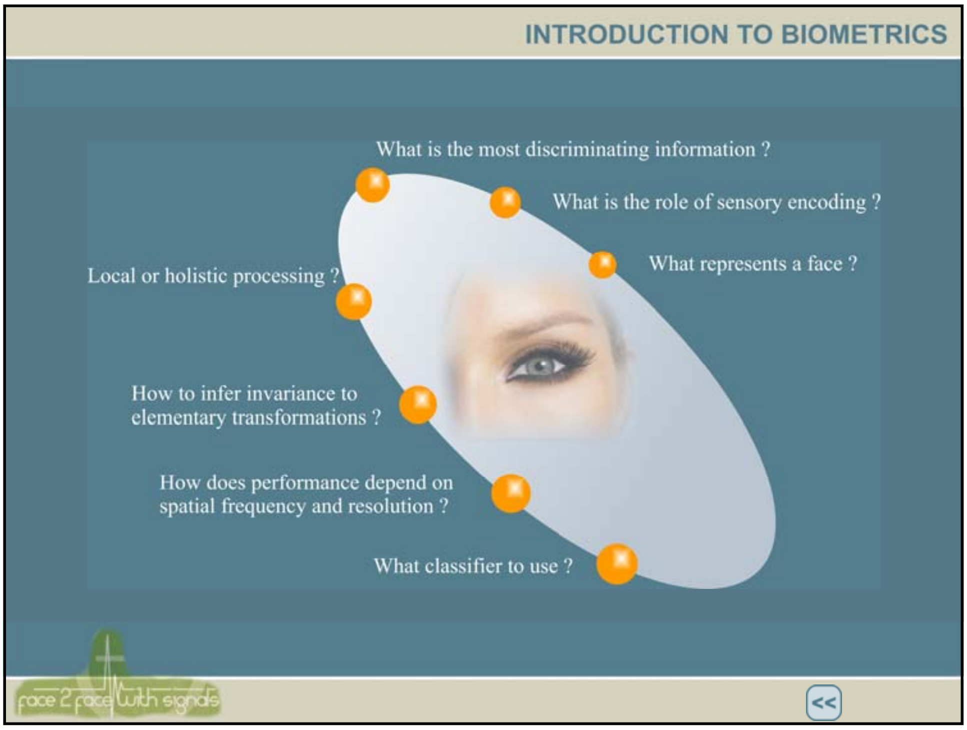
LDA seeks maximum discriminability berween clases, whereas PCA minimizes reconstruction error

INTRODUCTION TO BIOMETRICS

EBGM relies on the concept that real face images have many nonlinear characteristics that are not addressed by the linear analysis methods discussed earlier, such as variations in illumination, pose and expression. A Gabor wavelet transform creates a dynamic link architecture that projects the face onto an elastic grid. The **Gabor jet** is a node on the elastic grid, notated by circles on the image below, which describes the image behavior around a given pixel. It is the result of a convolution of the image with a Gabor filter, which is used to detect shapes and to extract features using image processing.
Recognition is based on the similarity of the Gabor filter response at each Gabor node. This biologically-based method using Gabor filters is a process executed in the visual cortex of higher mammals. The difficulty with this method is the requirement of accurate landmark localization, which can sometimes be achieved by combining PCA and LDA methods.

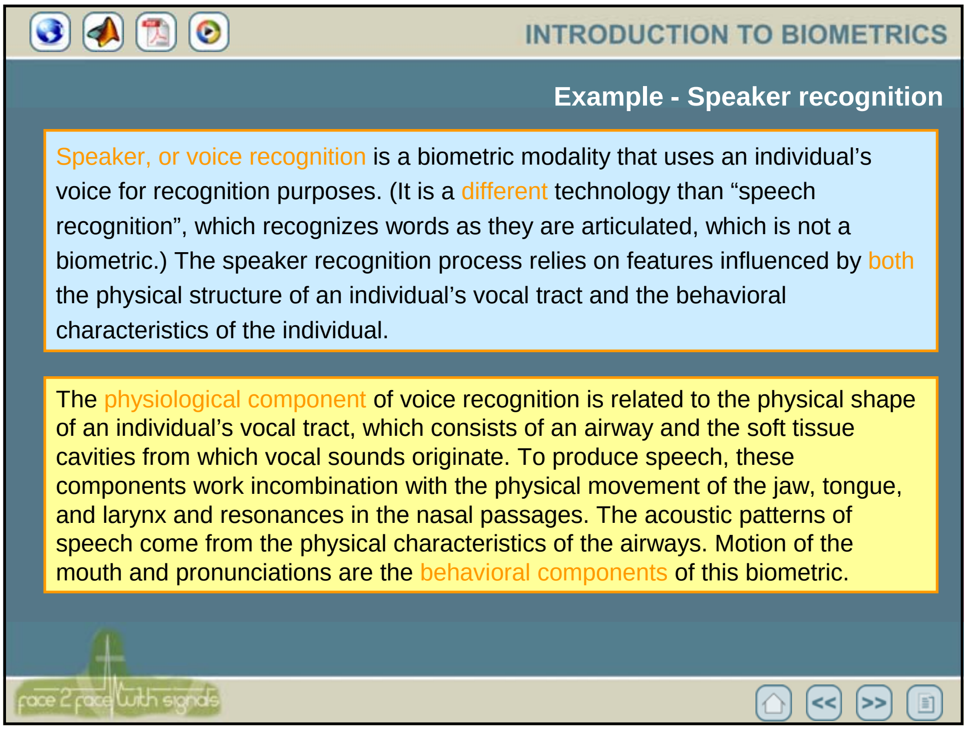


Elastic Bunch Map Graphing



INTRODUCTION TO BIOMETRICS

What is the most discriminating information ?
What is the role of sensory encoding ?
What represents a face ?
Local or holistic processing ?
How to infer invariance to elementary transformations ?
How does performance depend on spatial frequency and resolution ?
What classifier to use ?
<<

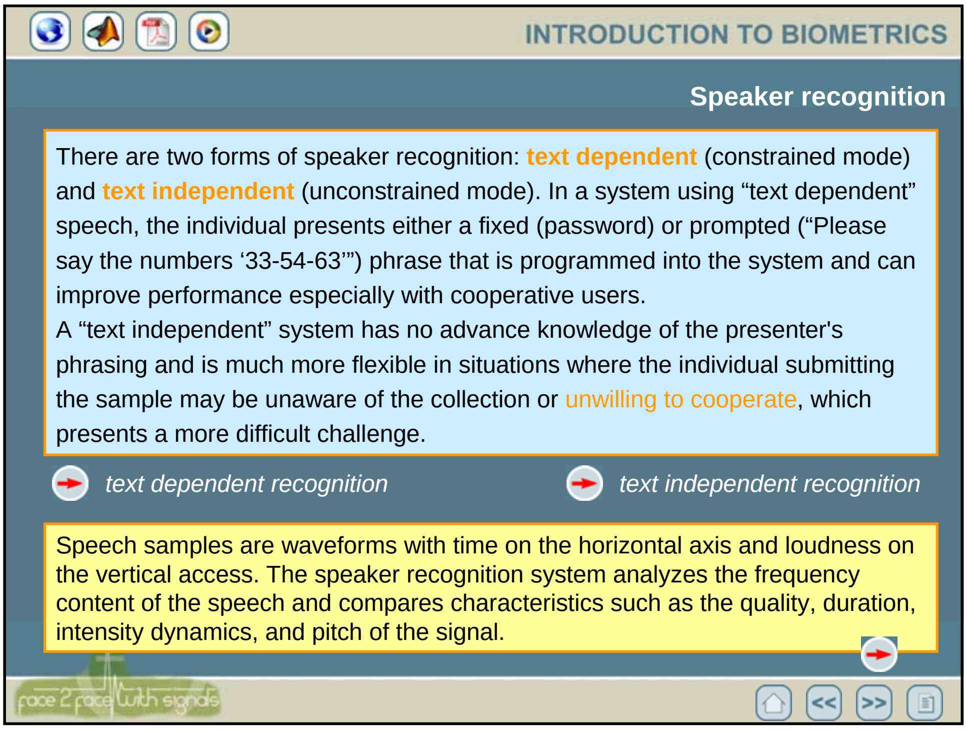


INTRODUCTION TO BIOMETRICS

Example - Speaker recognition

Speaker, or voice recognition is a biometric modality that uses an individual's voice for recognition purposes. (It is a different technology than "speech recognition", which recognizes words as they are articulated, which is not a biometric.) The speaker recognition process relies on features influenced by both the physical structure of an individual's vocal tract and the behavioral characteristics of the individual.

The physiological component of voice recognition is related to the physical shape of an individual's vocal tract, which consists of an airway and the soft tissue cavities from which vocal sounds originate. To produce speech, these components work incombination with the physical movement of the jaw, tongue, and larynx and resonances in the nasal passages. The acoustic patterns of speech come from the physical characteristics of the airways. Motion of the mouth and pronunciations are the behavioral components of this biometric.



INTRODUCTION TO BIOMETRICS

Speaker recognition

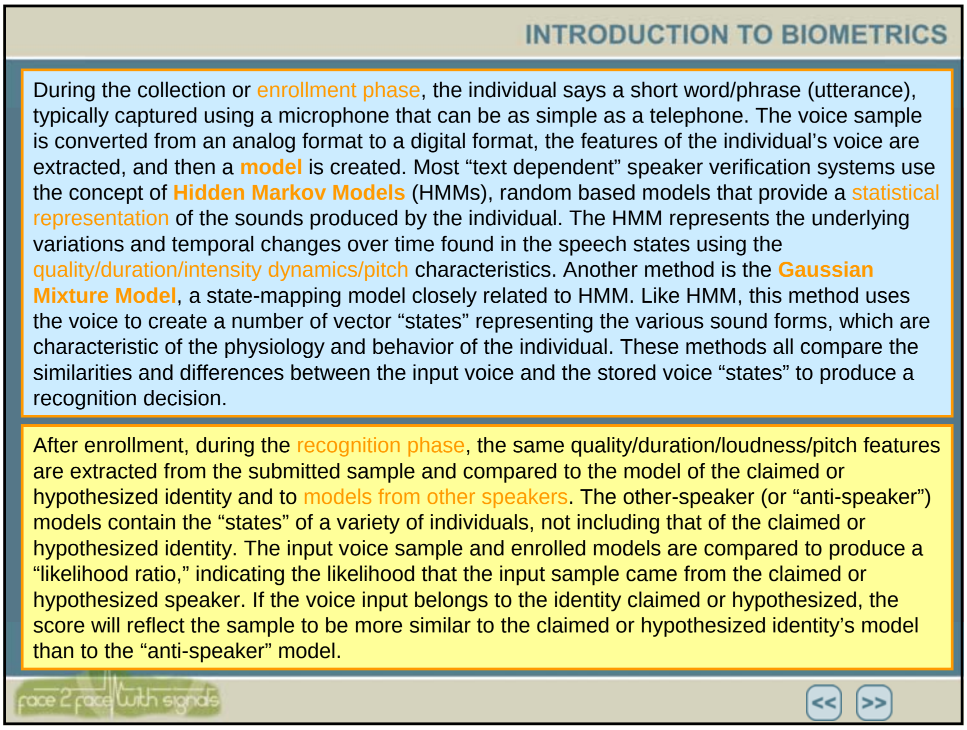
There are two forms of speaker recognition: **text dependent** (constrained mode) and **text independent** (unconstrained mode). In a system using “text dependent” speech, the individual presents either a fixed (password) or prompted (“Please say the numbers ‘33-54-63’”) phrase that is programmed into the system and can improve performance especially with cooperative users.

A “text independent” system has no advance knowledge of the presenter's phrasing and is much more flexible in situations where the individual submitting the sample may be unaware of the collection or unwilling to cooperate, which presents a more difficult challenge.

text dependent recognition

text independent recognition

Speech samples are waveforms with time on the horizontal axis and loudness on the vertical access. The speaker recognition system analyzes the frequency content of the speech and compares characteristics such as the quality, duration, intensity dynamics, and pitch of the signal.

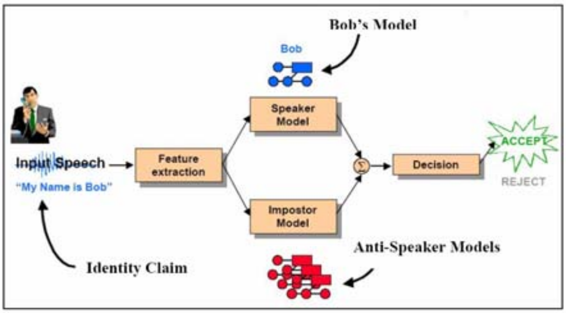


INTRODUCTION TO BIOMETRICS

During the collection or enrollment phase, the individual says a short word/phrase (utterance), typically captured using a microphone that can be as simple as a telephone. The voice sample is converted from an analog format to a digital format, the features of the individual’s voice are extracted, and then a **model** is created. Most “text dependent” speaker verification systems use the concept of **Hidden Markov Models** (HMMs), random based models that provide a statistical representation of the sounds produced by the individual. The HMM represents the underlying variations and temporal changes over time found in the speech states using the quality/duration/intensity dynamics/pitch characteristics. Another method is the **Gaussian Mixture Model**, a state-mapping model closely related to HMM. Like HMM, this method uses the voice to create a number of vector “states” representing the various sound forms, which are characteristic of the physiology and behavior of the individual. These methods all compare the similarities and differences between the input voice and the stored voice “states” to produce a recognition decision.

After enrollment, during the recognition phase, the same quality/duration/loudness/pitch features are extracted from the submitted sample and compared to the model of the claimed or hypothesized identity and to models from other speakers. The other-speaker (or “anti-speaker”) models contain the “states” of a variety of individuals, not including that of the claimed or hypothesized identity. The input voice sample and enrolled models are compared to produce a “likelihood ratio,” indicating the likelihood that the input sample came from the claimed or hypothesized speaker. If the voice input belongs to the identity claimed or hypothesized, the score will reflect the sample to be more similar to the claimed or hypothesized identity’s model than to the “anti-speaker” model.

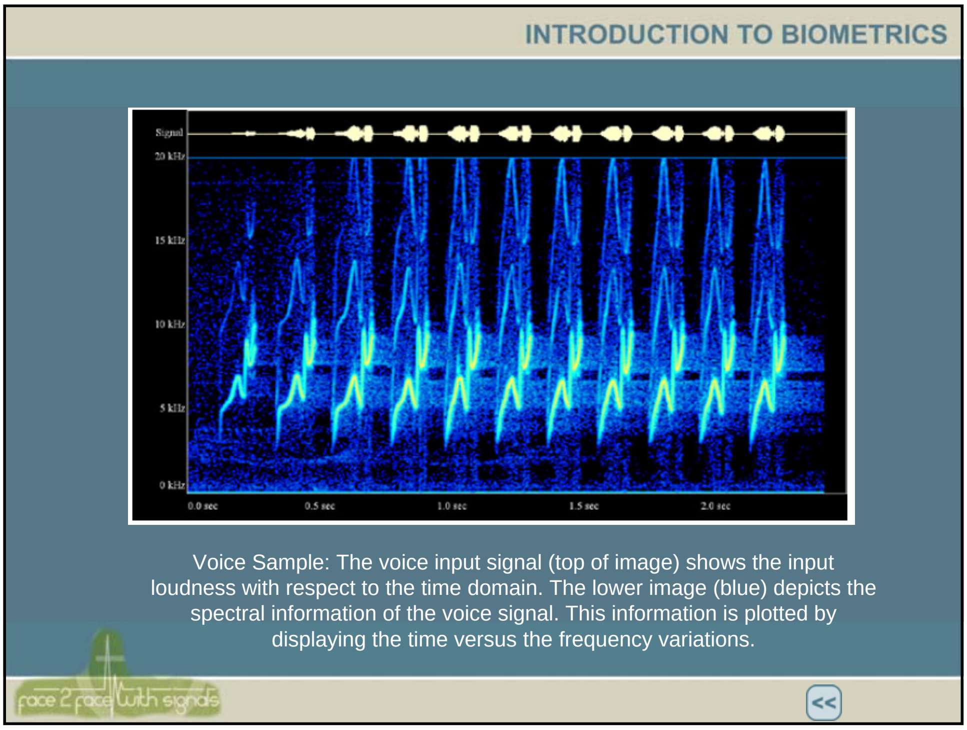
INTRODUCTION TO BIOMETRICS



Major weakness of speaker recognition are susceptibility to transmission channel and microphone variability and noise: systems can face problems when end users have enrolled on a clean landline phone and attempt verification using a noisy cellular phone. Speaker verification systems, except those using prompted phrases, are also susceptible to spoofing attacks through the use of recorded voice (requiring the utterance of a specified and random word or phrase may combat this weakness).

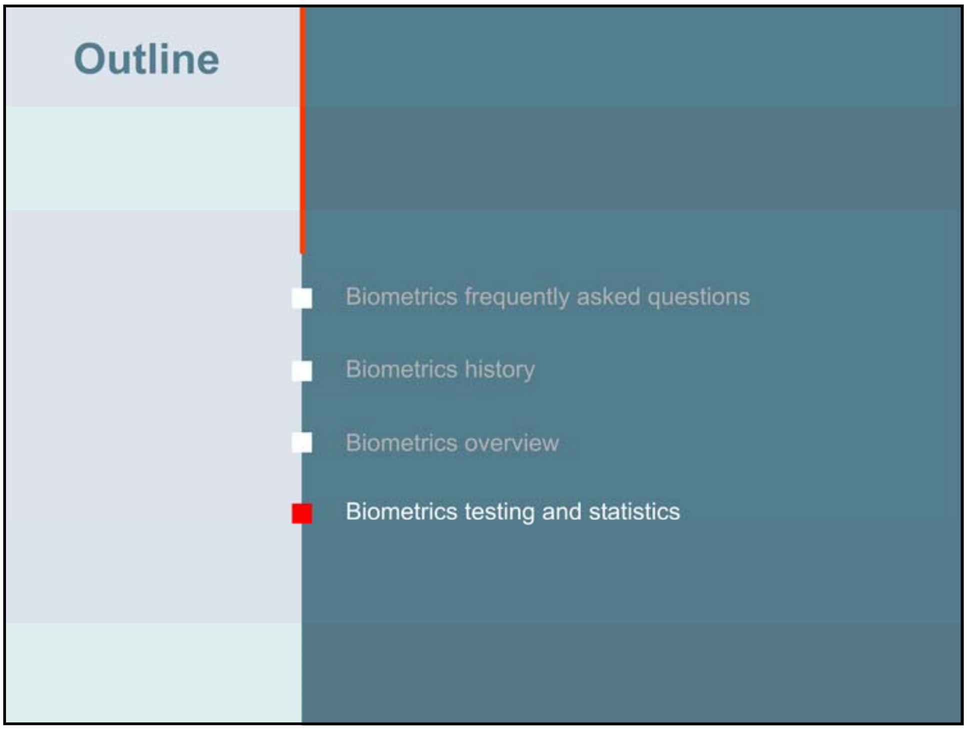
INTRODUCTION TO BIOMETRICS

Current research in the area of "text independent" speaker recognition is mainly focused on moving beyond the low-level spectral analysis previously discussed. Although the spectral level of information is still the driving force behind the recognitions, fusing higher level characteristics with the low level spectral information is becoming a popular laboratory technique. (Examples of higher level characteristics include: prosodic characteristics such as rhythm, speed, modulation and intonation, based on personality type and parental influence; and semantics, idiolects, pronunciations and idiosyncrasies, related to birthplace, socio-economic status, and education level.) Higher level characteristics can be combined with the underlying low-level spectral information to improve the performance of "text independent" speaker recognition systems.



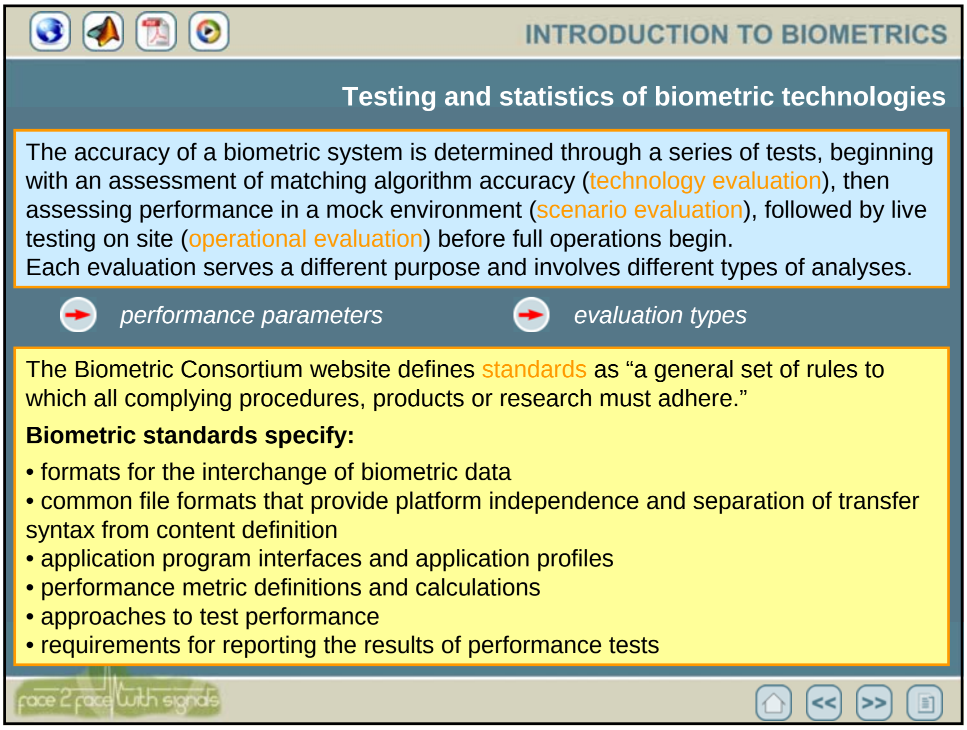
INTRODUCTION TO BIOMETRICS

Voice Sample: The voice input signal (top of image) shows the input loudness with respect to the time domain. The lower image (blue) depicts the spectral information of the voice signal. This information is plotted by displaying the time versus the frequency variations.



Outline

- Biometrics frequently asked questions
- Biometrics history
- Biometrics overview
- Biometrics testing and statistics



INTRODUCTION TO BIOMETRICS

Testing and statistics of biometric technologies

The accuracy of a biometric system is determined through a series of tests, beginning with an assessment of matching algorithm accuracy (technology evaluation), then assessing performance in a mock environment (scenario evaluation), followed by live testing on site (operational evaluation) before full operations begin.
Each evaluation serves a different purpose and involves different types of analyses.

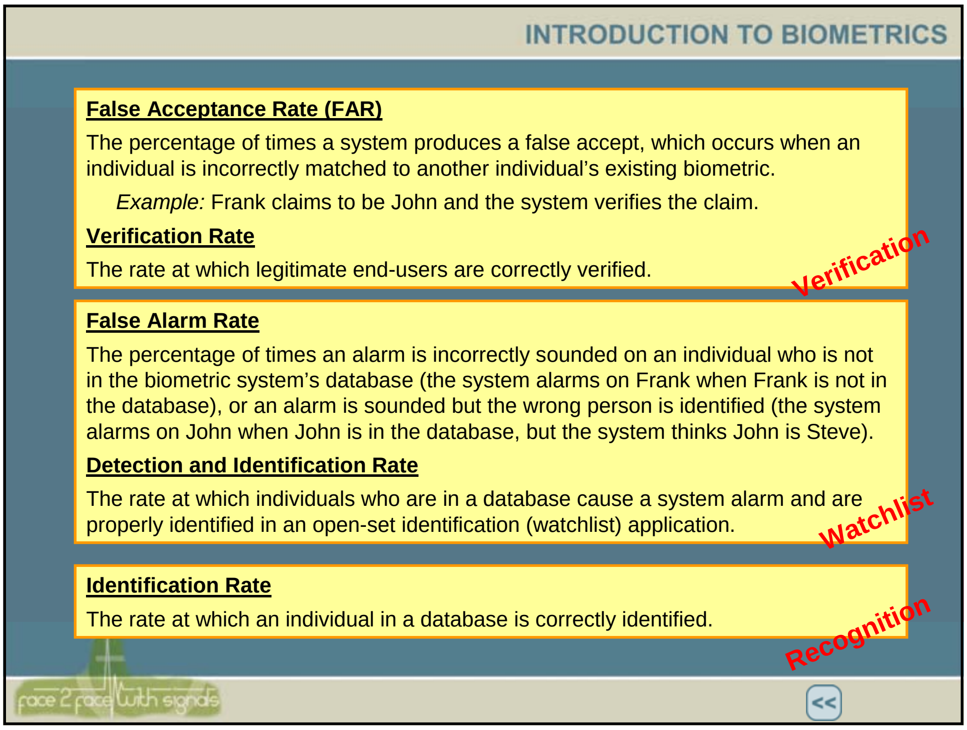
performance parameters

evaluation types

The Biometric Consortium website defines standards as “a general set of rules to which all complying procedures, products or research must adhere.”

Biometric standards specify:

- formats for the interchange of biometric data
- common file formats that provide platform independence and separation of transfer syntax from content definition
- application program interfaces and application profiles
- performance metric definitions and calculations
- approaches to test performance
- requirements for reporting the results of performance tests



INTRODUCTION TO BIOMETRICS

False Acceptance Rate (FAR)

The percentage of times a system produces a false accept, which occurs when an individual is incorrectly matched to another individual’s existing biometric.

Example: Frank claims to be John and the system verifies the claim.

Verification Rate

The rate at which legitimate end-users are correctly verified.

Verification

False Alarm Rate

The percentage of times an alarm is incorrectly sounded on an individual who is not in the biometric system’s database (the system alarms on Frank when Frank is not in the database), or an alarm is sounded but the wrong person is identified (the system alarms on John when John is in the database, but the system thinks John is Steve).

Detection and Identification Rate

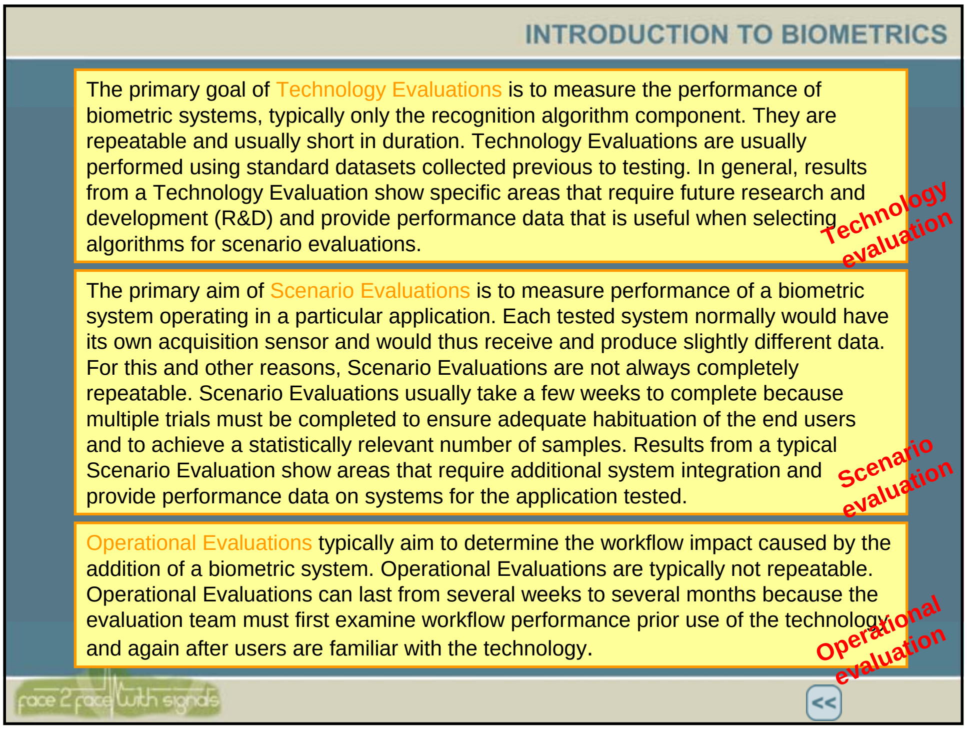
The rate at which individuals who are in a database cause a system alarm and are properly identified in an open-set identification (watchlist) application.

Watchlist

Identification Rate

The rate at which an individual in a database is correctly identified.

Recognition



INTRODUCTION TO BIOMETRICS

The primary goal of Technology Evaluations is to measure the performance of biometric systems, typically only the recognition algorithm component. They are repeatable and usually short in duration. Technology Evaluations are usually performed using standard datasets collected previous to testing. In general, results from a Technology Evaluation show specific areas that require future research and development (R&D) and provide performance data that is useful when selecting algorithms for scenario evaluations.

Technology evaluation

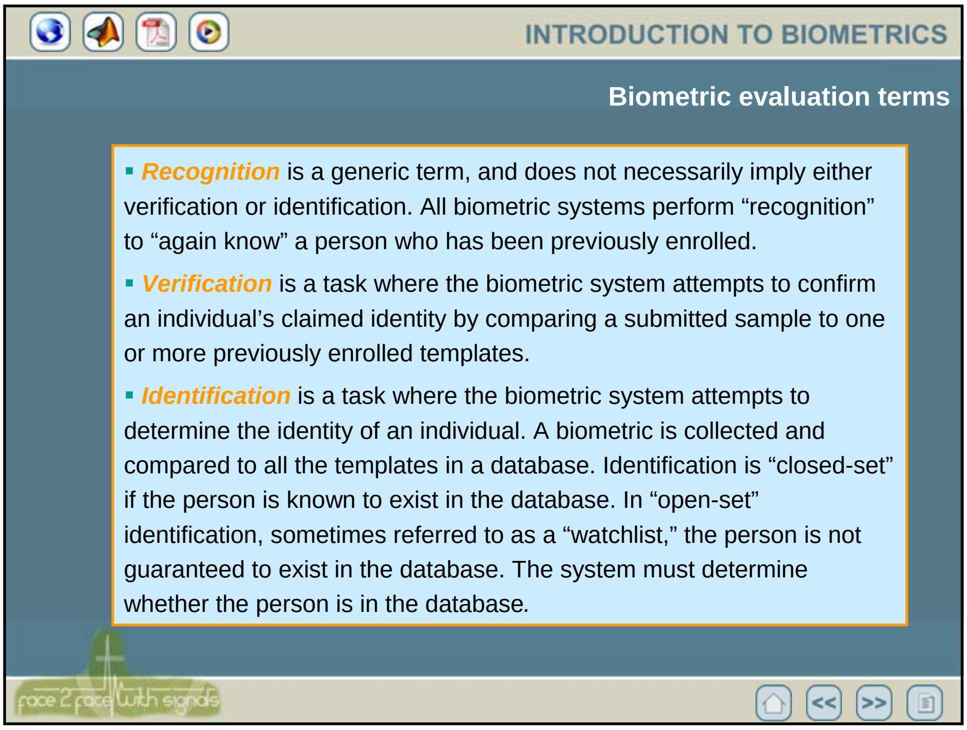
The primary aim of Scenario Evaluations is to measure performance of a biometric system operating in a particular application. Each tested system normally would have its own acquisition sensor and would thus receive and produce slightly different data. For this and other reasons, Scenario Evaluations are not always completely repeatable. Scenario Evaluations usually take a few weeks to complete because multiple trials must be completed to ensure adequate habituation of the end users and to achieve a statistically relevant number of samples. Results from a typical Scenario Evaluation show areas that require additional system integration and provide performance data on systems for the application tested.

Scenario evaluation

Operational Evaluations typically aim to determine the workflow impact caused by the addition of a biometric system. Operational Evaluations are typically not repeatable. Operational Evaluations can last from several weeks to several months because the evaluation team must first examine workflow performance prior use of the technology and again after users are familiar with the technology.

Operational evaluation

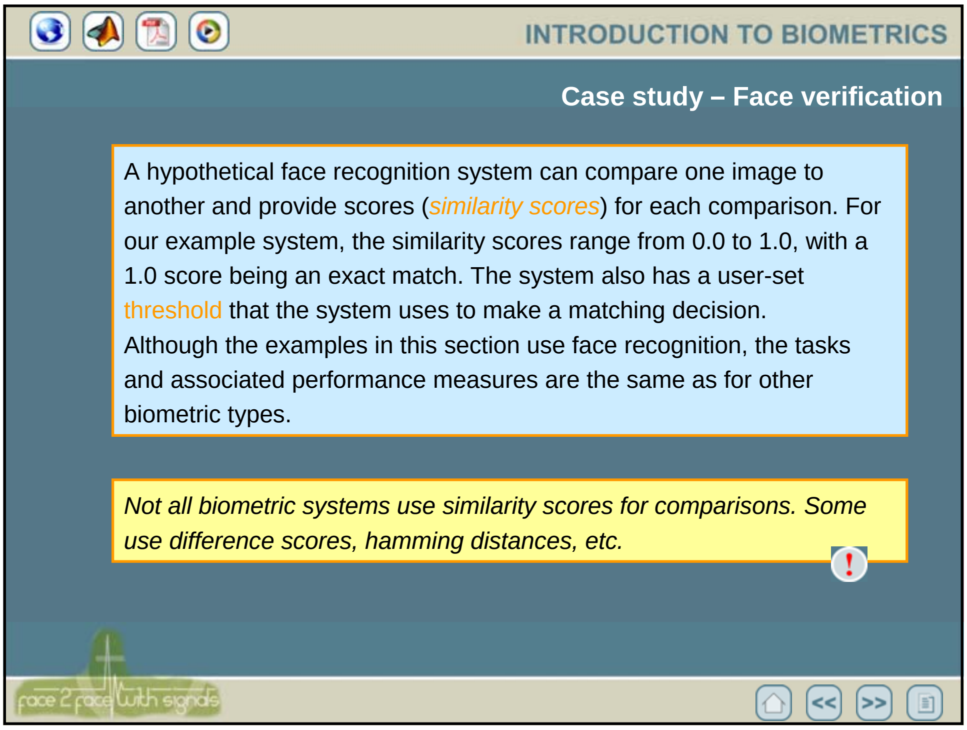
face 2 face with signals
<<



INTRODUCTION TO BIOMETRICS

Biometric evaluation terms

- ***Recognition*** is a generic term, and does not necessarily imply either verification or identification. All biometric systems perform “recognition” to “again know” a person who has been previously enrolled.
- ***Verification*** is a task where the biometric system attempts to confirm an individual’s claimed identity by comparing a submitted sample to one or more previously enrolled templates.
- ***Identification*** is a task where the biometric system attempts to determine the identity of an individual. A biometric is collected and compared to all the templates in a database. Identification is “closed-set” if the person is known to exist in the database. In “open-set” identification, sometimes referred to as a “watchlist,” the person is not guaranteed to exist in the database. The system must determine whether the person is in the database.

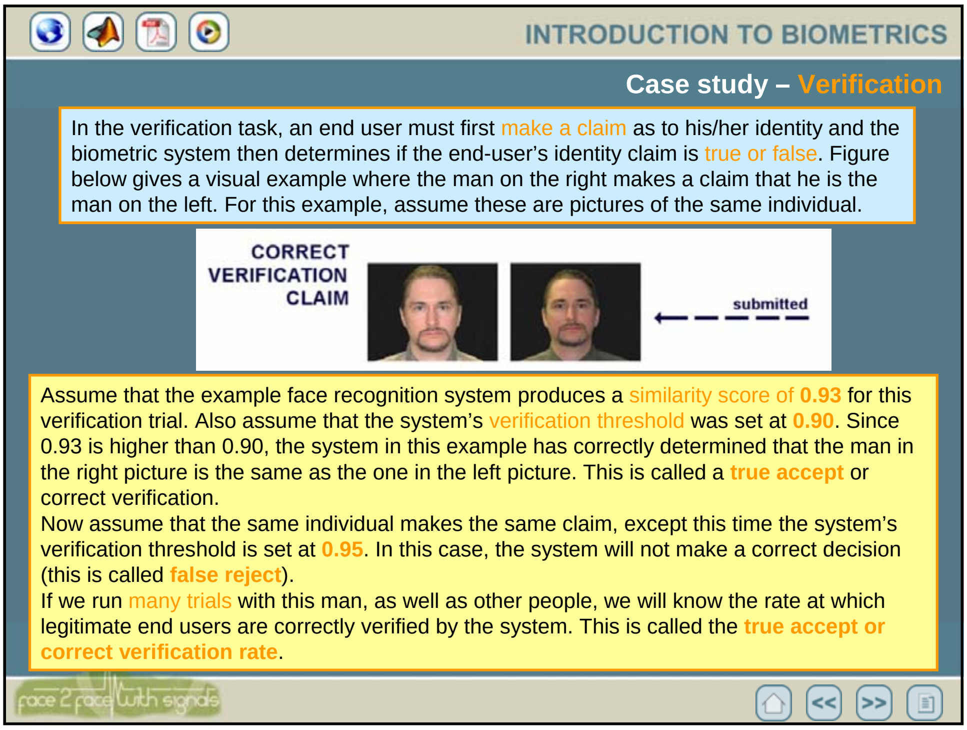


INTRODUCTION TO BIOMETRICS

Case study – Face verification

A hypothetical face recognition system can compare one image to another and provide scores (*similarity scores*) for each comparison. For our example system, the similarity scores range from 0.0 to 1.0, with a 1.0 score being an exact match. The system also has a user-set threshold that the system uses to make a matching decision.
Although the examples in this section use face recognition, the tasks and associated performance measures are the same as for other biometric types.

Not all biometric systems use similarity scores for comparisons. Some use difference scores, hamming distances, etc.

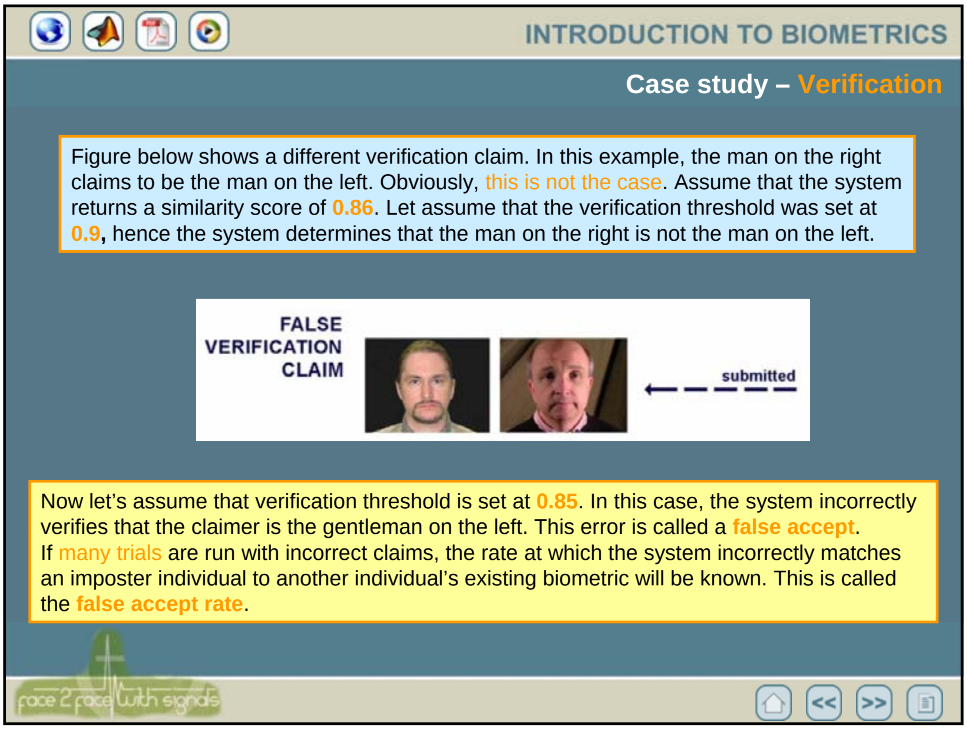


INTRODUCTION TO BIOMETRICS

Case study – Verification

In the verification task, an end user must first make a claim as to his/her identity and the biometric system then determines if the end-user's identity claim is true or false. Figure below gives a visual example where the man on the right makes a claim that he is the man on the left. For this example, assume these are pictures of the same individual.

Assume that the example face recognition system produces a similarity score of **0.93** for this verification trial. Also assume that the system's verification threshold was set at **0.90**. Since 0.93 is higher than 0.90, the system in this example has correctly determined that the man in the right picture is the same as the one in the left picture. This is called a **true accept** or correct verification.
Now assume that the same individual makes the same claim, except this time the system's verification threshold is set at **0.95**. In this case, the system will not make a correct decision (this is called **false reject**).
If we run many trials with this man, as well as other people, we will know the rate at which legitimate end users are correctly verified by the system. This is called the **true accept or correct verification rate**.

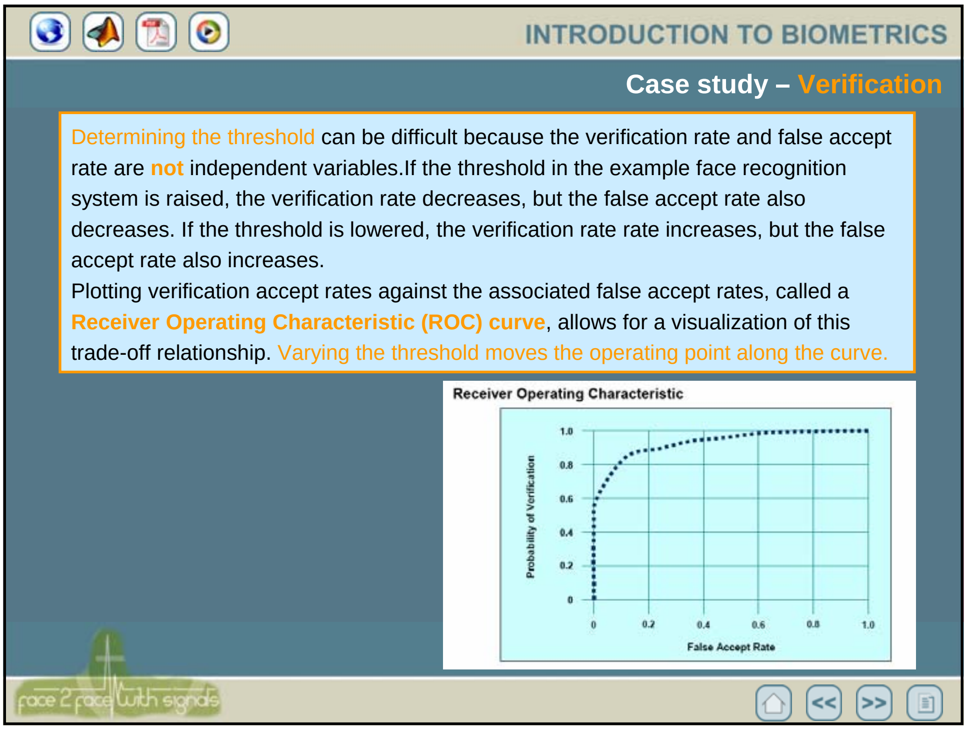


INTRODUCTION TO BIOMETRICS

Case study – Verification

Figure below shows a different verification claim. In this example, the man on the right claims to be the man on the left. Obviously, this is not the case. Assume that the system returns a similarity score of **0.86**. Let assume that the verification threshold was set at **0.9**, hence the system determines that the man on the right is not the man on the left.

Now let's assume that verification threshold is set at **0.85**. In this case, the system incorrectly verifies that the claimer is the gentleman on the left. This error is called a **false accept**.
If many trials are run with incorrect claims, the rate at which the system incorrectly matches an imposter individual to another individual's existing biometric will be known. This is called the **false accept rate**.

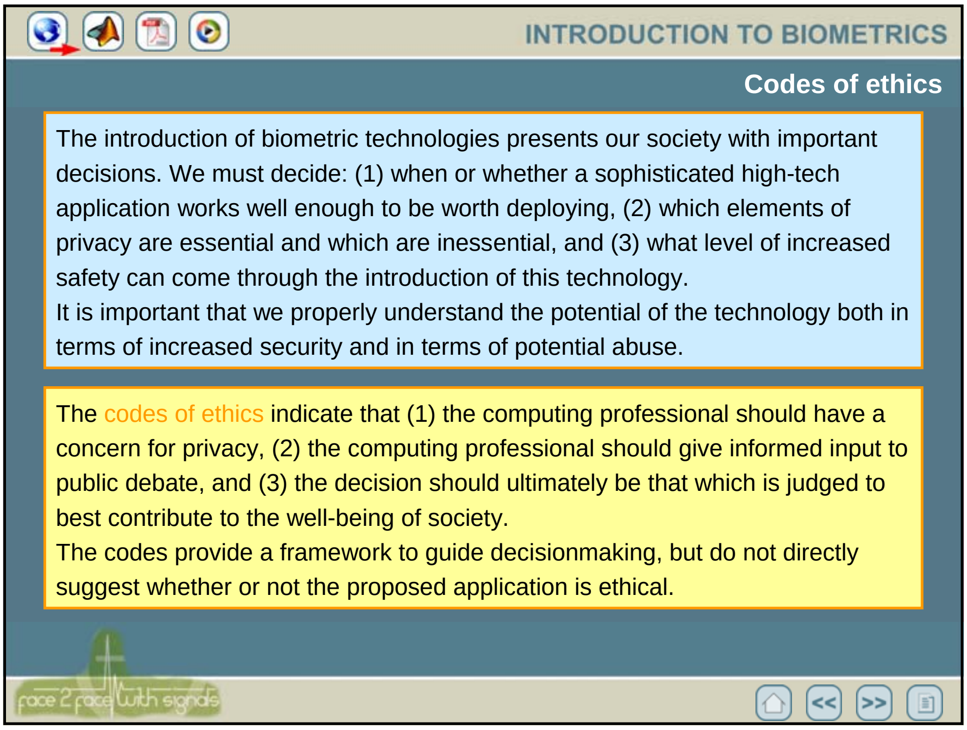


INTRODUCTION TO BIOMETRICS

Case study – Verification

Determining the threshold can be difficult because the verification rate and false accept rate are **not** independent variables.If the threshold in the example face recognition system is raised, the verification rate decreases, but the false accept rate also decreases. If the threshold is lowered, the verification rate rate increases, but the false accept rate also increases.
Plotting verification accept rates against the associated false accept rates, called a **Receiver Operating Characteristic (ROC) curve**, allows for a visualization of this trade-off relationship. Varying the threshold moves the operating point along the curve.

Receiver Operating Characteristic
Probability of Verification
1.0
0.8
0.6
0.4
0.2
0
0
0.2
0.4
0.6
0.8
1.0
False Accept Rate

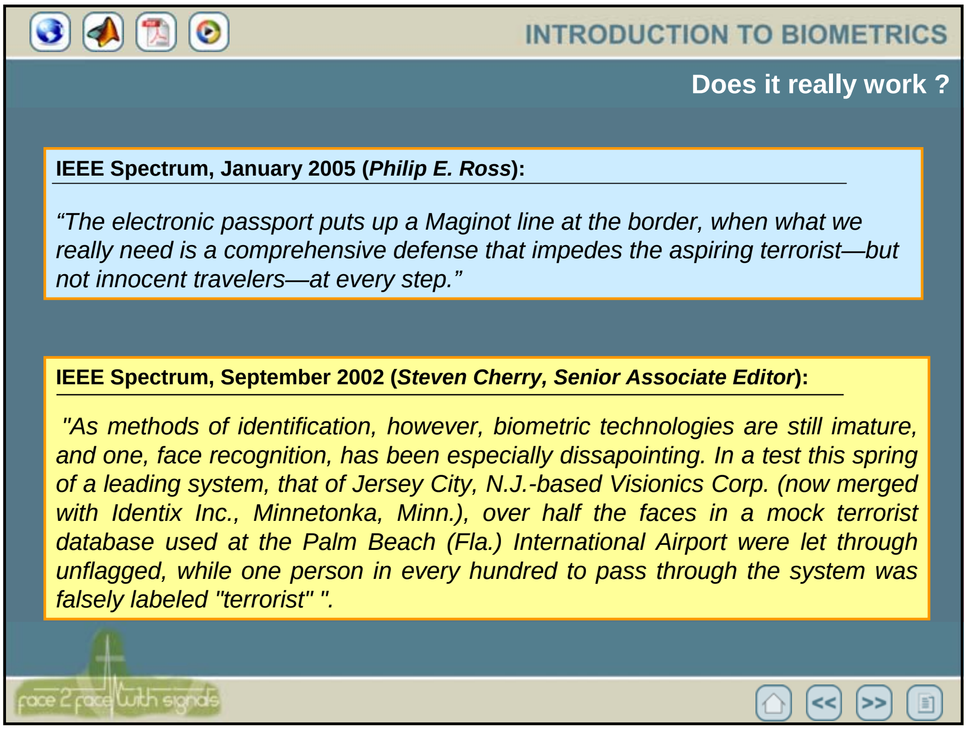


INTRODUCTION TO BIOMETRICS

Codes of ethics

The introduction of biometric technologies presents our society with important decisions. We must decide: (1) when or whether a sophisticated high-tech application works well enough to be worth deploying, (2) which elements of privacy are essential and which are inessential, and (3) what level of increased safety can come through the introduction of this technology.
It is important that we properly understand the potential of the technology both in terms of increased security and in terms of potential abuse.

The codes of ethics indicate that (1) the computing professional should have a concern for privacy, (2) the computing professional should give informed input to public debate, and (3) the decision should ultimately be that which is judged to best contribute to the well-being of society.
The codes provide a framework to guide decisionmaking, but do not directly suggest whether or not the proposed application is ethical.



INTRODUCTION TO BIOMETRICS

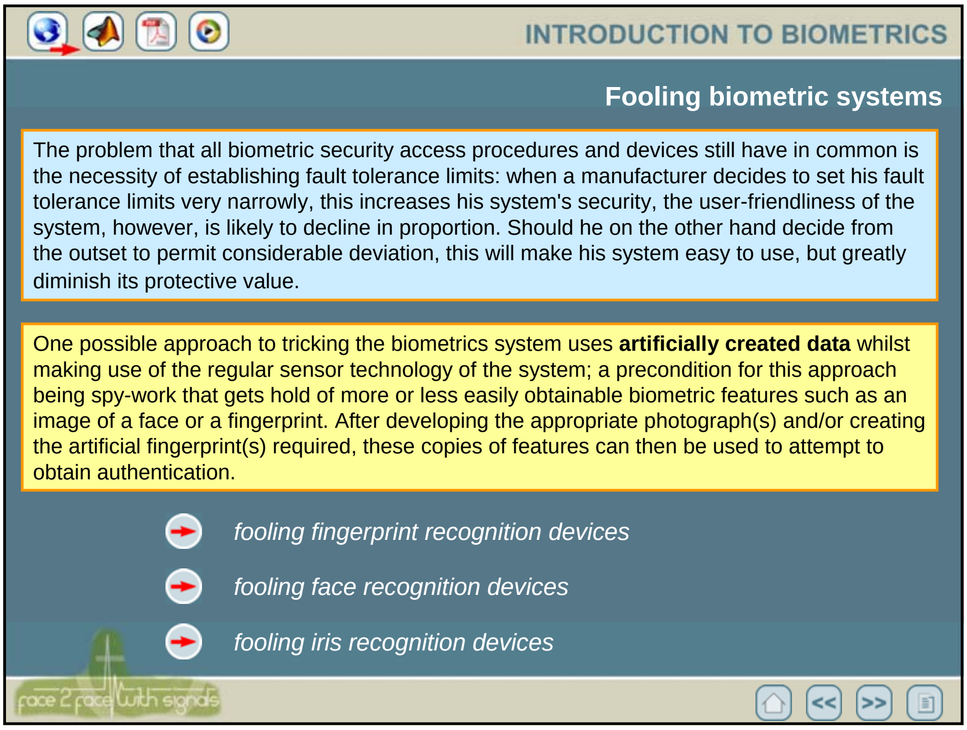
Does it really work ?

IEEE Spectrum, January 2005 (*Philip E. Ross*):

“The electronic passport puts up a Maginot line at the border, when what we really need is a comprehensive defense that impedes the aspiring terrorist—but not innocent travelers—at every step.”

IEEE Spectrum, September 2002 (*Steven Cherry, Senior Associate Editor*):

"As methods of identification, however, biometric technologies are still imature, and one, face recognition, has been especially dissapointing. In a test this spring of a leading system, that of Jersey City, N.J.-based Visionics Corp. (now merged with Identix Inc., Minnetonka, Minn.), over half the faces in a mock terrorist database used at the Palm Beach (Fla.) International Airport were let through unflagged, while one person in every hundred to pass through the system was falsely labeled "terrorist" ".



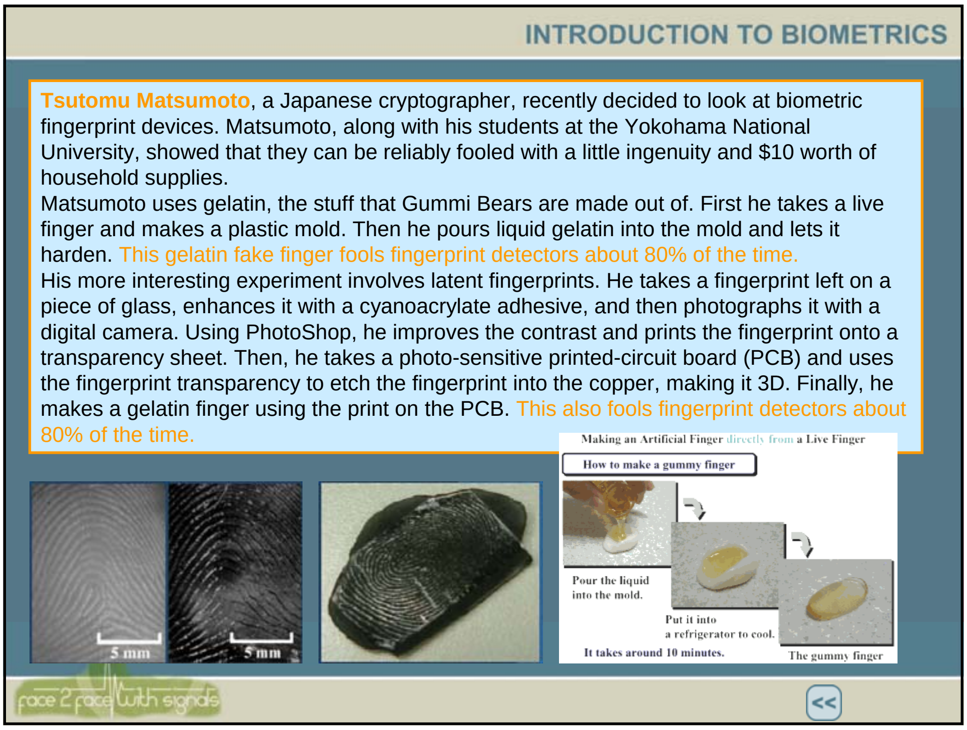
INTRODUCTION TO BIOMETRICS

Fooling biometric systems

The problem that all biometric security access procedures and devices still have in common is the necessity of establishing fault tolerance limits: when a manufacturer decides to set his fault tolerance limits very narrowly, this increases his system's security, the user-friendliness of the system, however, is likely to decline in proportion. Should he on the other hand decide from the outset to permit considerable deviation, this will make his system easy to use, but greatly diminish its protective value.

One possible approach to tricking the biometrics system uses **artificially created data** whilst making use of the regular sensor technology of the system; a precondition for this approach being spy-work that gets hold of more or less easily obtainable biometric features such as an image of a face or a fingerprint. After developing the appropriate photograph(s) and/or creating the artificial fingerprint(s) required, these copies of features can then be used to attempt to obtain authentication.

- *fooling fingerprint recognition devices*
- *fooling face recognition devices*
- *fooling iris recognition devices*



INTRODUCTION TO BIOMETRICS

Tsutomu Matsumoto, a Japanese cryptographer, recently decided to look at biometric fingerprint devices. Matsumoto, along with his students at the Yokohama National University, showed that they can be reliably fooled with a little ingenuity and $10 worth of household supplies.

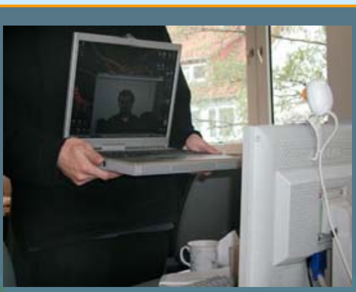
Matsumoto uses gelatin, the stuff that Gummi Bears are made out of. First he takes a live finger and makes a plastic mold. Then he pours liquid gelatin into the mold and lets it harden. This gelatin fake finger fools fingerprint detectors about 80% of the time.

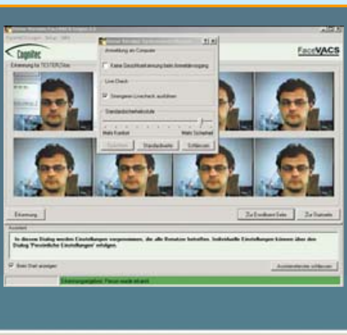
His more interesting experiment involves latent fingerprints. He takes a fingerprint left on a piece of glass, enhances it with a cyanoacrylate adhesive, and then photographs it with a digital camera. Using PhotoShop, he improves the contrast and prints the fingerprint onto a transparency sheet. Then, he takes a photo-sensitive printed-circuit board (PCB) and uses the fingerprint transparency to etch the fingerprint into the copper, making it 3D. Finally, he makes a gelatin finger using the print on the PCB. This also fools fingerprint detectors about 80% of the time.

5 mm
5 mm
Making an Artificial Finger directly from a Live Finger
How to make a gummy finger
Pour the liquid into the mold.
Put it into a refrigerator to cool.
It takes around 10 minutes.
The gummy finger

INTRODUCTION TO BIOMETRICS

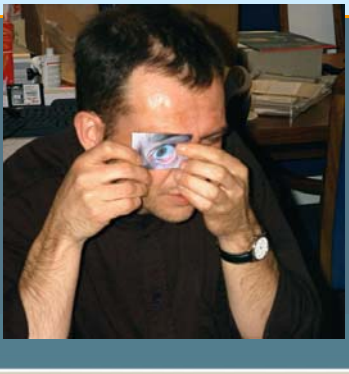
c’t found that Cognitec's FaceVACS-Logon, which commercially available Web cams as its sensor, could be outfoxed with a short video clip of a registered person, running on a notebook placed in front of the sensor. Still images taken on a digital camera proved almost as effective in gaining back door access.
To prevent this kind of deception, Cognitec has integrated a higher level of security known as Live-Check, but this made it harder for legitimate users to log on straight away, according to the tests. Worse, by shooting a film where a registered user moved his head from side to side it was again possible to fool the device.

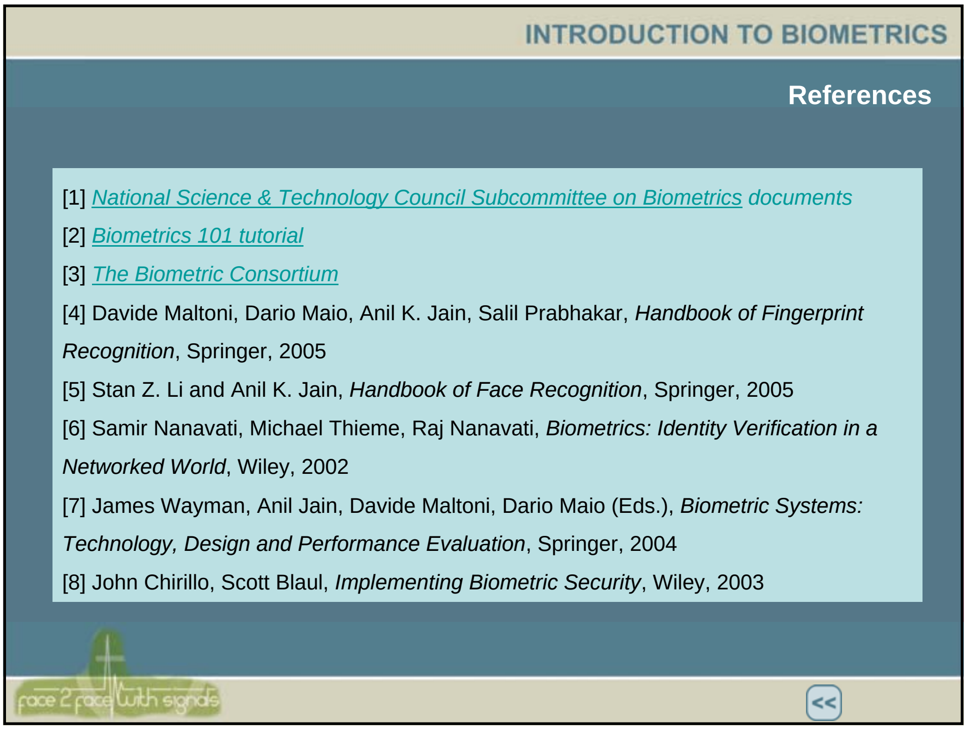




INTRODUCTION TO BIOMETRICS

If you think iris scanners might have faired better in the tests, think again.
c't looked at Panasonic's Authenticam BM-ET100, which is designed for the home market, and works with a Web cam.
This presented something of a challenge to break, but c't was eventually able to foil the device by using a high-quality printed image (with a hole cut in the middle) of a recognised user's iris, behind which the hidden eyes of a real human being peered. Anyway, presenting digital iris images to the system via a notebook display failed to yield access.





References

[1] National Science & Technology Council Subcommittee on Biometrics documents

[2] Biometrics 101 tutorial

[3] The Biometric Consortium

[4] Davide Maltoni, Dario Maio, Anil K. Jain, Salil Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2005

[5] Stan Z. Li and Anil K. Jain, *Handbook of Face Recognition*, Springer, 2005

[6] Samir Nanavati, Michael Thieme, Raj Nanavati, *Biometrics: Identity Verification in a Networked World*, Wiley, 2002

[7] James Wayman, Anil Jain, Davide Maltoni, Dario Maio (Eds.), *Biometric Systems: Technology, Design and Performance Evaluation*, Springer, 2004

[8] John Chirillo, Scott Blaul, *Implementing Biometric Security*, Wiley, 2003

<<