



Developed and Presented By Dr. Mehrdad Sepehri Sharbaf  
CSUDH  
Computer Science Department

<http://csc.csudh.edu/>

The some of the materials are excerpted from Paul Reid 's Book, John Chirillo and Scott Blaul 's Book, and Ross Anderson's Book

# BIOMETRICS

---

**WHO ARE YOU?**

# HOW ARE PEOPLE IDENTIFIED?

- ▮ People's identity are verified and identified by three basic means:
  - ▮ Something they **have** (identity document or token)
  - ▮ Something they **know** (password, PIN)
  - ▮ Something they **are** (human body such as fingerprint or iris).
- ▮ The strongest authentication involves a combination of all three.



# PERSON IDENTIFICATION

---

- ▮ Identifying fellow human beings has been crucial to the fabric of human society
- ▮ In the early days of civilization, people lived in small communities and everyone knew each other
- ▮ With the population growth and increase in mobility, we started **relying on documents and secrets to establish identity**
- ▮ Person identification is now an integral part of the infrastructure **needed for diverse business sectors** such as banking, border control, law enforcement.

# AUTOMATIC IDENTIFICATION

---

Different means of automatic identification:

- ▮ **Possession-based** (credit card, smart card)
  - ▮ *“something that you have”*
- ▮ **Knowledge-based** (password, PIN)
  - ▮ *“something that you know”*
- ▮ **Biometrics-based** (biometric identifier)
  - ▮ *“something about or produced by your physical make-up”*

# 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



# IDENTIFICATION PROBLEMS



- ▮ **Identity Theft:** Identity thieves steal PIN (e.g., date of birth) to open credit card accounts, withdraw money from accounts and take out loans

3.3 million identity thefts in U.S. in 2010; 6.7 million victims of credit card fraud

**Surrogate representations** of identity such as passwords and ID cards no longer suffice

# WHAT ARE BIOMETRICS?

---

- ▮ **Biometrics** – science, which deals with the automated recognition of individuals (or plants/animals) based on biological and behavioral characteristics
- ▮ **Biometry** – mathematical and statistical analysis of biological data
- ▮ **Biometric system** – a pattern recognition system that recognizes a person by determining the authenticity of a specific biological and/or behavioral characteristic (biometric)
- ▮ **Anthropometry**–measurement techniques of human body and its specific parts
- ▮ **Forensic (judicial) anthropometry**–identification of criminals by these measurement techniques



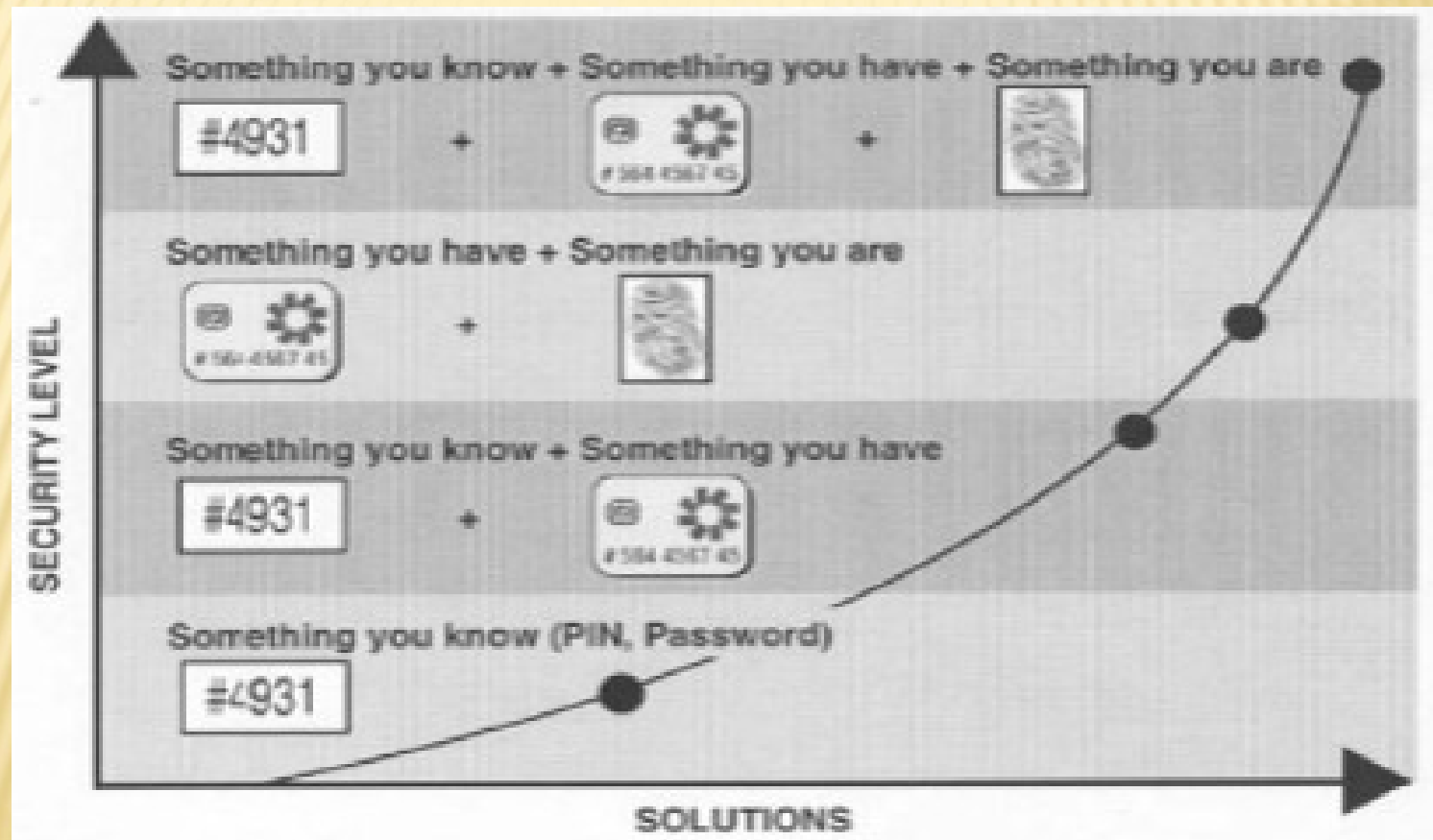
---

# WHY BIOMETRICS?

# WHY BIOMETRICS?



# MENTIONING THE OBVIOUS





# 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. Performance

- ▢ 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

# IDENTIFIABLE BIOMETRIC CHARACTERISTICS

---

- ▮ **Biological traces**

- ▮ DNA (DeoxyriboNucleic Acid), blood, saliva, etc.

- ▮ **Biological (physiological) characteristics**

- ▮ fingerprints, eye irises and retinas, hand palms and geometry, and facial geometry

- ▮ **Behavioral characteristics**

- ▮ dynamic signature, gait, keystroke dynamics, lip motion

- ▮ **Combined**

- ▮ voice

# BIOMETRICS IS NOT NEW!!

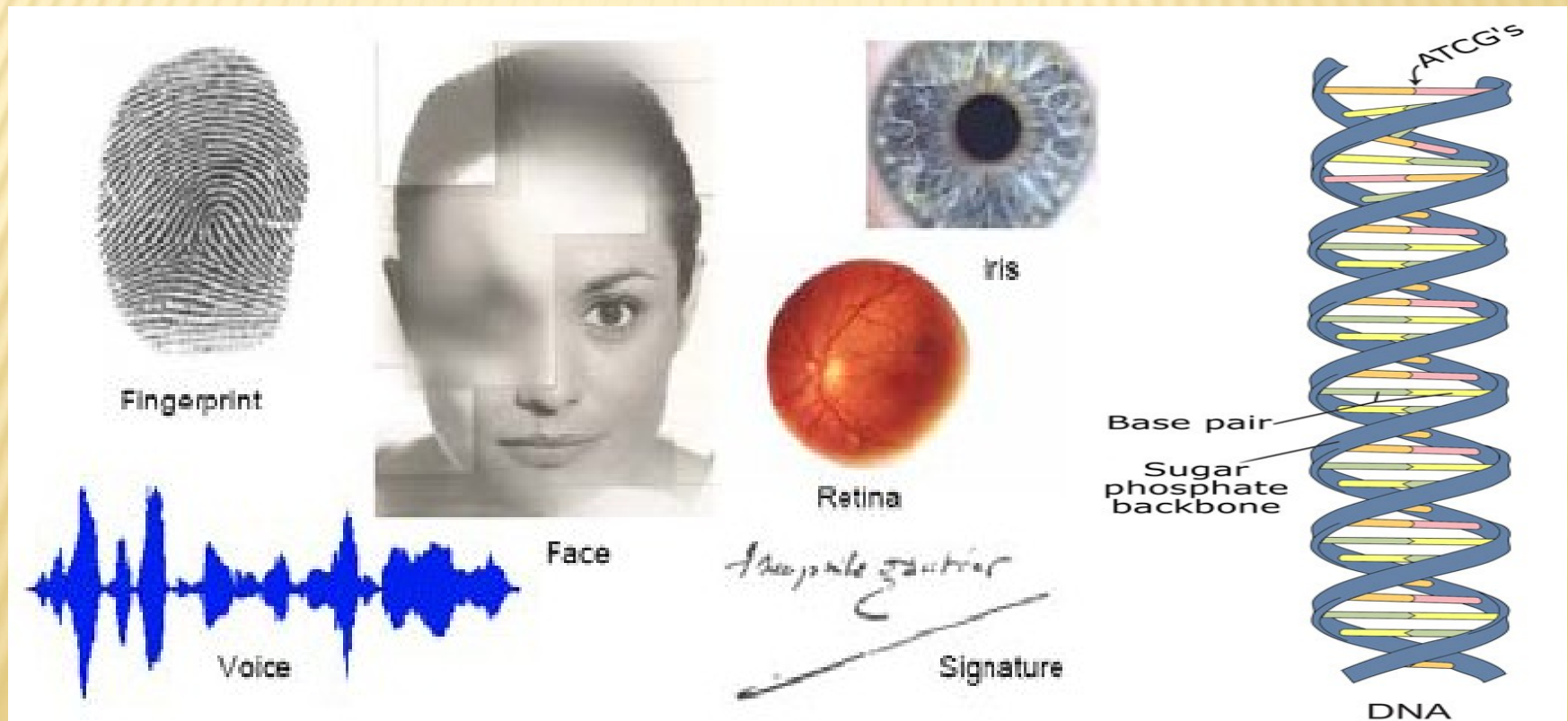
- ▯ Bertillon system (1882) took a subject's photograph, and recorded height, the length of one foot, an arm and index finger
- ▯ Galton/Henry system of fingerprint classification adopted by Scotland Yard in 1900
- ▯ FBI set up a fingerprint identification division in 1924
- ▯ AFIS installed in 1965 with a database of 810,000 fingerprints
- ▯ First face recognition paper published in 1971 (Goldstein et al.)
- ▯ FBI installed IAFIS in ~2000 with a database of **47 million 10 prints**; average of 50,000 searches per day; ~15% of searches are in **lights out** mode; 2 hour response time for criminal search

Emphasis now is to **automatically** perform **reliable** person identification in **unattended** mode, often **remotely** (or at a distance)

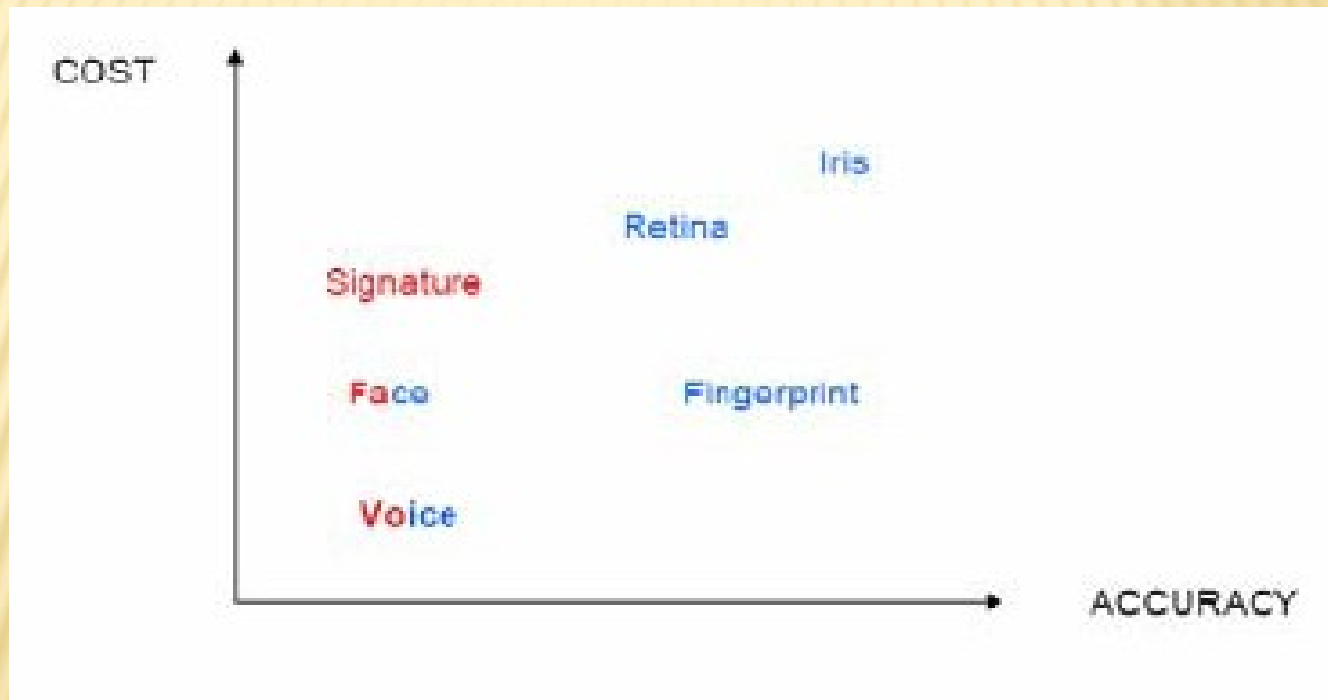


# Biometrics

- A biometric authentication system uses the physiological (fingerprints, face, hand geometry, iris) and/or behavioral traits (voice, signature, keystroke dynamics) of an individual to identify a person or to verify a claimed identity.



# COMPARISON OF BIOMETRIC TECHNIQUES



---

# KEY BIOMETRIC TERMS AND PROCESS



# WHAT IS BIOMETRIC?

---

- Biometrics is the automated use of physiological or behavioral characteristics to determine or verify identity.
- Automated use means using computers or machines, rather than human beings, to verify or determine physiological or behavioral characteristics.

# BIOMETRICS

---

- ▮ 2 Categories of Biometrics
  - ▮ Physiological – also known as static biometrics: Biometrics based on data derived from **the measurement of a part of a person's anatomy**. For example, fingerprints and iris patterns, as well as facial features, hand geometry and retinal blood vessels
  - ▮ Behavioral – biometrics based on data derived from **measurement of an action performed by a person**, and distinctively incorporating time as a metric, that is, the measured action. For example, voice (speaker verification)

---

# **USING BIOMETRICS**

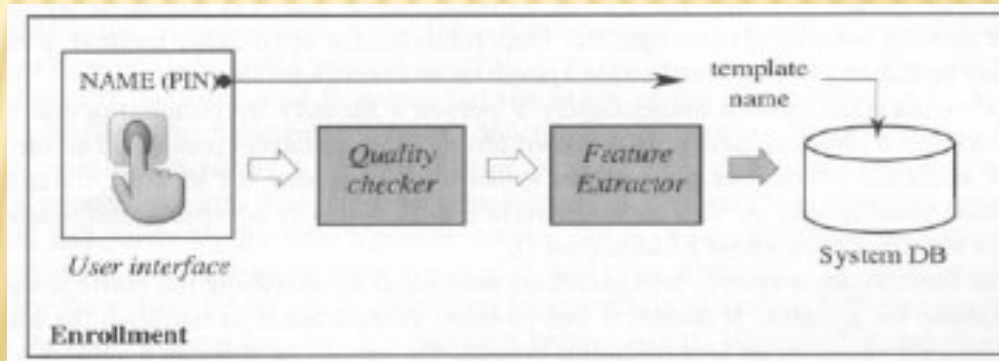
## **ENROLLMENT, VERIFICATION**

## **RECOGNITION**



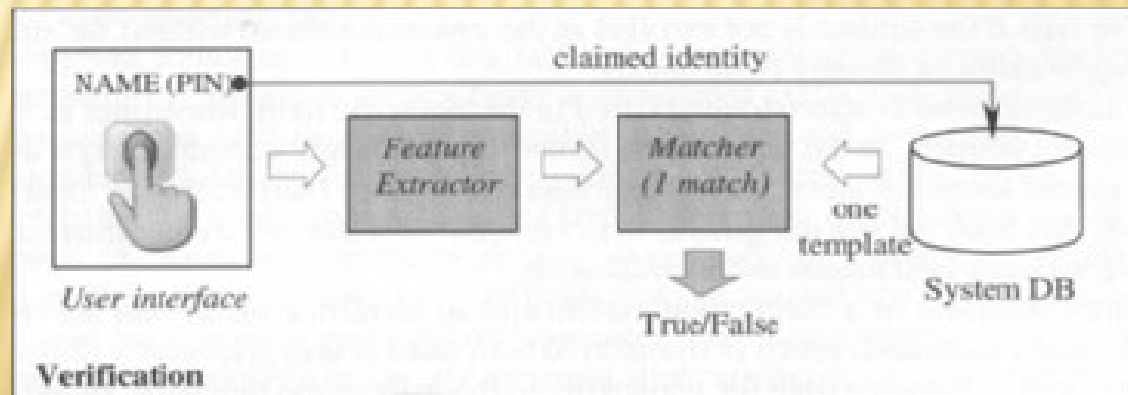
# USING BIOMETRICS

- Process flow includes **enrollment**, and **verification/identification**.
- Enrollment
  - Person entered into the database
  - Biometric data provided by a user is converted into a template.
  - Templates are stored in a biometric systems for the purpose of subsequent comparison.



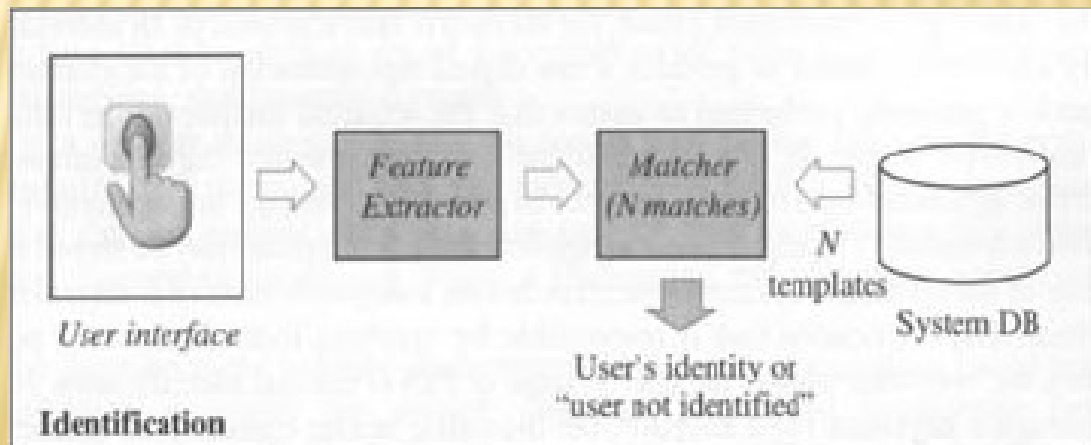
# VERIFICATION VERSUS IDENTIFICATION

- Verification: Am I who I claim to be?
  - One to one comparison
- Verification** can confirm or deny the specific identification claim of a person.



# IDENTIFICATION VERSUS VERIFICATION

- Identification: Who am I?
  - One to many comparison
  - can determine the identity of a person from a biometric database without that person first claiming an identity.

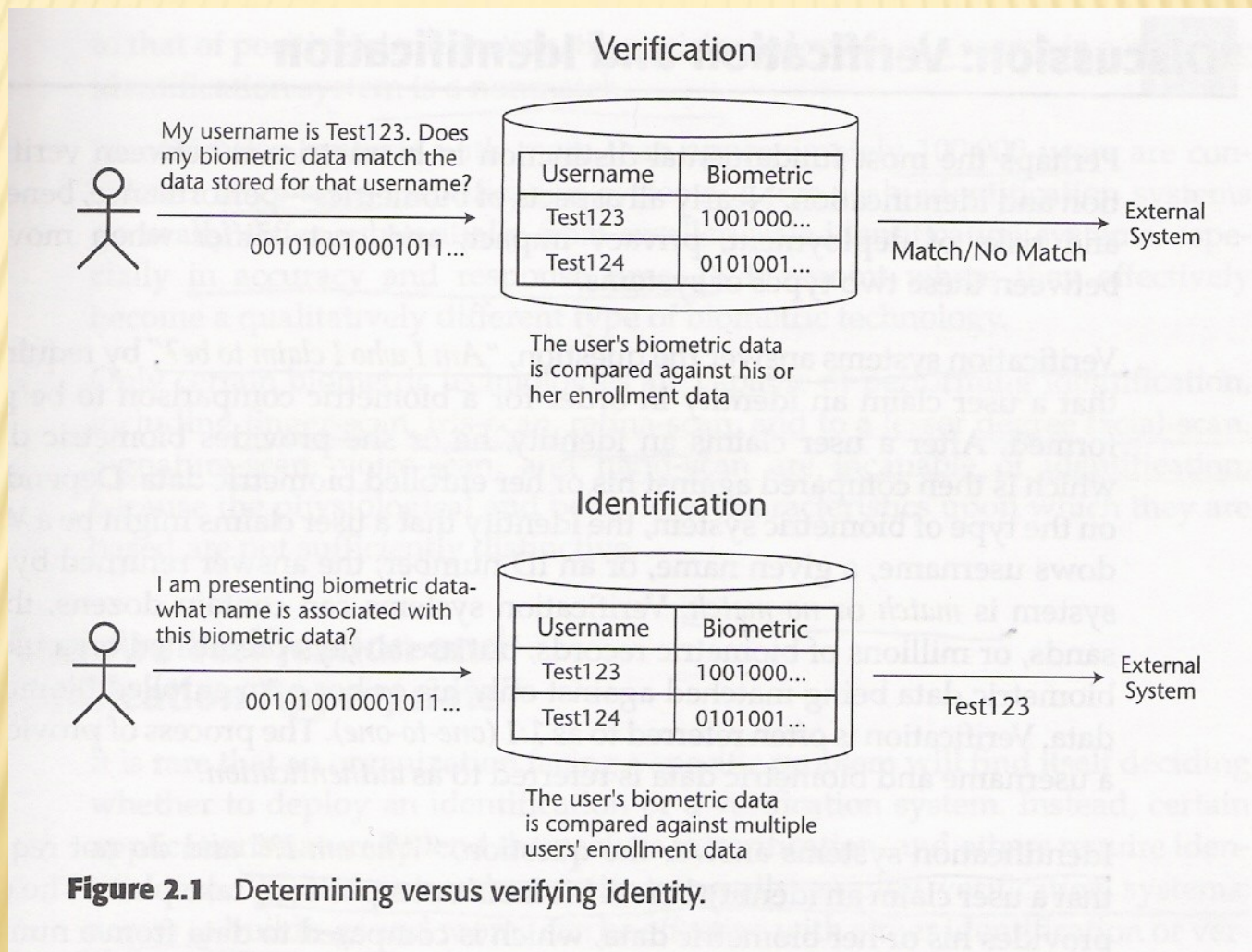




## DISCUSSION: VERIFICATION AND IDENTIFICATION

- Verification system answers the question:  
“Am I who I claim to be?”
- The answer returned by the system is match or no match.
- Identification systems answers the question:  
“Who am I”
- The answer returned by the system is an identity such as a name or ID number.

# DISCUSSION: VERIFICATION AND IDENTIFICATION



**Figure 2.1** Determining versus verifying identity.



# WHEN ARE VERIFICATION AND IDENTIFICATION APPROPRIATE?

---

- ▮ PC and Network Security -- verification
- ▮ Access to buildings and rooms – either verification (predominant) or identification
- ▮ Large-scale public benefit programs – identification
- ▮ Verification systems are generally faster and more accurate than identification systems.
- ▮ However, verification systems cannot determine whether a given person is present in a database more than once.

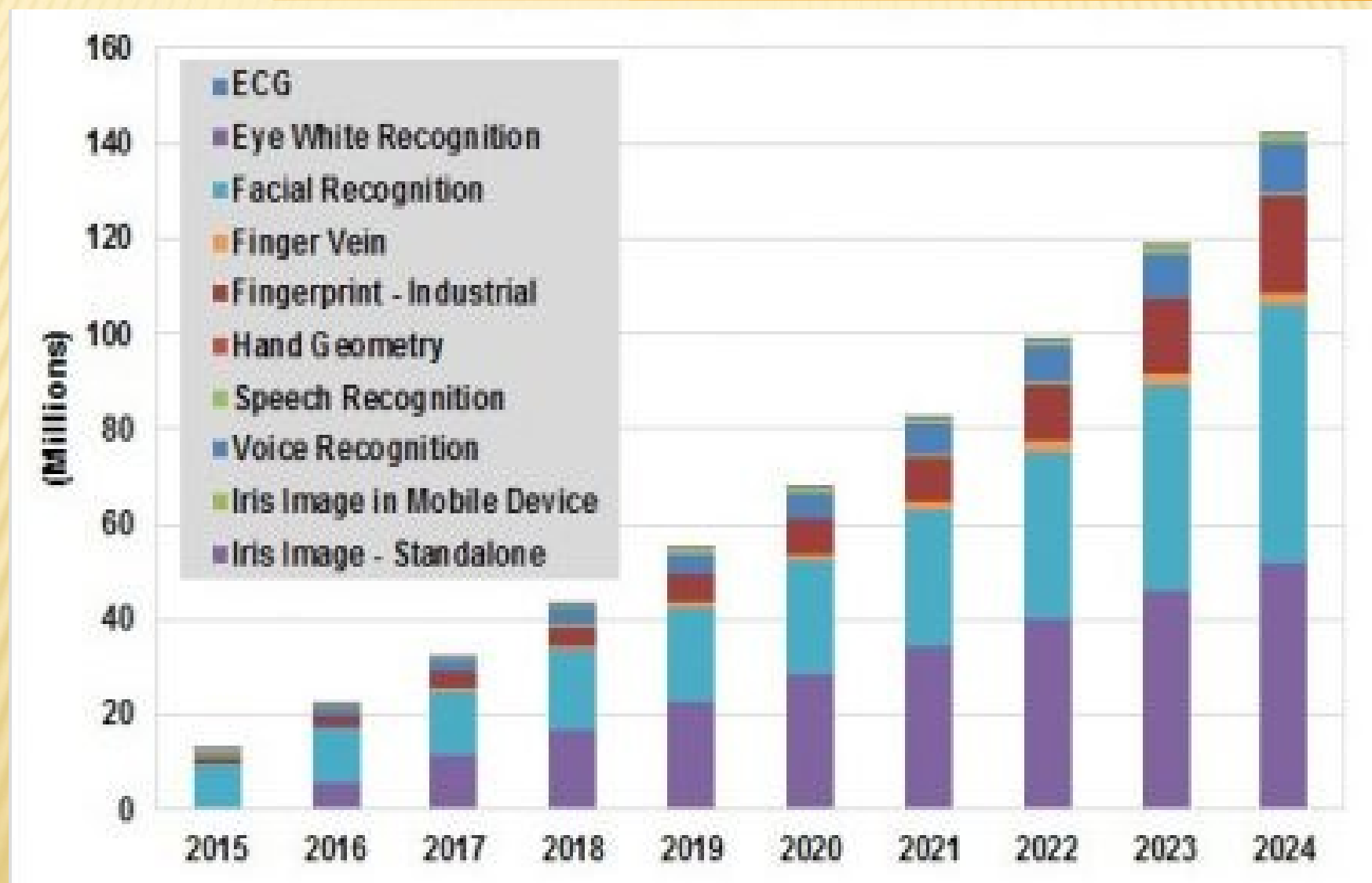


# WHEN ARE VERIFICATION AND IDENTIFICATION APPROPRIATE?

---

- ▮ Identification system requires more computational power than verification systems, and there are more opportunities for an identification system to err.
- ▮ As a rule, verification systems are deployed when identification simply does not make sense (to eliminate duplicate enrollment, for instance. )

# TOTAL BIOMETRICS MARKET



---

# DIFFERENT BIOMETRICS



# PHYSIOLOGICAL AND BEHAVIORAL CHARACTERISTICS

---

- ▮ Physiological or behavioral characteristics are **distinctive**, which provide basic measurement of biometrics.
- ▮ Physiological biometrics are based on **direct measurements of a part of the human body**, such as finger-scan, facial-scan, iris-scan, hand-scan, and retina-scan.
- ▮ Behavioral biometrics are based on **measurements and data derived from an action** and therefore **indirectly** measure characteristics of the human body, such as voice-scan and signature-scan.
- ▮ The element of **time** is essential to behavioral biometrics.

# DNA (DEOXYRIBO NUCLEIC ACID)

## THE ULTIMATE BIOMETRIC

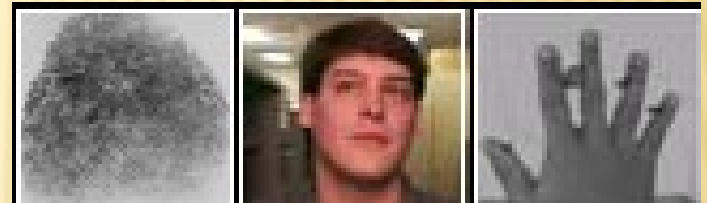
---

- ▮ One-dimensional unique code for one's individuality, but identical twins have identical DNA patterns
- ▮ Issues limiting the utility of DNA
  - ▮ Contamination
  - ▮ Access
  - ▮ Automatic real-time recognition issues
  - ▮ Privacy issues: information about susceptibilities of a person to certain diseases could be gained from the DNA pattern

# BEHAVIORAL VS PHYSICAL TRAITS

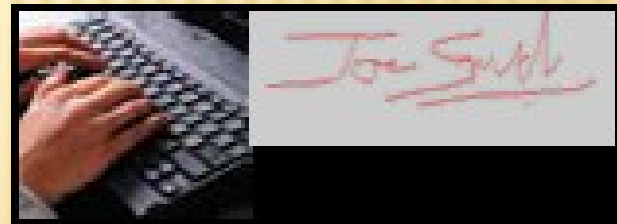
## Physical Characteristics

- ▮ Iris
- ▮ Retina
- ▮ Vein Pattern
- ▮ Hand Geometry
- ▮ Face
- ▮ Fingerprint
- ▮ Ear shape



## Behavioral Characteristics

- ▮ Keystroke dynamics
- ▮ Signature dynamics
- ▮ Walking Gait
- ▮ Voice

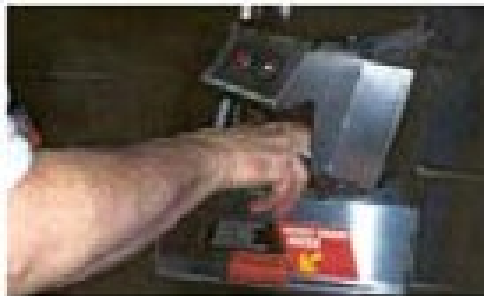




# FINGERPRINTS



Fingerprint at check-out counter



Disney World



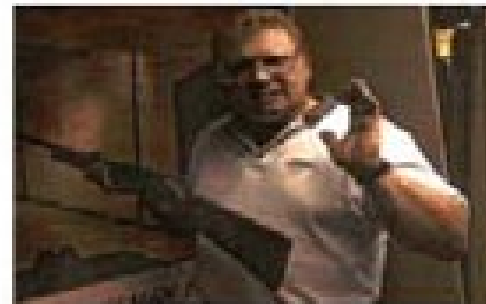
Smart card



Smart PDA

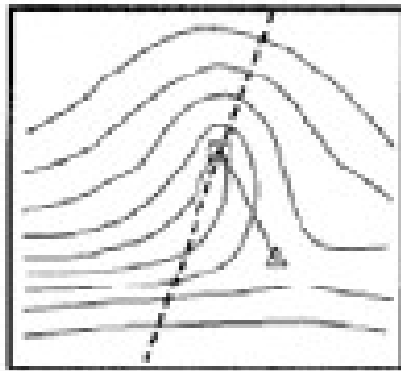


Cell phone with  
Fingerprint sensor

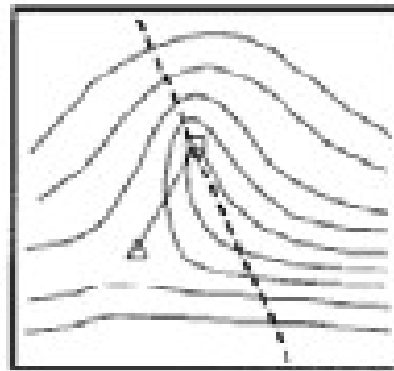


Smart gun

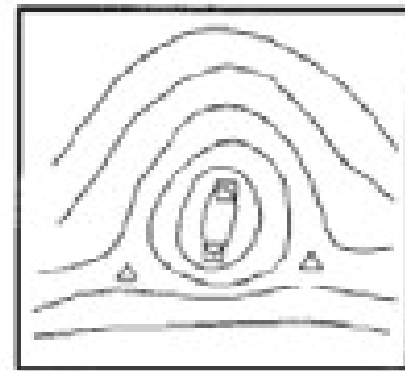
# FINGERPRINT FEATURES



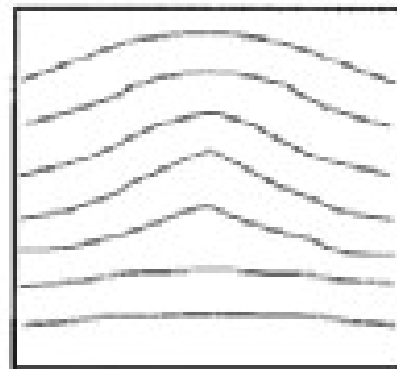
Left loop



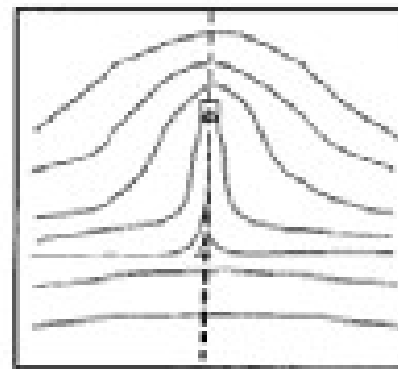
Right loop



Whorl



Arch



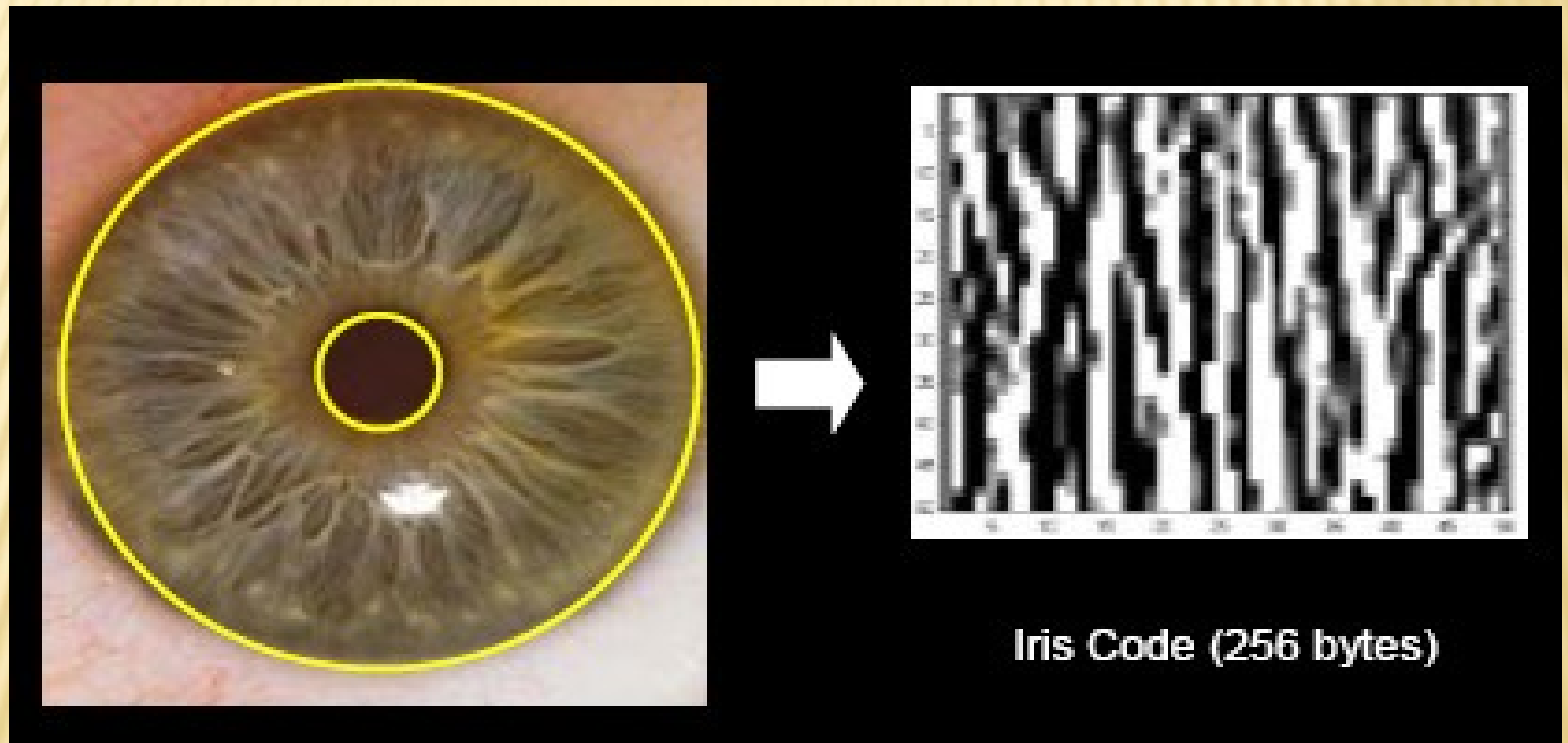
Tented arch

# IRIS RECOGNITION: EYE





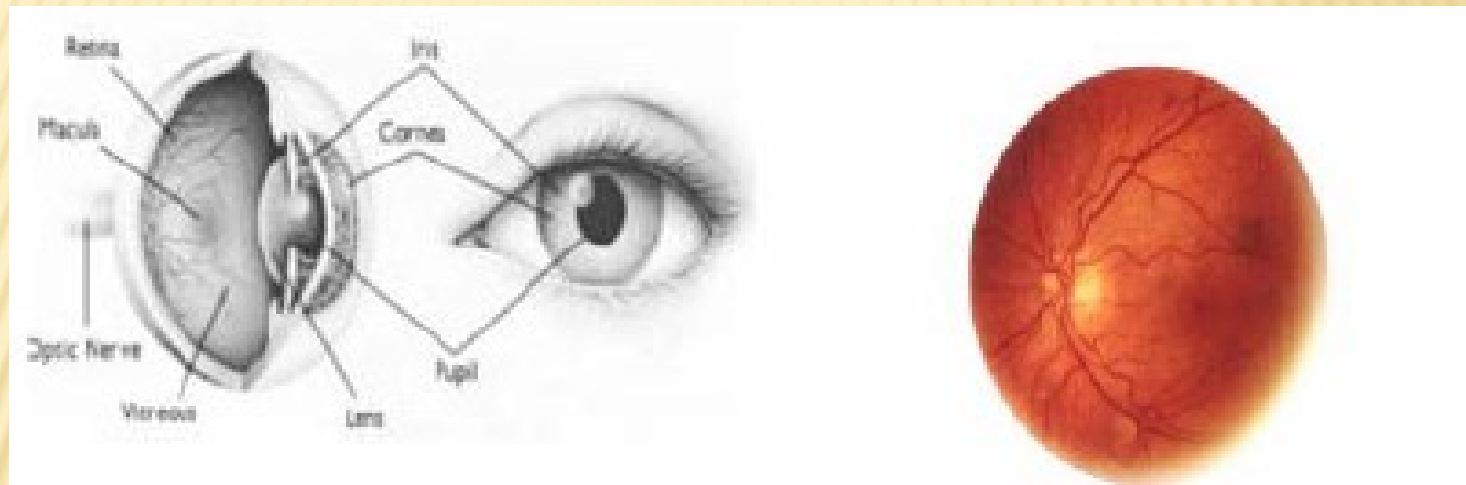
# IRIS CODE



# NATIONAL GEOGRAPHIC 1984 AND 2002



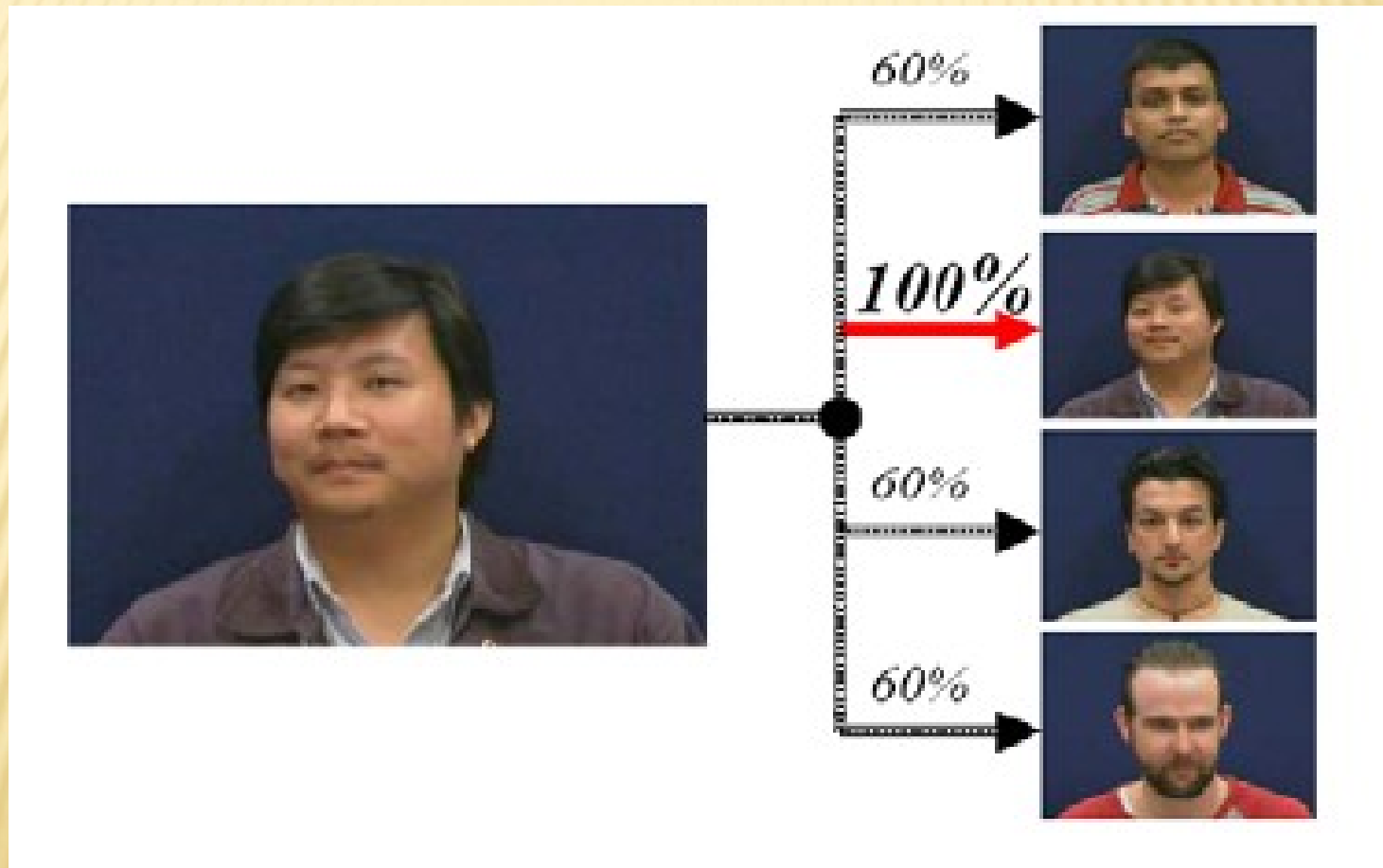
# RETINA



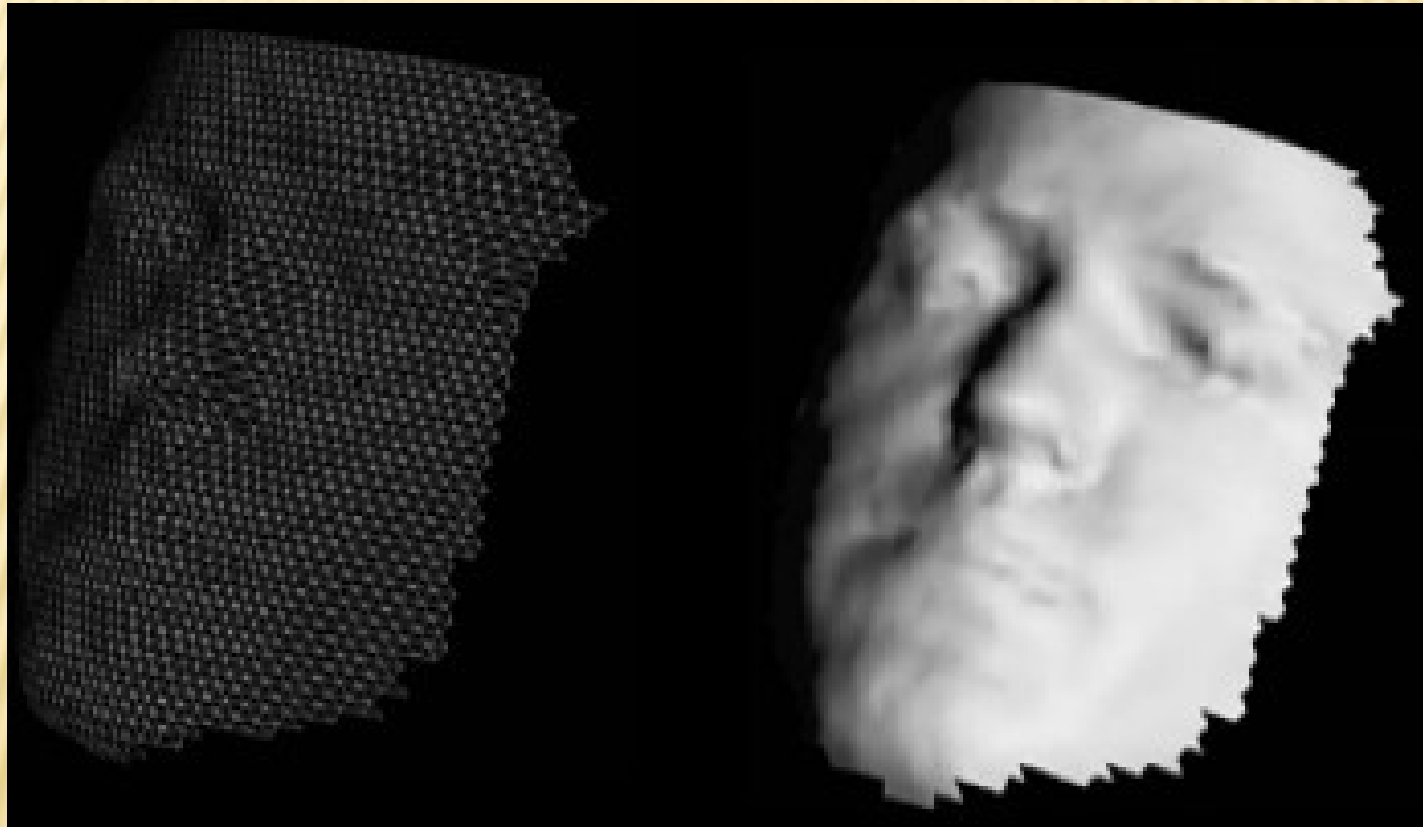
Every eye has its own totally unique pattern of blood vessels.



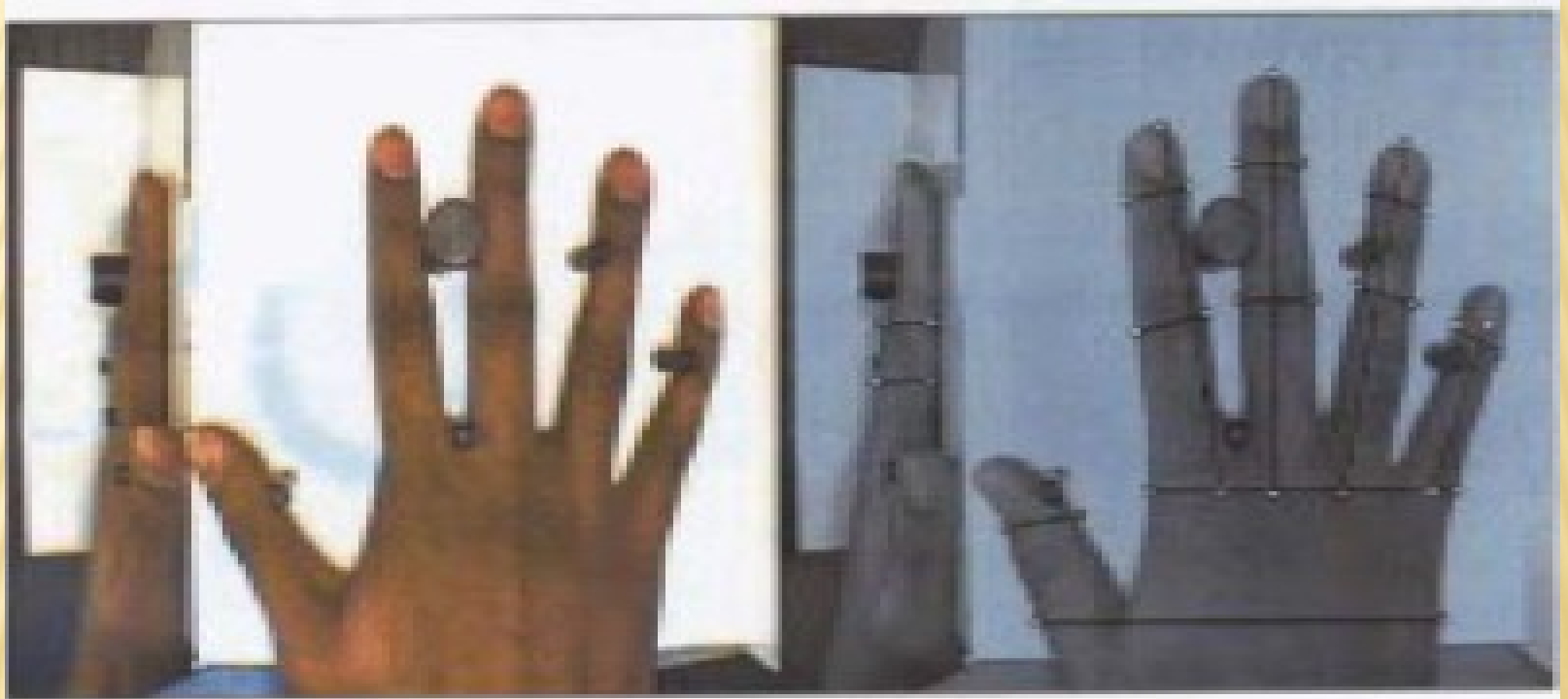
# FACE RECOGNITION: CORRELATION



# FACE RECOGNITION: 3D



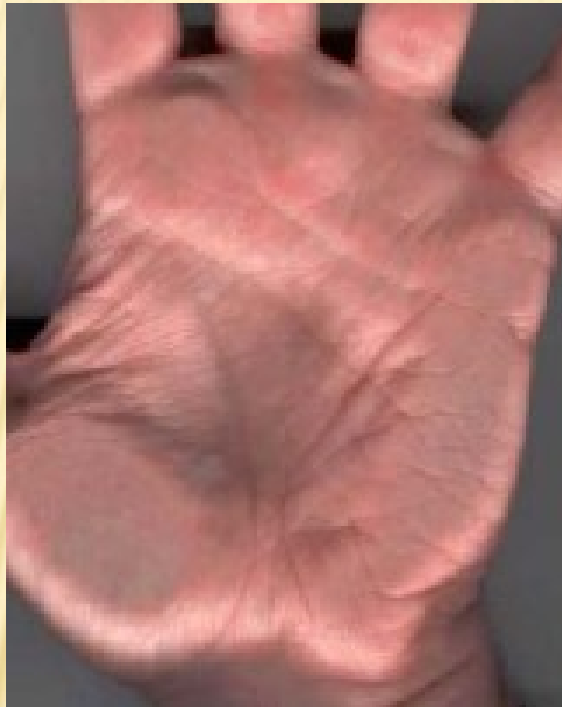
# HAND





# PALM

---



# VEIN

---



# EAR





# MARKET SHARE

## Biometrics Market Share

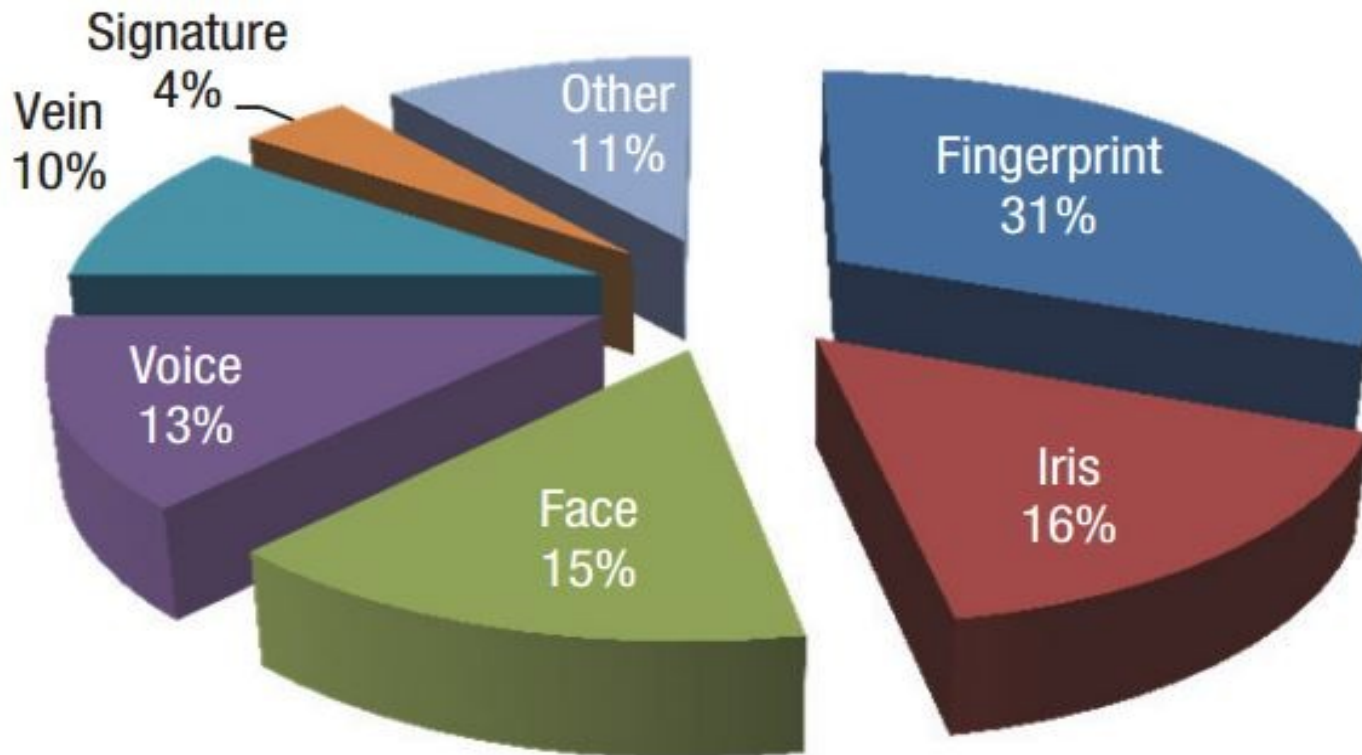


Figure 1: Biometrics market share by system type

---

# BIOMETRIC APPLICATIONS

# BIOMETRIC APPLICATION

- ▮ Biometric technology is used for many applications
  - ▮ Providing time and attendance functionality for a small company
  - ▮ Ensuring the integrity of a 10 million-person voter registration database
- ▮ The benefit of using biometrics include increased security, increased convenience, reduced fraud or delivery of enhanced services.



# UCSD BIOMETRIC SODA MACHINE



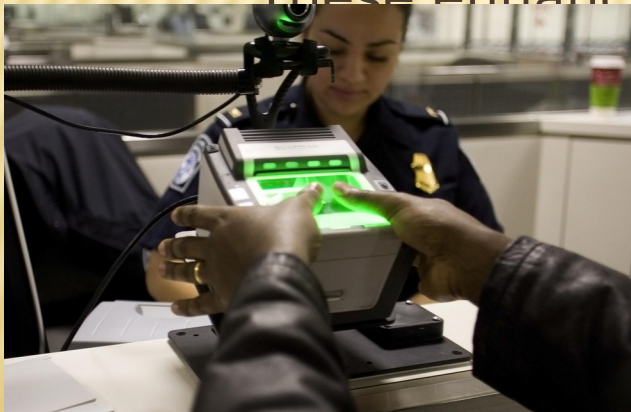
# US-VISIT

[www.dhs.gov/us-visit](http://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



# NATIONAL BIOMETRIC ID CARDS

## **U.K. to consider national biometric ID cards, database**

By Laura Rohde, COMPUTERWORLD (Nov 29, 2003)-

The U.K. government is set to consider legislation next year for the **establishment of compulsory biometric identity cards and a central database of all U.K. subjects**, it was announced by the government this week.

The information that the government is considering for inclusion on the card includes personal details such as a person's home address and telephone number, his National Insurance number (the equivalent of the U.S. Social Security number), medical information and criminal convictions, **as well as the biometric information, most likely in the form of an iris, fingerprint or palm print scan.**



# ACCESS CONTROL



<http://www.livetrp.com>

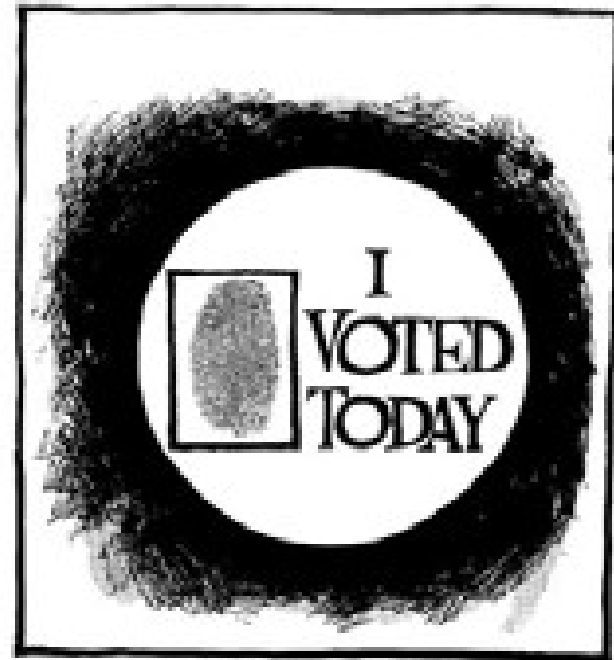


# DID YOU VOTE?



PAPER-BALLOT ERA

JIMMY KIMBLE



TOUCH-SCREEN ERA


# APPLICATIONS

## Video Surveillance (On-line or off-line)

### Face Scan at Airports



The 30, Peterburg-Cheremetov Airport installed facial-recognition systems at two security checkpoints in January. The first full-length scanner (shown above) examines that snap pictures of passengers as they pass through passport-meters. The passengers' faces instantly are compared to a database of images of wanted criminals. Sheriff Forrest Rice (shown left) was one of the first people to pass through the new security system.



[www.facesnap.de](http://www.facesnap.de)

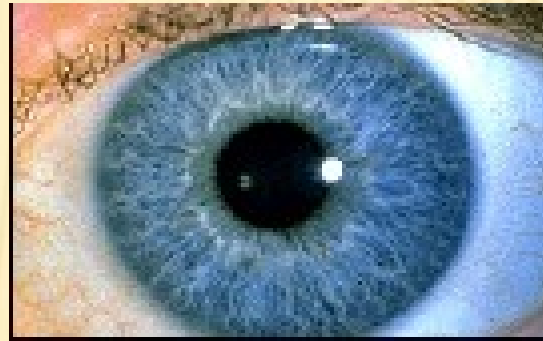
# FINGERPRINT SYSTEM AT GAS STATIONS

“Galp Energia SGPS SA of Lisbon won the technology innovation award for developing a payment system in which gasoline-station customers can **settle their bills simply by pressing a thumb against a glass pad**. Scanning technology identifies the thumbprint and sends the customer's identification information into Galp's back-office system for payment authorization.”  
THE WALL STREET JOURNAL,  
November 15, 2004





# 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.

# FINGERPRINT SYSTEM AT BORDER CROSSINGS

“Foreigners entering the United State in three cities, including Port Huron, were fingerprinted, photographed and subjected to background checks on Monday in a test of a program that will eventually be extended to every land border crossing nationwide.”

**Lansing State Journal, Nov.  
16, 2004**



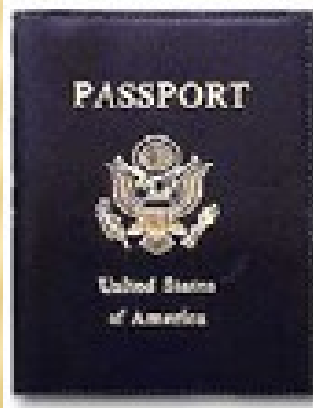
# NEW PASSPORTS

**"ICAO TAG-MRTD/NTWG RESOLUTION N001 - Berlin, 28 June 2002**

**ICAO TAG-MRTD/NTWG** endorses the use of **face recognition** as the globally interoperable biometric for machine assisted identity confirmation with machine readable travel documents.

**ICAO TAG-MRTD/NTWG** further recognizes that Member States may elect to use fingerprint and/or iris recognition as additional biometric technologies in support of machine assisted identity confirmation.

***Endorsement: Unanimous"***



The new passports have an embedded contactless (ISO 14443) “**smart-card**” **chip** that stores personal information and a biometric template. Two problems: **reliability and privacy**



# WANT TO CHARGE IT? YOU'LL HAVE TO TALK TO YOUR CREDIT CARD



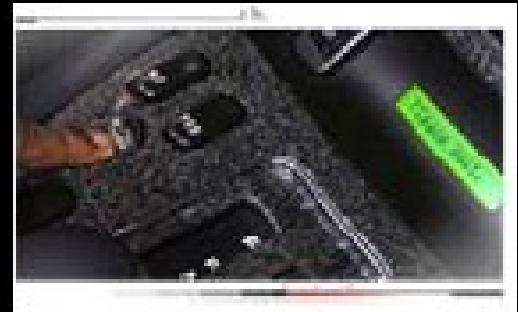
Beepcard, a company in California, has designed a credit card that **works only when it recognizes the voice** of its rightful owner. Enclosed in the card is a tiny microphone, a loudspeaker and a speech recognition chip that compares the spoken password with a recorded sample. If the voices match, the card emits a set of beeps that authorize a transaction over the telephone or the Internet. If the voices do not match, the card will not beep.

The system **tolerates some variations in voice** to accommodate cold or background noise. But it might not work if there is a blaring music in the background.



# BIOMETRICS FOR PERSONALIZATION

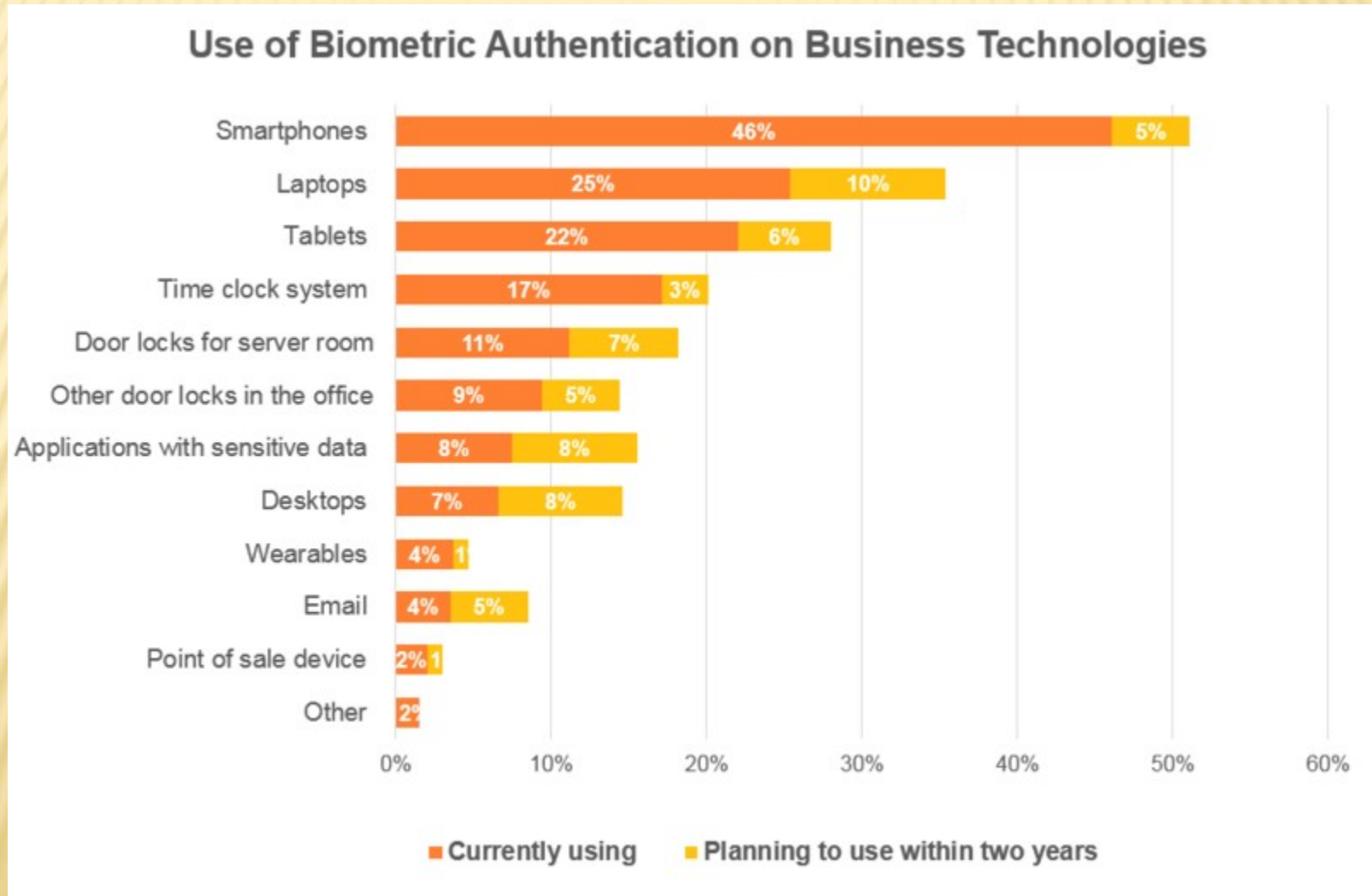
- Automatic personalization of vehicle settings:
  - Seat position
  - Steering wheel position
  - Mirror positions
  - Lighting
  - Radio station preferences
  - Climate control settings
- URLs at your fingertips



<http://www.virtex.com>



# DOMAINS OF APPLICATION



---

# KEY TERMS



# TEMPLATE (1)

---

- A template is a small file derived from the distinctive features of a user's biometric data, used to perform biometric matches.
- Templates, is calculated during enrollment or verification phase. The template be understood as a compact representation of the collected feature data, where useless or redundant information is discarded.
- Biometric systems store and compare biometric templates, **NOT** biometric data.

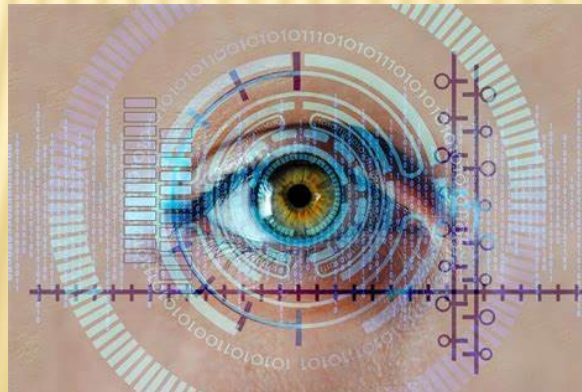
## TEMPLATE (2)

---

- ▮ Most templates occupy less than 1 kilobyte, and some of them are as small as 9 bytes; size of template differs from vendor to vendor.
- ▮ Templates are proprietary to each vendor and each technology, and there is no common biometric template format.
- ▮ This is beneficial from a privacy perspective, but the lack of interoperability deterred some would-be users.

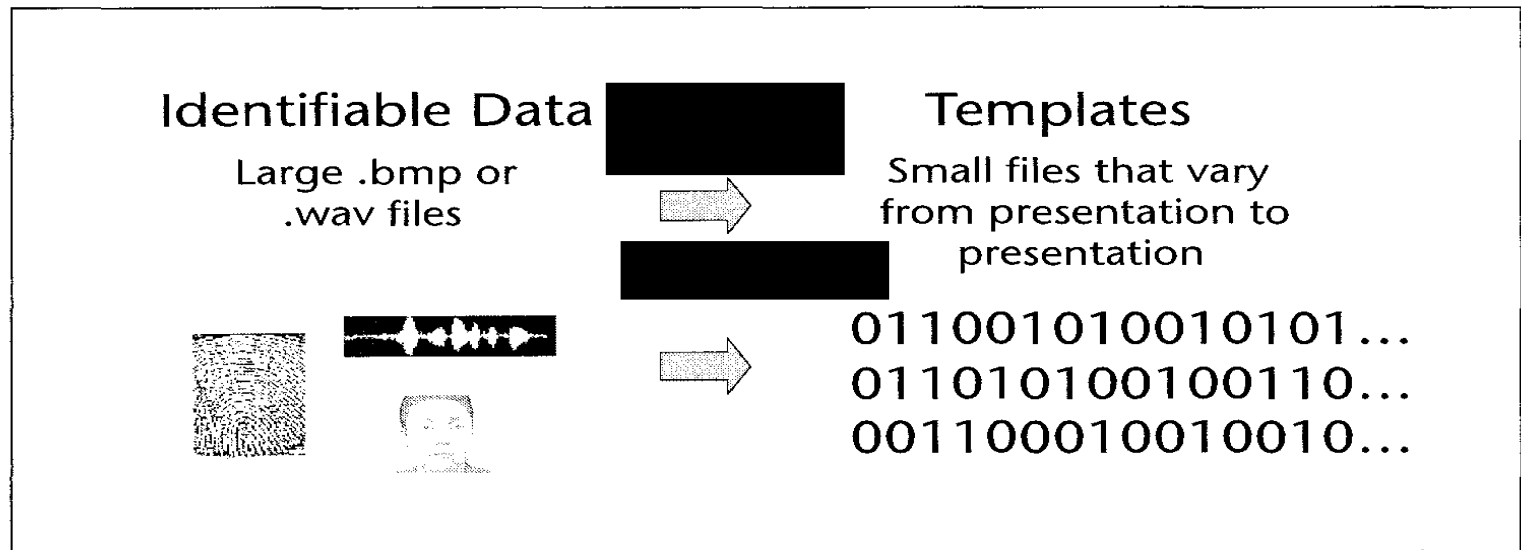
# TEMPLATES

- Biometric data **CAN NOT** be reconstructed from biometric templates.
- Templates are extractions of distinctive features and not adequate to reconstruct the full biometric image or data.
- Unique templates** are generated **every time** a user presents biometric data. For example, two immediate successive placement of a finger on a biometric device generate entirely different templates which are processed by vendor's algorithm and recognizable as being from the same person, but are not identical.





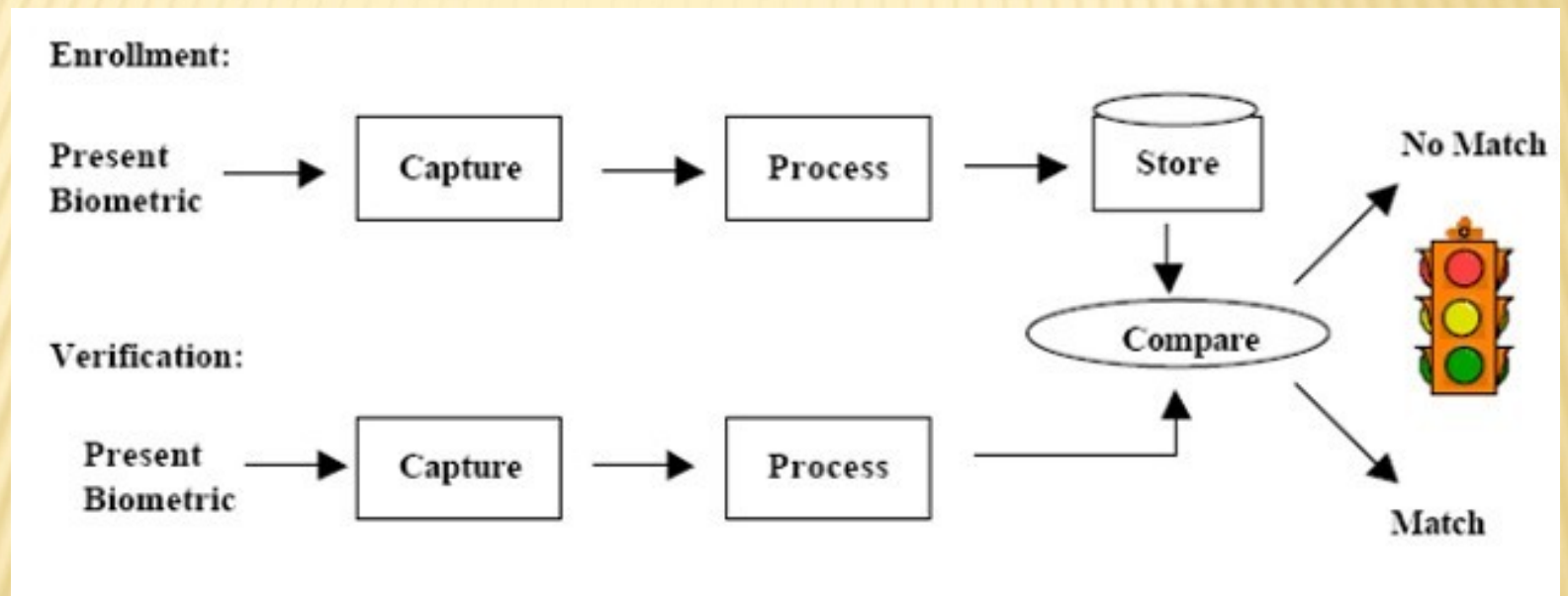
# BIOMETRIC TEMPLATES VERSUS IDENTIFIABLE BIOMETRIC DATA



**Figure 2.3** Biometric templates versus identifiable biometric data.

Depending on when they are generated, templates can be referred to as enrollment templates or match templates.

# THE TWO STAGES OF A BIOMETRIC SYSTEM



# ENROLLMENT AND TEMPLATE CREATION (1)

---

- ▮ **Enrollment** is a process to acquire, assess, process, and store user's biometric data in the form of a template.
- ▮ **Stored templates** are used for subsequent verification and identification.
- ▮ **Quality enrollment** is a critical factor in the long-term accuracy of biometric system.



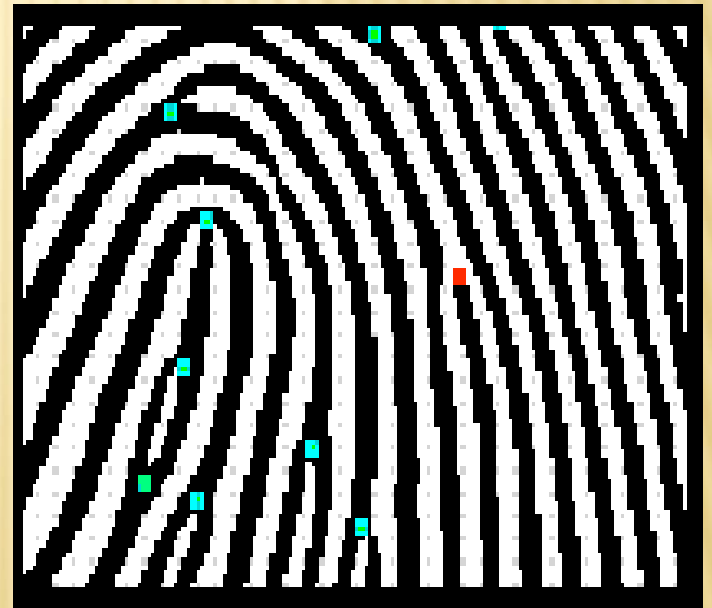
# ENROLLMENT AND TEMPLATE CREATION (2)

---

- ▮ **Presentation** is the process by which a user provides biometric data to an acquisition device – the hardware used to collect biometric data.
- ▮ For example, looking in the direction of a camera, placing a finger on a platen, or reciting a passphrase.

# ENROLLMENT AND TEMPLATE CREATION (3)

- ▮ **Biometric data** are converted to templates through feature extraction.
- ▮ **Feature extraction** is the automated process of locating and encoding distinctive characteristics from biometric data in order to generate a template.
- ▮ Feature extraction removes noises and unwanted data, and digitize biometric traits.



# ENROLLMENT AND TEMPLATE CREATION (4)

- ▮ A user may need to present biometric data **several times** in order to enroll.
- ▮ Enrollment score or quality score indicates the enrollment attempt is successful or not.
- ▮ If the user's biometric data contains **highly distinctive features or an abundance of features**, there will likely be a high enrollment score.
- ▮ Vendor's feature extraction processes are generally patented and are always held secret.



# HOW BIOMETRIC MATCHING WORKS

---

- Verification/Identification template is compared with enrollment templates.
- The comparison renders **a score, or confident value**.
- The score is compared with **threshold**.
- If the score exceeds the threshold, the comparison is a match, non-match otherwise.

# BIOMETRIC ALGORITHM

---

- A biometric algorithm is a recipe for turning **raw data** - like physical traits - into a digital representation in the form of a template. It also allows the matching of an enrolled template with a new template just created for verifying an identity, called the **live template**.

# BIOMETRIC MATCHING

---

- Matching is the comparison of **enrolled biometric templates** with **a new template** just created for verification to determine their degree of similarity or correlation.
- In **verification** systems, a verification template is matched against a user's enrollment template or templates (multiple).
- In **Identification** systems, the verification template is matched against dozens, thousands, even millions of enrollment templates.



# BIOMETRIC MATCHING – SCORING

- Biometric systems utilize proprietary algorithms to process templates and generate scores.
- Some of them use a scale of 1 to 100, others use a scale of -1 to 1.
- Traditional authentication methods such as password offer on a yes'/no response.
- In biometric system, there is no 100 percent correlation between enrollment and verification templates.

# BIOMETRIC MATCHING –THRESHOLD

- ▮ A threshold is a predefined number, which establishes the degree of correlation necessary for a comparison to be deemed a match.
- ▮ Thresholds can vary from user to user, from transaction to transaction, and from verification to verification attempt.
- ▮ System can be either highly secure for valuable transaction or less secure for low-value transaction, depending on their threshold settings.
- ▮ Traditional authentication can not offer such flexibility.

# BIOMETRIC MATCHING – DECISION

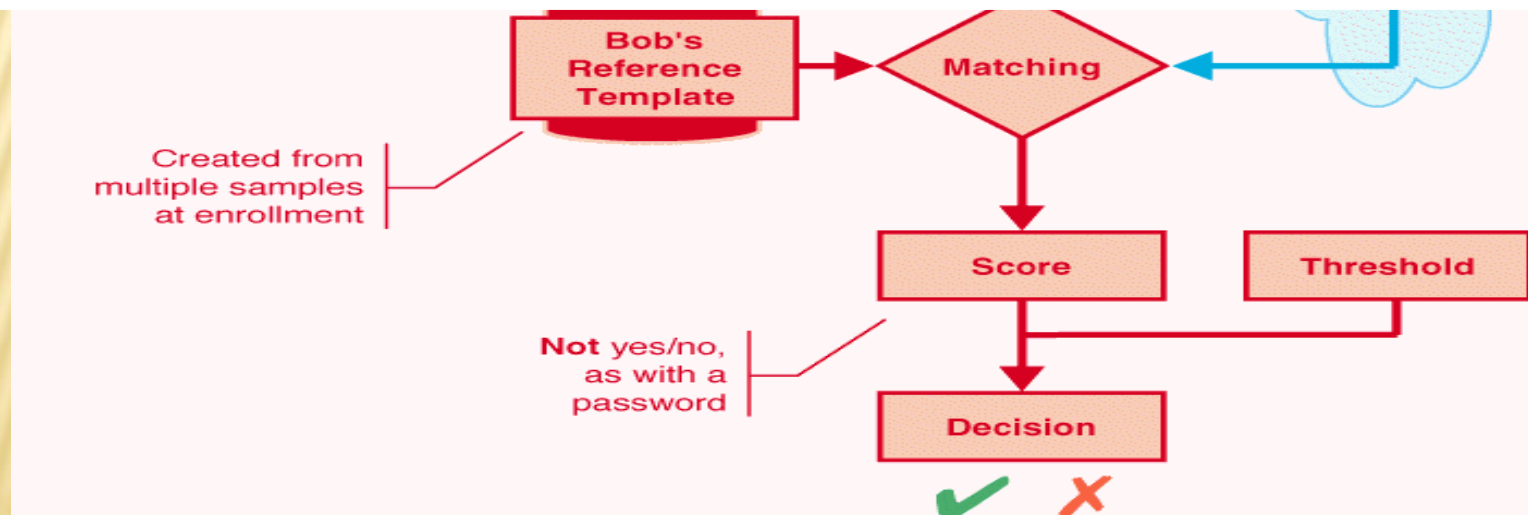
---

- The result of the comparison between the score and the threshold is a decision.
- The decisions a biometric system can make include *match*, *non-match*, and *inconclusive*.



# BIOMETRIC MATCHING: PROCESS FLOW

- The user submits a sample (biometric data) via an acquisition device (for example, a scanner or camera)
- This biometric is then processed to extract information about distinctive features to create a trial template or verification template
- Templates are large number sequences. The trial/match template is the user's "password."
- Trial/match template is compared against the reference template stored in biometric database.



# OVERVIEW OF BIOMETRICS

Biometric	Acquisition Device	Sample	Feature Extracted
Iris	Infrared-enabled video camera, PC camera	Black and white iris image	Furrows and striations of iris
Fingerprint	Desktop peripheral, PC card, mouse chip or reader embedded in keyboard	Fingerprint image (optical, silicon, ultrasound or touchless)	Location and direction of ridge endings and bifurcations on fingerprint, minutiae
Voice	Microphone, telephone	Voice Recording	Frequency, cadence and duration of vocal pattern
Signature	Signature Tablet, Motion-sensitive stylus	Image of Signature and record of related dynamics measurement	Speed, stroke order, pressure and appearance of signature
Face	Video Camera, PC camera, single-image camera	Facial image (optical or thermal)	Relative position and shape of nose, position of cheekbones
Hand	Proprietary Wall-mounted unit	3-D image of top and sides of hand	Height and width of bones and joints in hands and fingers
Retina	Proprietary desktop or wall mountable unit	Retina Image	Blood vessel patterns and retina

# STRENGTHS, WEAKNESSES AND USABILITY OF BIOMETRICS

Biometric	Strengths	Weakness	Usability
Iris	<ul style="list-style-type: none"> <li>• Very stable over time</li> <li>• Uniqueness</li> </ul>	<ul style="list-style-type: none"> <li>• Potential user resistance</li> <li>• Requires user training</li> <li>• Dependant on a single vendor's technology</li> </ul>	<ul style="list-style-type: none"> <li>• Information security access control, especially for Federal Institutions and government agencies</li> <li>• Physical access control (FIs and government)</li> <li>• Kiosks (ATMs and airline tickets)</li> </ul>
Fingerprint	<ul style="list-style-type: none"> <li>• Most mature biometric technology</li> <li>• Accepted reliability</li> <li>• Many vendors</li> <li>• Small template (less than 500 bytes)</li> <li>• Small sensors that can be built into mice, keyboards or portable devices</li> </ul>	<ul style="list-style-type: none"> <li>• Physical contact required (a problem in some cultures)</li> <li>• Association with criminal justice</li> <li>• Vendor incompatibility</li> <li>• Hampered by temporary physical injury</li> </ul>	<ul style="list-style-type: none"> <li>• IS access control</li> <li>• Physical access control</li> <li>• Automotive</li> </ul>
Optical	<ul style="list-style-type: none"> <li>• Most proven over time</li> <li>• Temperature stable</li> </ul>	<ul style="list-style-type: none"> <li>• Large physical size</li> <li>• Latent prints</li> <li>• CCD coating erodes with age</li> <li>• Durability unproven</li> </ul>	



# STRENGTHS, WEAKNESSES AND USABILITY OF BIOMETRICS

Biometrics	Strengths	Weakness	Usability
<b>Silicon</b>	<ul style="list-style-type: none"> <li>• Small physical size</li> <li>• Cost is declining</li> </ul>	<ul style="list-style-type: none"> <li>• Requires careful enrollment</li> <li>• Unproven in sub optimal conditions</li> </ul>	
<b>Ultrasound</b>	<ul style="list-style-type: none"> <li>• Most accurate in sub optimal conditions</li> </ul>	<ul style="list-style-type: none"> <li>• New technology, few implementations</li> <li>• Unproven long term performance</li> </ul>	
<b>Voice</b>	<ul style="list-style-type: none"> <li>• Good user acceptance</li> <li>• Low training</li> <li>• Microphone can be built into PC or mobile device</li> </ul>	<ul style="list-style-type: none"> <li>• Unstable over time</li> <li>• Changes with time, illness stress or injury</li> <li>• Different microphones generate different samples</li> <li>• Large template unsuitable for recognition</li> </ul>	<ul style="list-style-type: none"> <li>• Mobile phones</li> <li>• Telephone banking and other automated call centers</li> </ul>
<b>Signatures</b>	<ul style="list-style-type: none"> <li>• High user acceptance</li> <li>• Minimal training</li> </ul>	<ul style="list-style-type: none"> <li>• Unstable over time</li> <li>• Occasional erratic variability</li> <li>• Changes with illness, stress or injury</li> <li>• Enrollment takes times</li> </ul>	<ul style="list-style-type: none"> <li>• Portable devices with stylus input</li> <li>• Applications where a “wet signature” ordinarily would be used.</li> </ul>

# STRENGTHS, WEAKNESSES AND USABILITY OF BIOMETRICS

Biometric s	Strengths	Weakness	Usability
<b>Face</b>	<ul style="list-style-type: none"> <li>• Universally present</li> </ul>	<ul style="list-style-type: none"> <li>• Cannot distinguish identical siblings</li> <li>• Religious or cultural prohibitions</li> </ul>	<ul style="list-style-type: none"> <li>• Physical access control</li> </ul>
<b>Hand</b>	<ul style="list-style-type: none"> <li>• Small template (approximately 10 bytes)</li> <li>• Low failure to enroll rate</li> <li>• Unaffected by skin condition</li> </ul>	<ul style="list-style-type: none"> <li>• Physical size of acquisition device</li> <li>• Physical contact required</li> <li>• Juvenile finger growth</li> <li>• Hampered by temporary physical injury</li> </ul>	<ul style="list-style-type: none"> <li>• Physical access control</li> <li>• Time and attendance</li> </ul>
<b>Retina</b>	<ul style="list-style-type: none"> <li>• Stable over time</li> <li>• Uniqueness</li> </ul>	<ul style="list-style-type: none"> <li>• Requires user training and cooperation</li> <li>• High user resistance</li> <li>• Slow read time</li> <li>• Dependent on a single vendor's technology</li> </ul>	<ul style="list-style-type: none"> <li>• IS access control, especially for high security government agencies</li> <li>• Physical access control (same as IS access control)</li> </ul>

# ACCURACY IN BIOMETRIC SYSTEMS

---



# HOW TO EVALUATE PERFORMANCE OF A SPECIFIC TECHNOLOGY?

---

- ❑ False acceptance rate
- ❑ False rejection rate
- ❑ Failure-to-enroll rate
- ❑ No single metric indicates how well a biometric system or device performs:  
**Analysis of all three metrics is necessary to assess the performance of a specific technology.**

# FALSE ACCEPTANCE RATE

---

- ▮ If John Smith enters Jane Doe's username or ID, presents biometric data, and successfully matching as Jane Doe.
- ▮ This is classified as **false acceptance**.
- ▮ The probability of this happening is referred to as **false acceptance rate** (FAR)[ stated as: percentage, fraction]
- ▮ This is because two people have *similar enough biometric characteristics* – a fingerprint, a voice, or a face – that the system finds a *high degree of correlation* between the users' template.

# FALSE ACCEPTANCE RATE

---

- ❑ FAR can be *reduced* by adjusting the thresholds but the false rejection rate will increase.
- ❑ A system with a false acceptance rate of *0 percent*, but false rejection rate of *50 percent*, is secure but unusable.
- ❑ False acceptance rate is the most critical accuracy metric because an imposter break-in will certainly be a more attention-getting event than other failings of a biometric system.
- ❑ The most important false match metric in real-world deployments is the *system false match rate*.



# FALSE REJECTION RATE

---

- ▮ If John Smith enters his username or ID, presents his biometric data to a biometric system, and fails to match.
- ▮ This is classified as **false rejection**.
- ▮ The probability of this happening is the **false rejection rate** (FRR).
- ▮ This can be attributed to changes in user's biometric data, changes in how a user presents biometric data, and changes in the environment in which data is presented.
- ▮ High FRR will result in lost productivity, frustrated users, and an increased burden on help desk or support personnel.

# REASONS OF FRR

---

- ▮ Changes in user's biometric data
  - ▮ Voice-scan system is influenced by sore throats
  - ▮ Facial-scan system is affected by changes in weight
  - ▮ Fingerprint changes over time, scars, aging and general wear.

# ACCEPTANCE AND REJECTIONS

---

- If someone else is trying to verify as you, the system would try to match the two templates.
  - If the two templates were to match – this is classified as **false acceptance**.
  - If your authentication template fails to match your enrolled template, then this is referred to as a **false rejection**.
  - If you are new and fail to enroll to a biometric system, this is called – **failure to enroll** (FTE).



# ACCURACY RATES

---

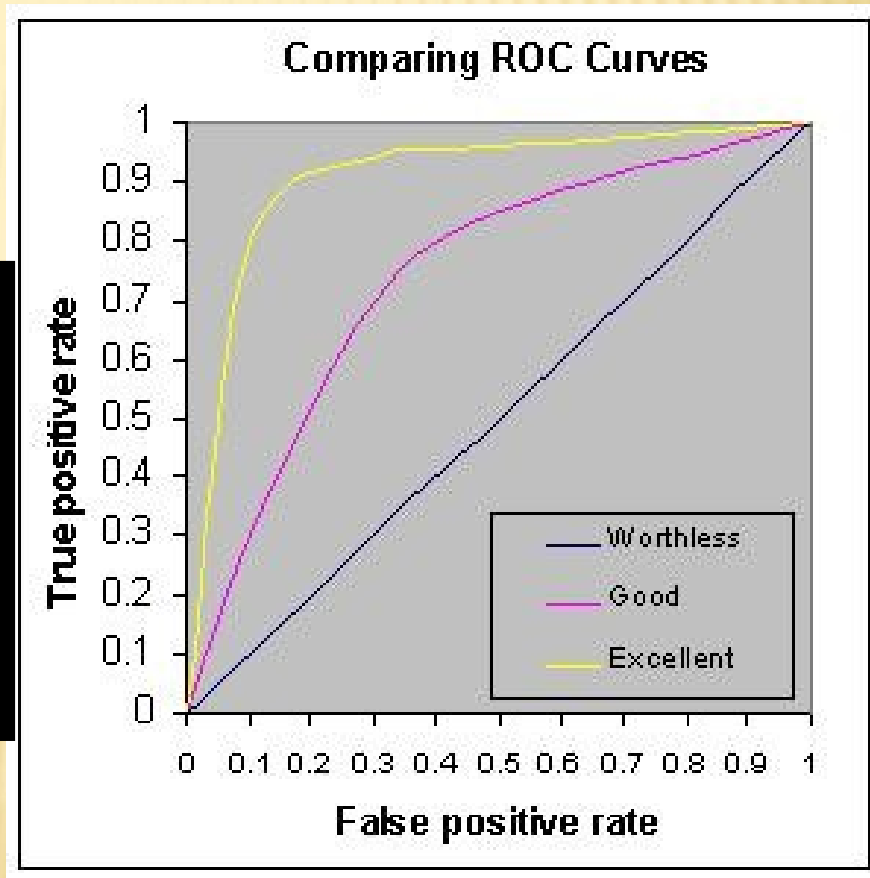
- Single False Acceptance Rate vs. System False Acceptance Rate
  - If the FAR is 1/10,000 but you have 10,000 templates on file — odds of a match are very high
- Ability to Verify (ATV) rate:
  - % of user population that can be verified
  - $ATV = (1-FTE)(1-FRR)$

# RECEIVER OPERATING CHARACTERISTIC (ROC) CURVE

- Cost/benefit analysis of decision making.
- Tradeoff b/w true acceptance rate and false rejection rate.

Legitimate users  
get accepted.

True acceptance  
rate



Legitimate users  
get rejected.

False rejection rate

# THE FUTURE OF BIOMETRICS

---



# OPERATION AND PERFORMANCE

- ▮ In a typical IT biometric system, a person registers with the system when one or more of his physical and behavioral characteristics are obtained. This information is then processed by a numerical algorithm, and entered into a database.
- ▮ The algorithm creates a digital representation of the obtained biometric – a template.
- ▮ If the user is new to the system, he or she enrolls, which means that the digital template of the biometric is entered into the database.
- ▮ Each subsequent attempt to use the system, or authenticate, requires the biometric of the user to be captured again, and processed into a digital template. That template is then compared to those existing in the database to determine a match.
- ▮ The process of converting the acquired biometric into a digital template for comparison is completed each time the user attempts to authenticate to the system.
- ▮ The comparison process involves the use of a Hamming distance. This is a measurement of how similar two bit strings are.

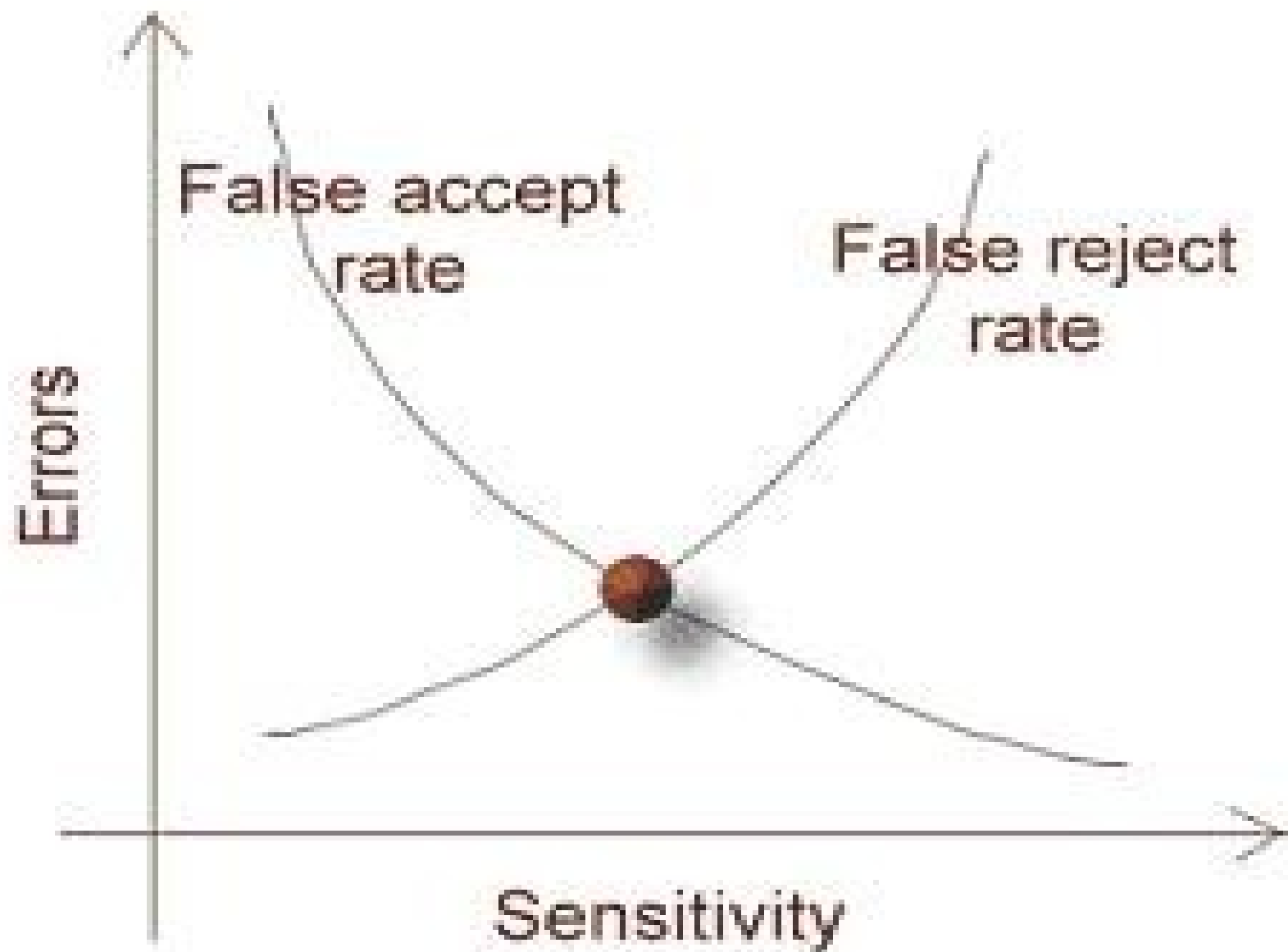
- ▮ For example, two identical bit strings have a Hamming Distance of zero, while two totally dissimilar ones have a Hamming Distance of one.
- ▮ Thus, the Hamming distance measures the percentage of dissimilar bits out of the number of comparisons made.
  - ▮ Ideally, when a user logs in, nearly all of his/her features match;
  - ▮ However, if someone else tries to log in, who does not fully match, the system will not allow the new person to log in.
- ▮ Current technologies have widely varying Equal Error Rates, varying from as low as 60% and as high as 99.9%.

## ▢ Performance of a biometric measure is usually referred to in terms:

- ▢ false accept rate (FAR)- percent of invalid users who are incorrectly accepted as genuine users,
  - ▢ false non match or reject rate (FRR)- percent of valid users who are rejected as impostors ,
  - ▢ failure to enroll rate (FTE or FER).
- ▢ In real-world biometric systems the FAR and FRR can typically be traded off against each other by changing some parameter.



- One of the most common measures of real-world biometric systems is the rate at which both accept and reject errors are equal:
  - the equal error rate (EER),
  - also known as the cross-over error rate (CER).
- The lower the EER or CER, the more accurate the system is considered to be.
- An EER is desirable for a biometric system because it balances the sensitivity of the system.



Biometrics	Univer- sality	Unique- ness	Perma- nence	Collect- ability	Perfor- mance	Accept- ability	Circum- vention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L
H=High, M=Medium, L=Low							



# ISSUES AND CONCERNS

- Excessive concern with the biometric may have the an eclipsing effect on the performance of the technology that one could:
  - plant DNA at the scene of the crime
  - associate another's identity with his biometrics, thereby impersonating without arousing suspicion
  - interfere with the interface between a biometric device and the host system, so that a "fail" message gets converted to a "pass".

# IDENTITY THEFT AND PRIVACY ISSUES

- ▮ Concerns about Identity theft through biometrics use have not been resolved. If their iris scan is stolen, though, and it allows someone else to access personal information or financial accounts, the damage could be irreversible.
- ▮ Often, biometric technologies have been rolled out without adequate safeguards for personal information gathered about individuals.
- ▮ Also, the biometric solution to identity theft is only as good as the information in the database that is used for verifying identity.
- ▮ There are problems of getting accurate and usable initial information (enrollment) -- witness the current troubles with the No fly list of the Dept of Homeland security.
- ▮ Presumably after the initial information is correctly stored, future computer error or vandalism (hacking) would prevent biometrics from being 100% foolproof against identity theft.
- ▮ Because biometrics are touted as a way to restrict criminality, privacy advocates fear biometrics may be used to diminish personal liberties of law abiding citizens as well.
- ▮ .



# SOCIOLOGICAL CONCERNS

- ▮ As technology advances, more private companies and public utilities are using biometrics for safe, accurate identification. However, these advances are raising more concerns like:
  - ▮ Physical - Some believe this technology can cause physical harm to an individual using the methods, or that instruments used are unsanitary. For example, there are concerns that retina scanners might not always be clean.
  - ▮ Personal Information - There are concerns whether our personal information taken through biometric methods can be misused, tampered with, or sold, e.g. by criminals stealing, rearranging or copying the biometric data. Also, the data obtained using biometrics can be used in unauthorized ways without the individual's consent.
- ▮ Society fears in using biometrics will continue over time. As the public becomes more educated on the practices, and the methods are being more widely used, these concerns will become more and more evident.
- ▮ This technology is being used at border crossings that have electronic readers that are able to read the chip in the cards and verify the information present in the card and on the passport.
- ▮ This method allows for the increase in efficiency and accuracy of identifying people at the border crossing. CANPASS, by Canada Customs is currently being used by some major airports that have kiosks set up to take digital pictures of a person's eye as a means of identification.



# CONCLUSIONS

- ▮ Despite these misgivings, biometric systems have the potential to identify individuals with a very high degree of certainty.
- ▮ Forensic DNA evidence enjoys a particularly high degree of public trust at present
- ▮ Also substantial claims are being made in respect of iris recognition technology, which has the capacity to discriminate between individuals with identical DNA, such as monozygotic twins.