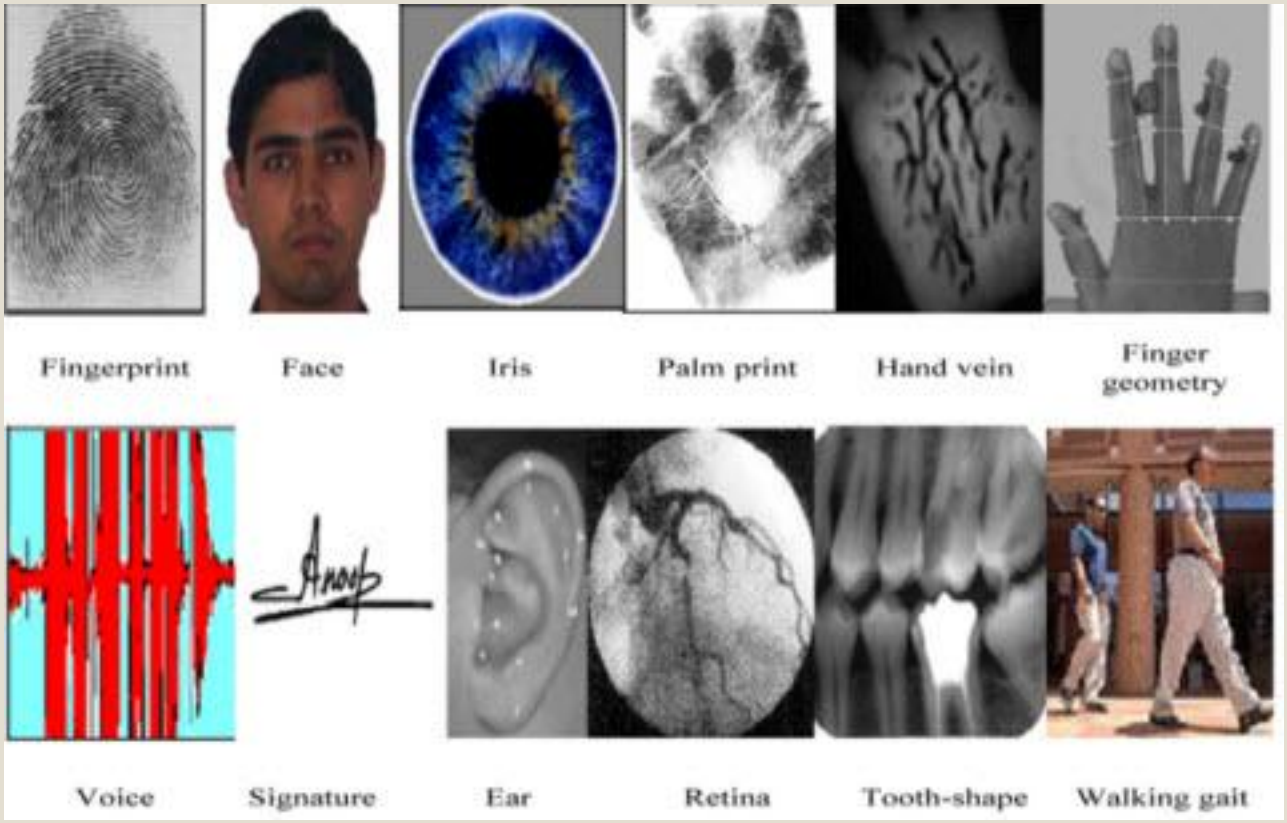
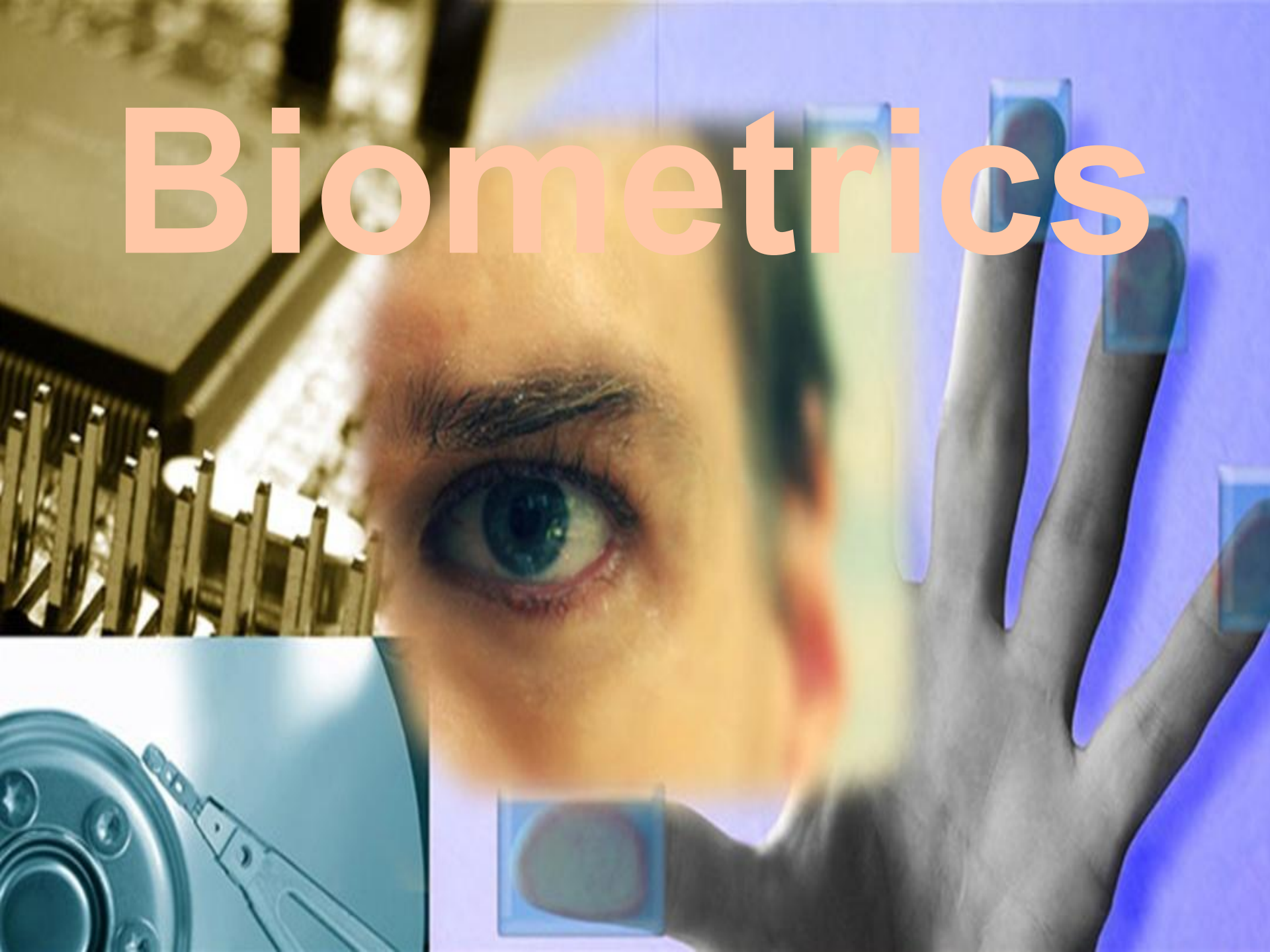

SCAN COMPLETE
PASSWORD PROTECT
HACKING DETECTED

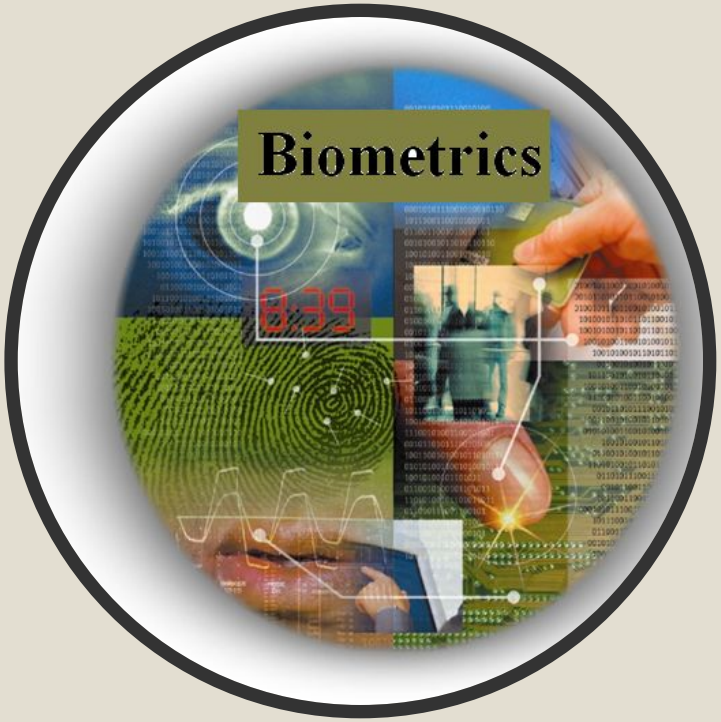

Fingerprint
Face
Iris
Palm print
Hand vein
Finger geometry
Voice
Signature
Ear
Retina
Tooth-shape
Walking gait

Biometrics



Biometrics Overview

- **What are Biometrics?**
  - Automated methods of identifying or verifying the identity of a person based on a physiological or behavioral characteristic



- **Physical:**
  - Fingerprint
  - Facial Recognition
  - Hand Geometry
  - Iris Scan
  - Retinal Scan
  - DNA
- **Behavioral:**
  - Speaker Recognition
  - Signature Recognition

Biometrics Overview

2 ways to recognize a person:

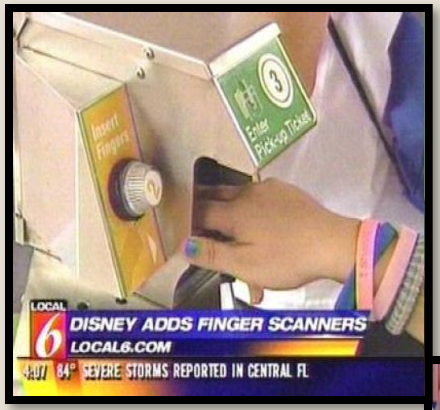
- Verification
  - *Am I who I claim to be?*
- Identification
  - *Who am I?*

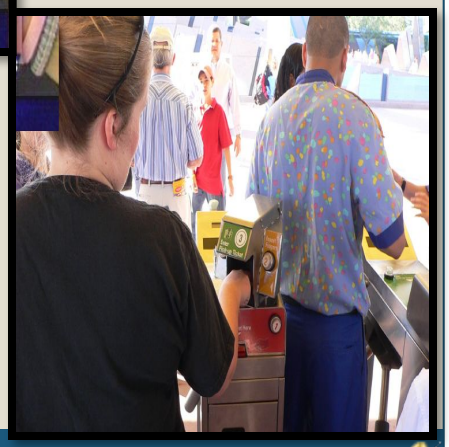
Confirm or establish identity based on <u>who person is</u>

- NOT what person possesses
  - ID card
- NOT what person remembers
  - Password

Fingerprint

- Fingerprint Pattern Analysis
- Typical System: fingerprint scanner maps the series of whorls, ridges, furrows and minutiae on the surface of the finger
- Applications:
  - Law Enforcement
  - Entry Devices for Buildings
  - Computer Network Access
  - New: grocery stores checkout, ATM authorization
- Softwares used :
  - C#, VB.Net, VB 6.0 etc



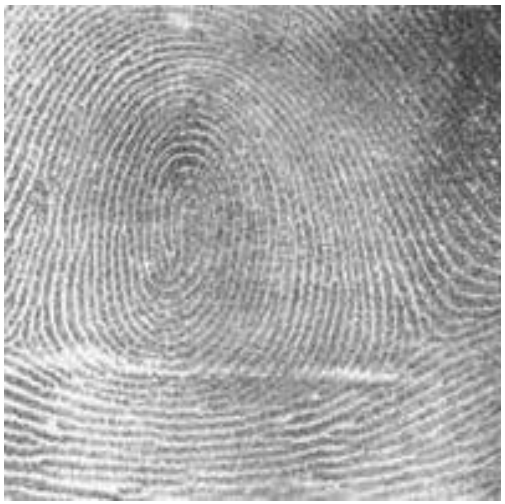


Fingerprint : Background

- The analysis of fingerprints for matching purposes generally requires the comparison of several features of the ***print pattern***. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns.

Arch

Loop



Whorl

Fingerprint : Background

- The major Minutia features of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

Ridge Ending

Bifurcation

Short Ridge (Dot)

Facial Recognition

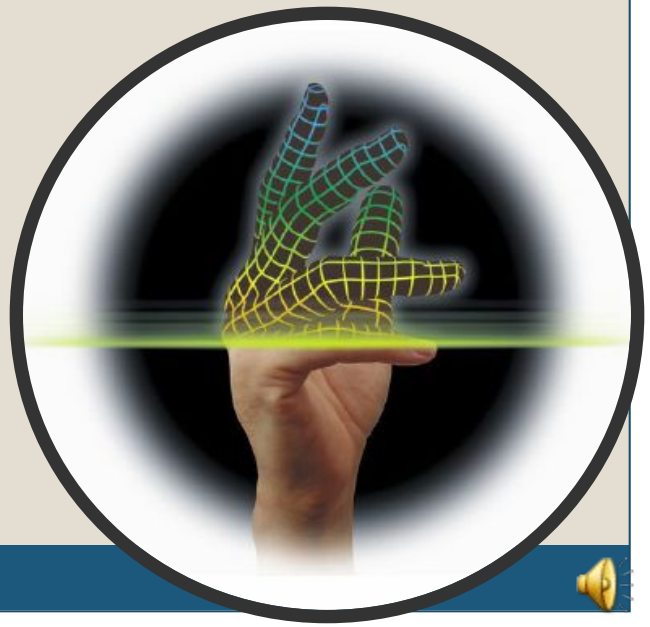
- Face characteristics analysis
- Typical system: digital video camera input of a person's face images - measures facial structure; compares against database
- Principle: analysis of the unique shape, pattern and positioning of facial features.
- Applications:
  - Law enforcement
  - Automated bank tellers- user verification purposes

Facial Recognition : Techniques

- **Traditional**
  - Some facial recognition algorithms identify facial features by extracting landmarks, or features, from an image of the subject's face, for example, the relative position, size, and/or shape of the eyes, nose, cheekbones, and jaw. These features are then used to search for other images with matching features.
- **3-D Recognition**
  - This technique uses 3D sensors to capture information about the shape of a face. This information is then used to identify distinctive features on the surface of a face, such as the contour of the eye sockets, nose, and chin.
  - One advantage of 3D facial recognition is that it is not affected by changes in lighting like other techniques. It can also identify a face from a range of viewing angles.
- **Skin Texture Analysis**
  - Another emerging trend uses the visual details of the skin, as captured in standard digital or scanned images. This technique, called skin texture analysis, turns the unique lines, patterns, and spots apparent in a person’s skin into a mathematical space. Increases performance by 20 to 25 percent.

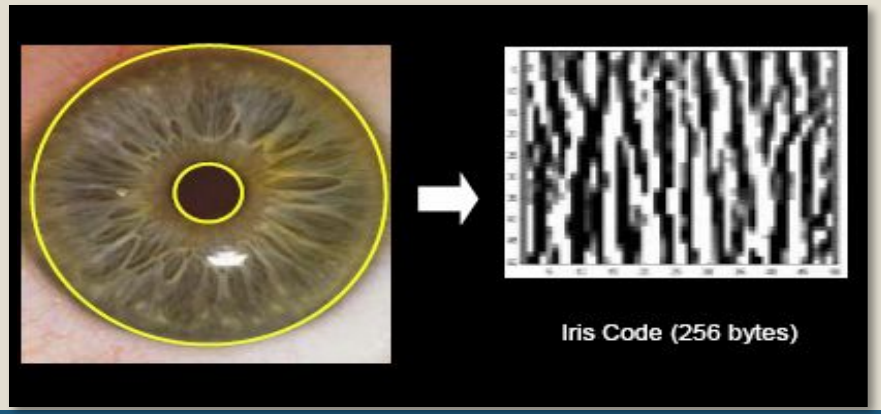
Hand Geometry

- Hand shape analysis and measurement
- Typical system: scanners with guidance pegs that position the hand property for analysis
- A camera captures an image of the hand, with the help of a mirror to get also the edge. The silhouette/shape of the hand is extracted, and some geometrical characteristics stored.
- Applications:
  - Access Control for Airports
  - Immigration facilities
  - Day Care Centers
  - Time & Attendance Operations



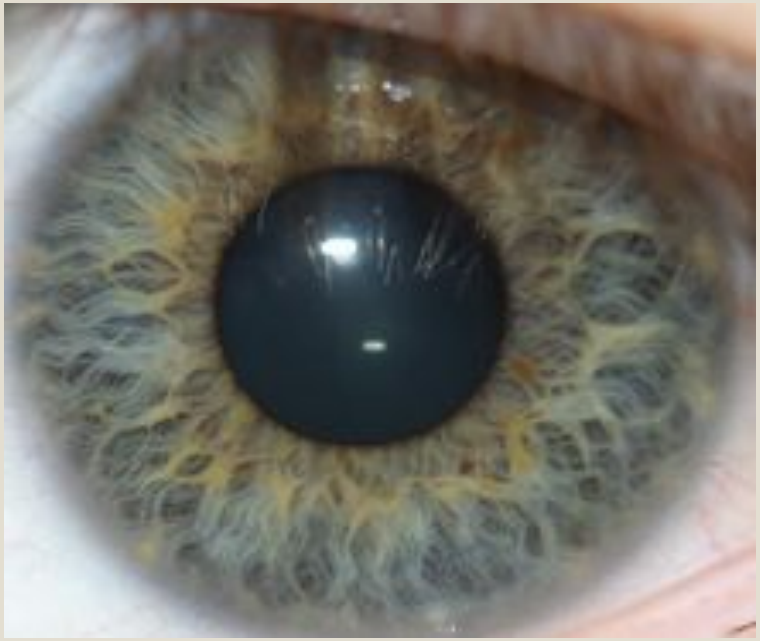
Iris Recognition

- Iris analysis
- Typical system: scanner analyzes the colored tissue around the pupil – 200 points: rings, furrows, freckles
- Applications:
  - Law Enforcement
  - Employee Security Check



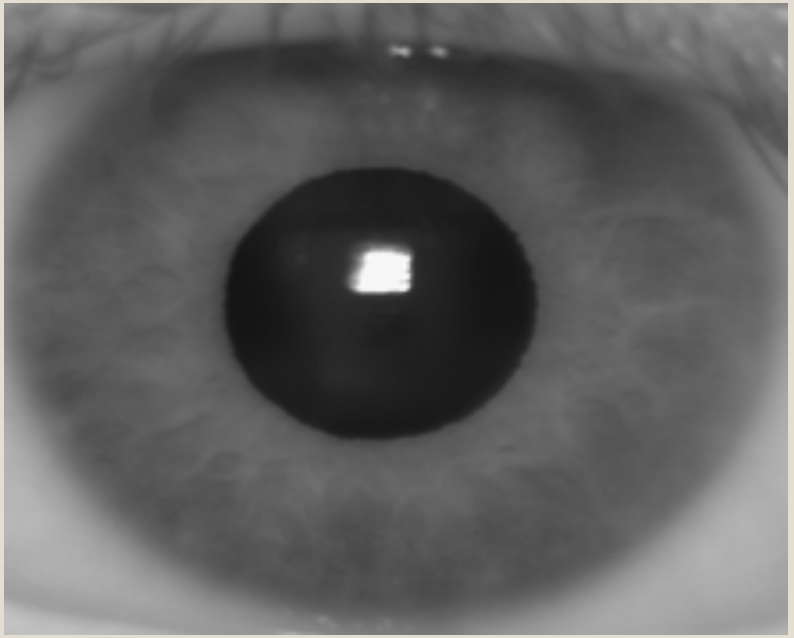
Iris Recognition

Visible Wavelength Iris Image



- Visible light reveals rich pigmentation details of an Iris by exciting Melanin, the main colouring component in the iris.

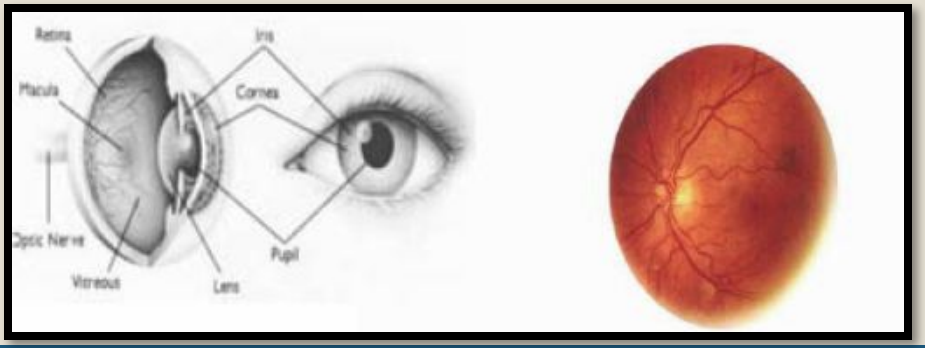
Near Infrared (NIR) version



- Pigmentation of the Iris is much less visible due to the negligible effects of Melanin at longer wavelengths in the NIR spectrum

Retina Scanning

- Analysis of layer of blood vessels at the back of the eye
- Typical system: low-intensity light source and an optical coupler; the user needs to remove glasses, keep the eye focused on the light, 15 seconds
- Applications:
  - High-end security: military etc.
  - Used for authentication and identification purposes

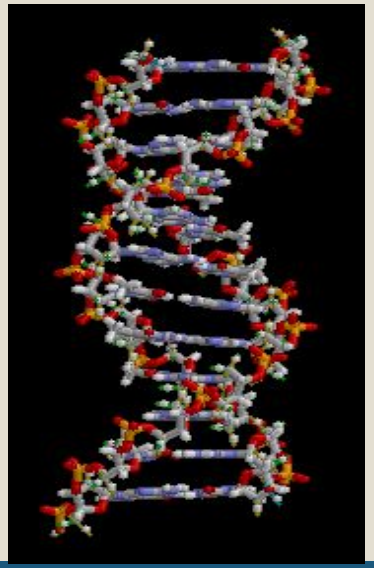


Retina Scanning

- The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. The network of blood vessels in the retina is so complex that even identical twins do not share a similar pattern.
- A biometric identifier known as a **retinal scan** is used to map the unique patterns of a person's retina. The blood vessels within the retina absorb light more readily than the surrounding tissue and are easily identified with appropriate lighting. A retinal scan is performed by casting an unperceived beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece. This beam of light traces a standardized path on the retina. Because retinal blood vessels are more absorbent of this light than the rest of the eye, the amount of reflection varies during the scan. The pattern of variations is converted to computer code and stored in a database.

DNA (Deoxyribonucleic acid)

- A DNA sample is used to produce either a DNA fingerprint or a DNA profile
- DNA has been called the “ultimate identifier”
- Identifies information from every cell in the body in a digital form
- Not yet fully automated, not fast and expensive
- Applications:
  - Medical applications
  - Paternity Tests
  - Criminal identification and forensics
  - Commercial applications limited



Speaker Recognition

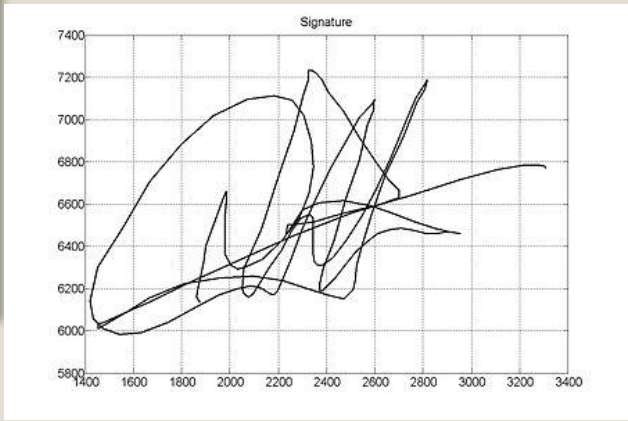
- Voice print analysis
- Typical system: uses the pitch, pattern, tone, rhythm of speech for identification purposes; only biometric that allows users to authenticate remotely
- Applications:
  - Call Centers
  - Law enforcement – house arrest authentication
  - Electronic commerce
  - Customer authentication for service calls

Speaker Recognition

- **Verification versus Identification**
  - There are two major applications of *speaker recognition* technologies and methodologies. If the speaker claims to be of a certain identity and the voice is used to verify this claim, this is called *verification* or *authentication*. On the other hand, *identification* is the task of determining an unknown speaker's identity. In a sense *speaker verification* is a 1:1 match where one speaker's voice is matched to one template (also called a "voice print" or "voice model") whereas *speaker identification* is a 1:N match where the voice is compared against N templates.
- **Variants of Speaker Recognition**
  - Each *speaker recognition* system has two phases: Enrollment and verification. During enrollment, the speaker's voice is recorded and typically a number of features are extracted to form a *voice print*, *template*, or *model*. In the verification phase, a speech sample or "utterance" is compared against a previously created voice print. For identification systems, the utterance is compared against multiple voice prints in order to determine the best match(es) while verification systems compare an utterance against a single voice print. Because of the process involved, verification is faster than identification.

Signature Recognition

- **Signature recognition** is a behavioural biometric. It can be operated in two different ways:
  - **Static:** In this mode, users write their signature on paper, digitize it through an optical scanner or a camera, and the biometric system recognizes the signature analyzing its shape. This group is also known as “off-line”.
  - **Dynamic:** In this mode, users write their signature in a digitizing tablet, which acquires the signature in real time. Another possibility is the acquisition by means of stylus-operated PDAs. Dynamic recognition is also known as “on-line”.
- Applications
  - Access to documents
  - Execution of contracts
  - Banking services



Comparison Chart Accuracy/Reliability

Biometric	Accuracy	Reliability	Errors
Fingerprint	Very High	High	Dirt, dryness
Facial Recognition	High	Medium	Hair, glasses, age
Hand Geometry	High	Medium	Hand injury
Iris Scan	Very High	High	Poor lighting
Retinal Scan	Very High	High	Glasses
DNA	Very High	High	none
Speaker Recognition	Medium	Low	Noise, colds
Signature Recognition	Medium	Low	Changing signatures

Accuracy: How well can the specific biometric is able to tell individual apart
Reliability: how dependable the specific biometric is for recognition purposes

What Biometrics are Replacing

Traditional verification methods:

- Passwords
  - PIN numbers
- Tokens
  - Photo ID cards
  - Smart cards
  - Magnetic strip cards
  - Physical keys
  - Key chains

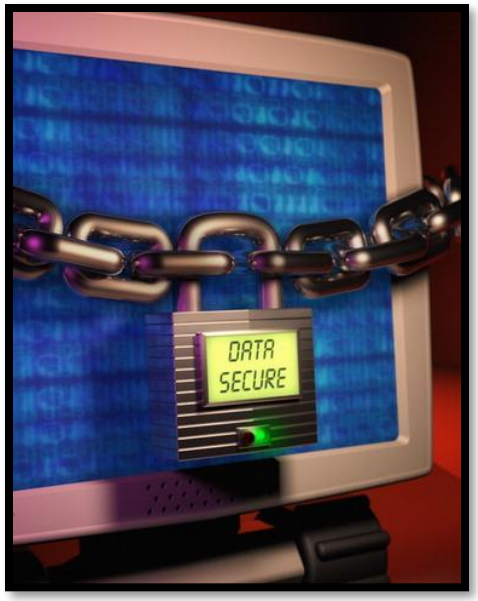
Benefits of Biometrics

- Increased security

- Convenience

- Opportunity to build a sustainable competitive advantage

- Growing technology and advancement



Benefits of Biometrics

For Employers

- **Increased security measures** due to lack of sharing passwords and identification cards
- **Reduce costs** of password and ID card maintenance
- **Reduce payroll costs** of "buddy punching" timecards
- **Sustainable competitive advantage** for businesses – advanced technology to ensure security for clientele
- Ability to **track employees** and link activities

For Employees

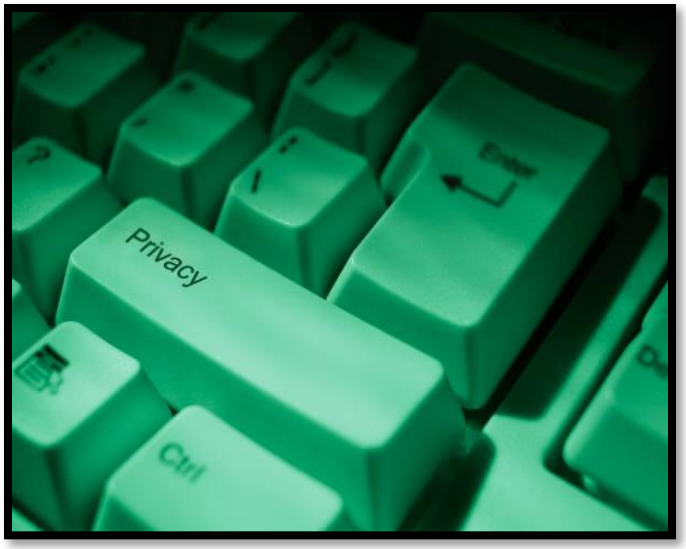
- **Convenience** – no passwords to forget
- **Eliminate problems** of long passwords and lost/stolen identification cards and PIN numbers
- **Faster login time**
- **Improved security** of sensitive information

Concerns with Biometrics

- Sensitive biometric information susceptible to hackers

- Lack of privacy for employees

- Costly and time consuming to implement



Concerns with Biometrics

For Employers

- Biometric data is very sensitive and security of this information is vital – more **susceptible to hackers**
- It is possible to **steal fingerprints** by using the "latent fingerprint" – residue left from touching a surface
- Text-based **voice recognition may have errors** identifying individuals if their voice changes
- Biometrics **can't be used with certain groups** such as people with disabilities
- Biometrics, like all other security identification methods, is **not foolproof**
- Biometric systems **costly and time consuming** to implement

For Employees

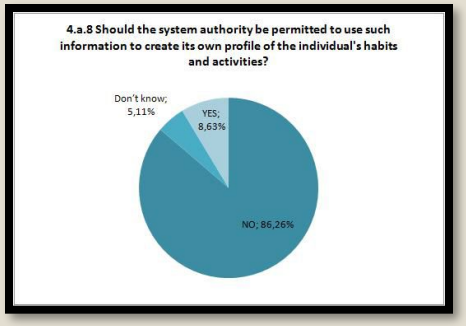
- Biometrics can seem **intrusive** to employees – intrudes on personal space
- Employees may be **reluctant to change**
- Biometric identification **cannot work with all employees,** such as disabled individuals
- Employees **scared** of biometric information to be **abused or stolen**

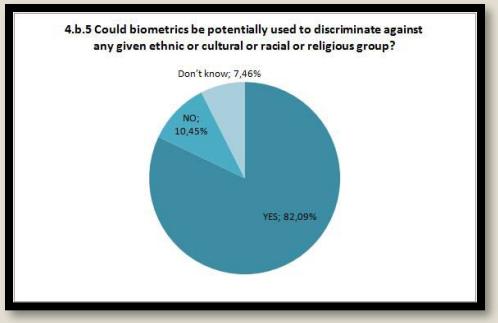
Concerns with Biometrics

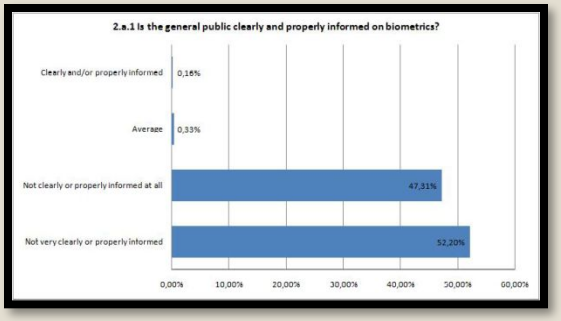
- As with many emerging technologies, there are concerns with the abuse of biometric technology and identification.
- **The BITE Project** (Biometric Identification Technology Ethics) is a team in Europe that looks at the social, cultural and ethical factors arising from emerging biometric identification technologies.

Concerns with Biometrics

- The information gathered from The BITE project is helpful to understand the scope of how employees view biometric technology and their concerns of ethics and privacy.
  - 99.51% surveyed feel the general public is not clearly or poorly informed of biometrics
  - 82.09% feel that biometrics can potentially used to discriminate against ethnic/cultural/racial/religious groups
  - 86.26% feel biometrics should not be permitted to use information to create its own profile of the individual's habits and activities







Biometrics in Business

Current Biometric Applications:

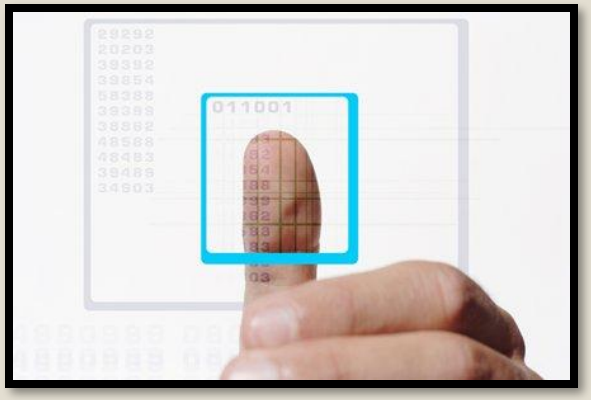
- Computer logins
- ATMs
- Grocery stores
- Airport kiosks
- Driver's licenses
- Internet banking
- National ID cards
- Welfare disbursement
- International border crossing
- Forensics – criminal identification
- Annual amusement park pass holders
- Speaker verification for television home shopping

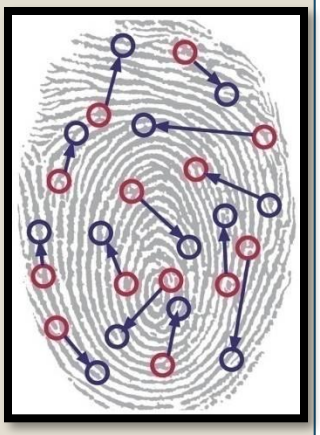
Biometrics in Business

- Signature verification:
  - Electronic commerce
  - E-business essential factors for growth:
    - Highly secure
    - Trustworthy

- Speaker recognition:
  - Large voice processing
  - Verify customer during transactions via telephone

- Fingerprint identification:
  - Social services
  - Background checks
  - Criminal identification





Biometrics in Business

Other biometric technology being used:

- Automobiles
  - Replace keys for keyless entry and keyless ignition
- E-passports
  - Passports with embedded chip containing person's facial image and other traits

Biometrics in Business

Travel and Transport

- Biometrics is growing in the travel and transportation industry due to heightened security measures since 9/11
- Examples of how biometrics will be used in the future:
  - Identification of employees in secure areas at airports, ports
  - Identification of passengers and monitor of international travel against illegal immigrants
  - Surveillance of individuals in terminals in regards to criminal activities
  - Visa control


Thanks