# Introduction to Biometrics

Brian Lovell

# Outline

- Definition of Biometrics
- Biometrics vs alternative methods of identification
- Types of Biometric technologies
  - Fingerprint, face, iris, voice
- Terminology
  - Enrolment, templates, matching, accuracy, false reject, false accept
- Description of technologies:
  - Fingerprint, Face, Iris, Voice
- Implementation issues
- Cultural and social issues
- Overview of private sector trends
- Government uses of biometrics

# Definition of Biometrics

1. Biometrics is the science and technology of measuring and analyzing biological data. (e.g. Biometrica Journal)
2. In information technology, **biometrics refers to technologies that measure and analyze human body characteristics**, such as DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, **for authentication purposes.**

- http://searchsecurity.techtarget.com/definition/biometrics

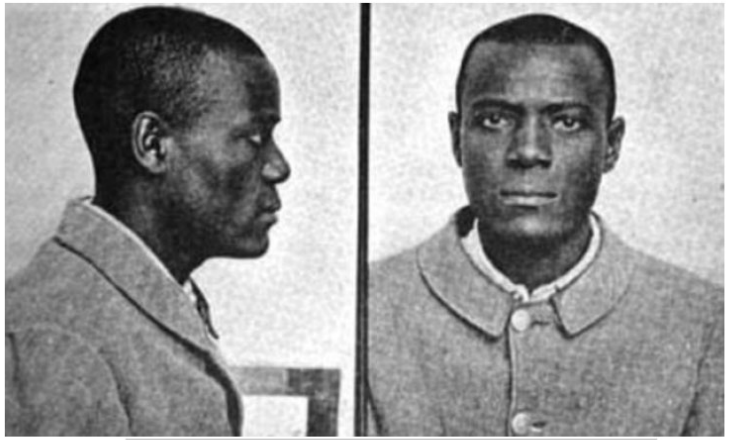
# Early History

- In the early 1900's the law was changed so that punishment was increased for repeat offenders
- The need emerged to identify re-offenders
- Bertillon's *Identification anthropométrique* (1893)


1. Taille. — 2. Envergure. — 3. Buste. —
4. Longueur de la tête. — 5. Largeur de la tête. — 6. Oreille droite. —
7. Pied gauche. — 8. Médius gauche. — 9. Coudée gauche.

# The Strange Case of Will West and William West

Where there's a Will: In 1903 Will West arrived at Leavenworth Penitentiary in Kansas, where the records clerk was certain that he'd seen him before



Where there's another Will: The record clerk pulled out this file photo of William West, who looked almost identical to Will West

McClaughry, still convinced the man before him had already been to the prison, looked up his name in his filing system and found one William West – who looked identical to Will West in the photographs in every respect.

They even shared the same Bertillon measurements.

But Will West insisted to McClaughry that it was not him: 'That's my picture, but I don't know where you got it, for I know I have never been here before.'

To McClaughry's shock, he was absolutely right, too. William West was a different person altogether and in fact had been admitted to the prison two years previously for murder.

The case highlighted the flaws in the Bertillon method and it wasn't long before the U.S authorities turned to fingerprinting.

http://www.dailymail.co.uk/news/article-1392418/The-amazing-pictures-sparked-need-fingerprinting.html

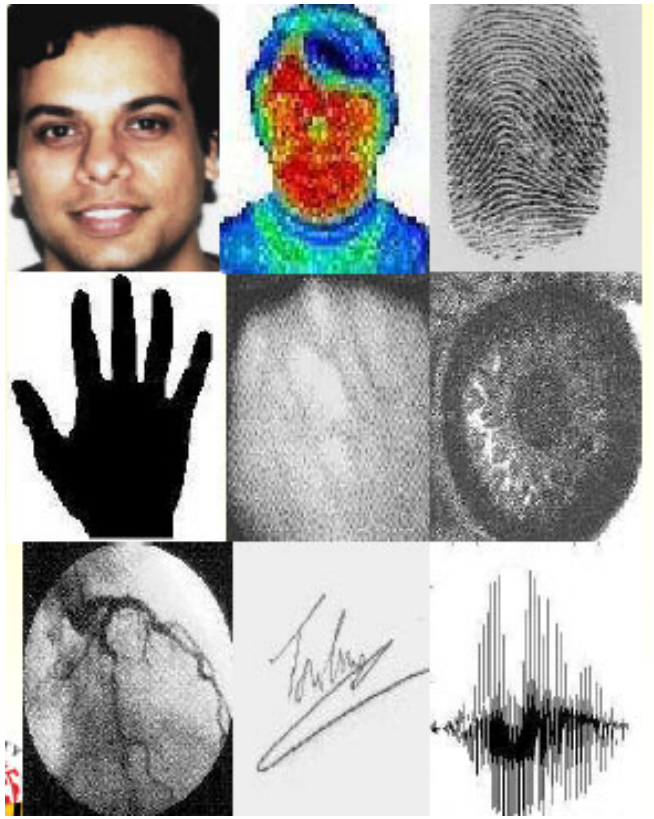
# Biometrics vs Other Authentication Methods

- Artefacts (Keys, Cards)
  - Easily lost
  - Can be retrieved to pass on and revoke authority (car keys)
  - Fairly easily cancellable (change locks)
  - Easy to manage
- Secret Knowledge (PINs, Passwords)
  - Easily lost or forgotten
  - Once disclosed there is no way to retrieve them
  - Easily cancellable (password reset)
  - Simple to manage
- Biometrics
  - Rarely lost or forgotten
  - **Unique to each person**, cannot be transferred (no good for car)
  - Not cancellable in most cases
  - Complicated technology with significant false accepts and rejects

Three Factors
- Something you **have**
- Something you **know**
- Something you **are**

# Types of Biometric Technology

- **Fingerprint**
- **Face**
- **Iris**
- **Voice**
- Hand geometry
- Signature
- Retina
- Thermal
- Vein Patterns



# Terminology

- Enrolment
  - Adding a new person to the biometric collection or **gallery**
- Template
  - The mathematical representation of the biometric used for search and matching purposes. The template is generally much more compact than the raw representation (e.g., image, audio).
- Matching
  - Templates that are very similar to each other according to some distance measure (metric) are said to match
- Accuracy
  - **False reject** rate: Rate at which the true person is not accepted (big problem)
  - **False accept** rate: Rate at which imposters are accepted
- Gallery:
  - The collection of enrolled persons. Gallery size and makeup is important.
- Probe
  - The query image or template for matching

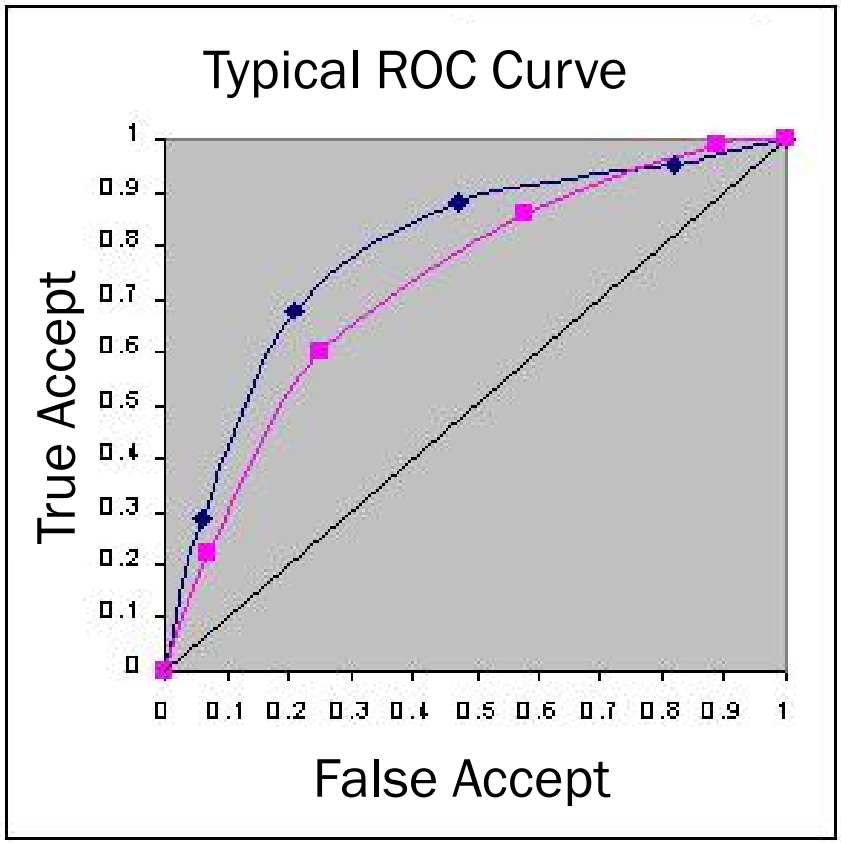
# Terminology

- Cooperative
  - Person knows about the biometric examination
- Non-cooperative
  - Person does not know the biometric is being captured
- Detectable
  - Person can detect biometric capture equipment
- Undetectable
  - Person cannot detect biometric equipment
    - e.g. due to long range capture
- Cancellable Biometric
  - Reduces risk if template is compromised. Template + encryption or distortion

# Biometric Modes of Operation

- Verification or 1-to-1 matching
  - Is the person who they claim to be?
- Recognition, or 1-to-many matching
  - Who is this person? Are they in the gallery?
- Watch List or 1-to-some matching
  - Is this person on our watch list?
- Closed Set Matching
  - Everyone we encounter is in the gallery
  - Find best match
- Open Set Matching
  - Many people we see are not in the gallery
  - Best match is unlikely to be true identity
  - Need to estimate likelihood that person is in gallery

# Receiver Operating Characteristic (ROC) Curve




True_Accept = 1- False_Reject

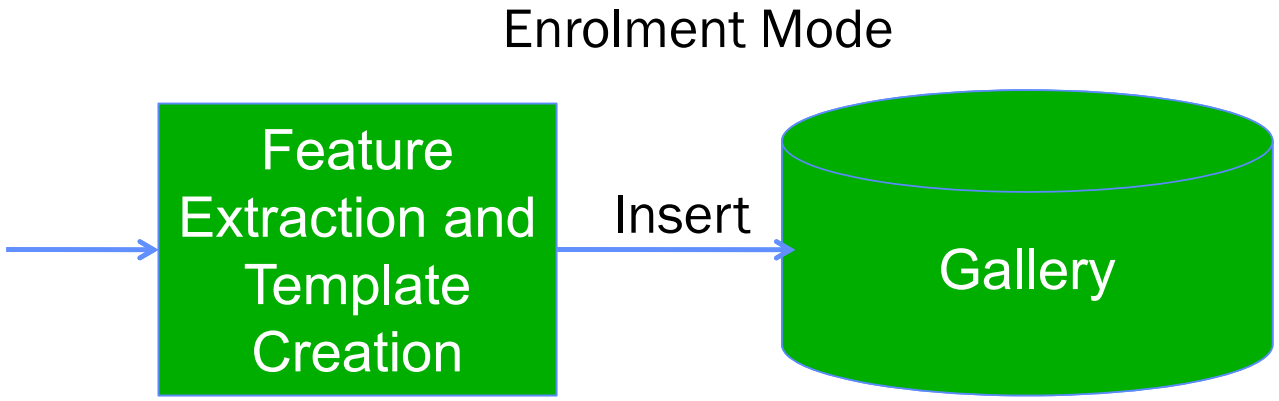
False Accept up -> False Reject down

There is **always** a tradeoff between acceptance and rejection errors

**The moral of the story is that one error can always be improved at the expense of the other**

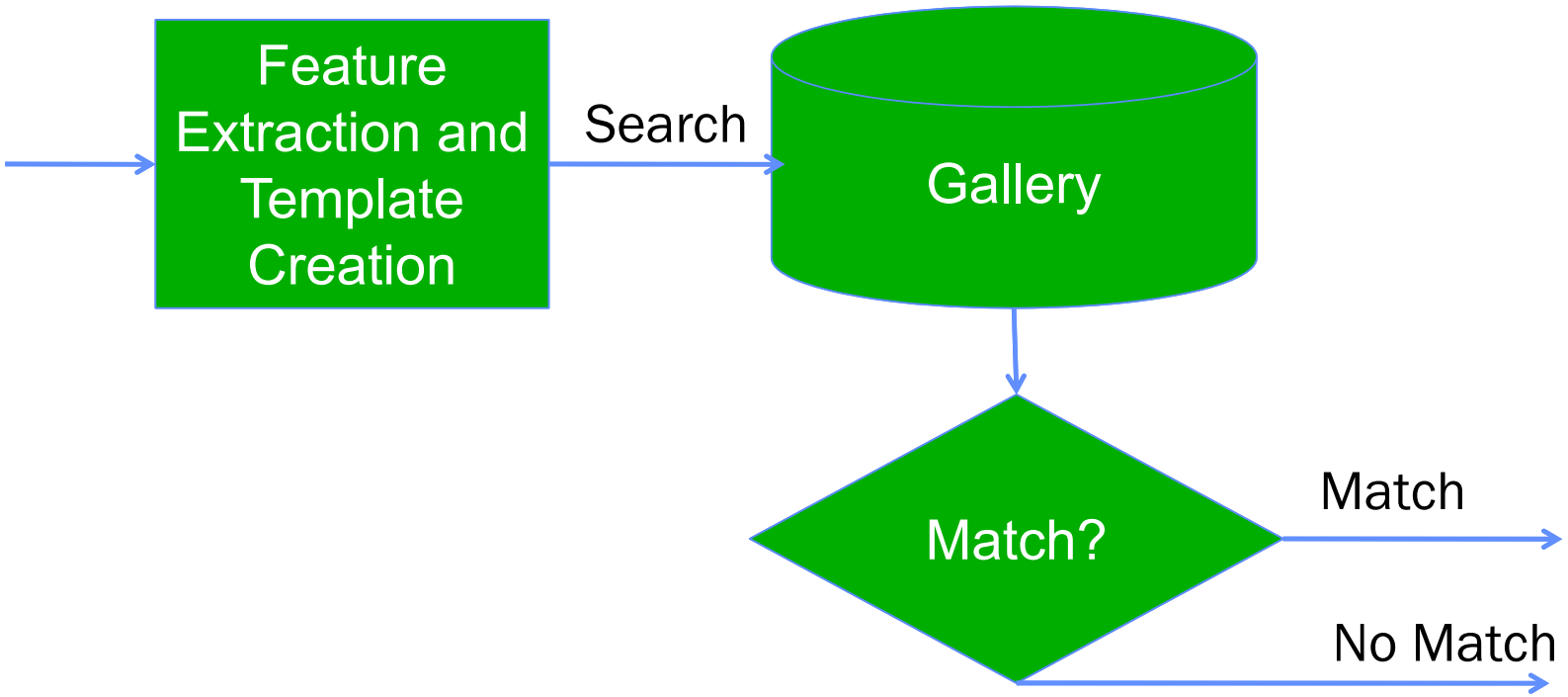
Typically fix FRR at 0.1% and report FAR

# How Biometrics Work



# How Biometrics Work

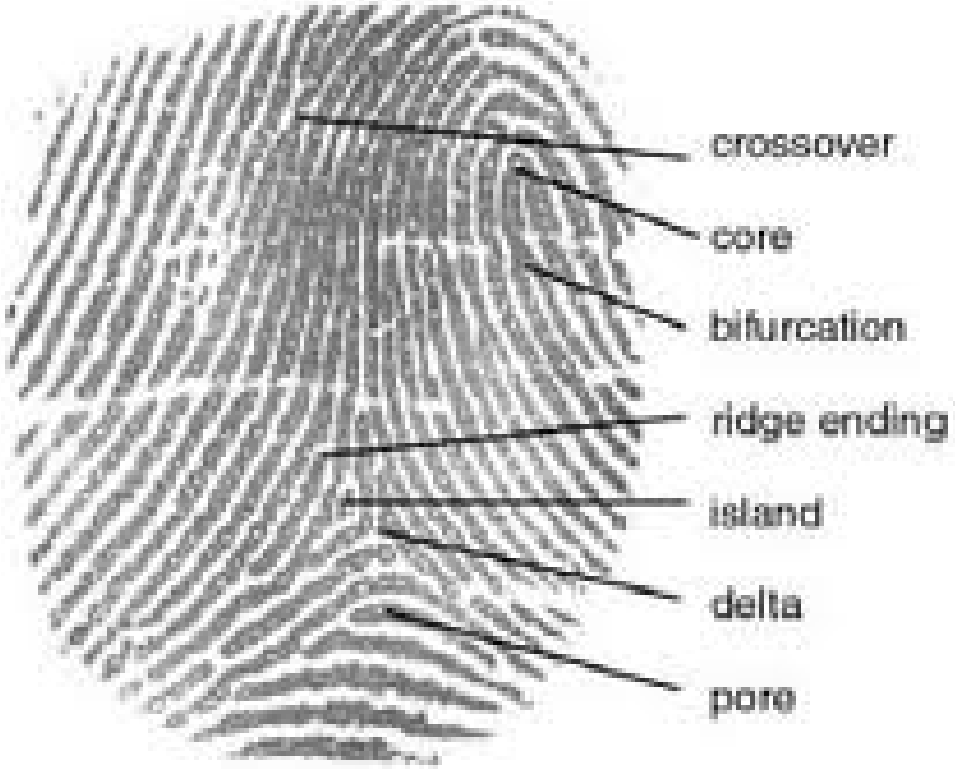
Verification/Recognition Mode



# Fingerprint Recognition

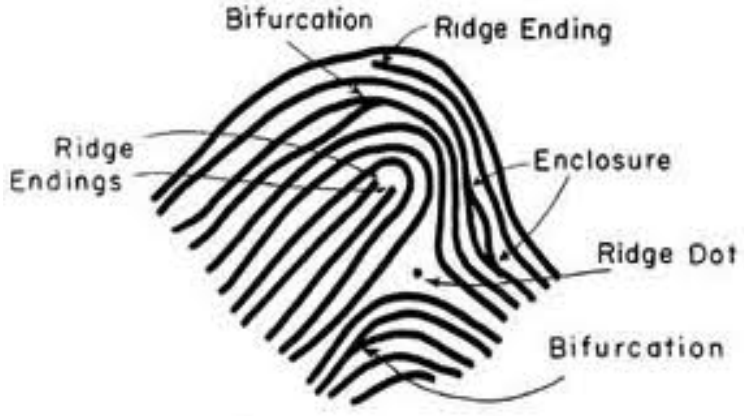
- Well-developed technology with good forensic accuracy
- Contact-based technology
- Hygiene issues for mass transport usage
- Slow enrolment but fairly fast recognition
- Unsuitable for about 3% of the population (weak fingerprint ridges)
- Can tell twins apart –fingerprint and iris are not DNA coded
- Mostly cooperative and very detectable

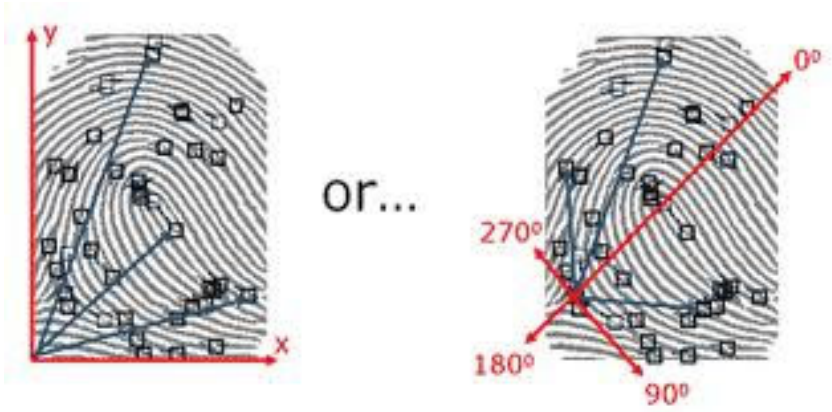
# Fingerprint Recognition





# Principle of Operation



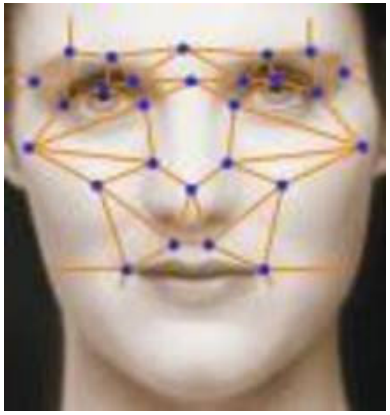

Match 7 to 10 minutiae points by aligning prints. The more matches, the more accurate the fingerprint match.

Can use all fingers and thumbs to improve match.

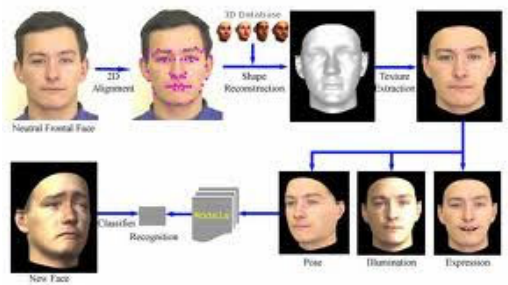
# Face Recognition

- Often needs a **face detection** stage before recognition
- Good performance generally requires controlled image capture conditions
- Can work over the internet (social networks)
- Passport quality verification works quite well (SmartGate)
- CCTV, uncooperative, and low-resolution recognition is much harder
- This is the biometric that humans use everyday, so untrained people can verify automated result. Thus there can be a low cost for false alarms, if implemented well
- Can be problems with large galleries and twins
- Easy to collect from a large distance with telephoto lenses
- Can be uncooperative and undetectable

# Principles of Operation

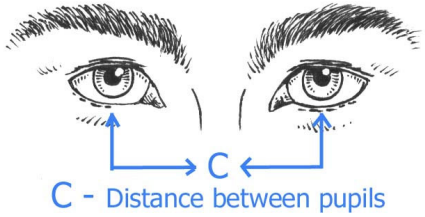


Elastic Bunch Graphs



Pose Compensation

PCA or Eigenface




**Huge** variety of methods

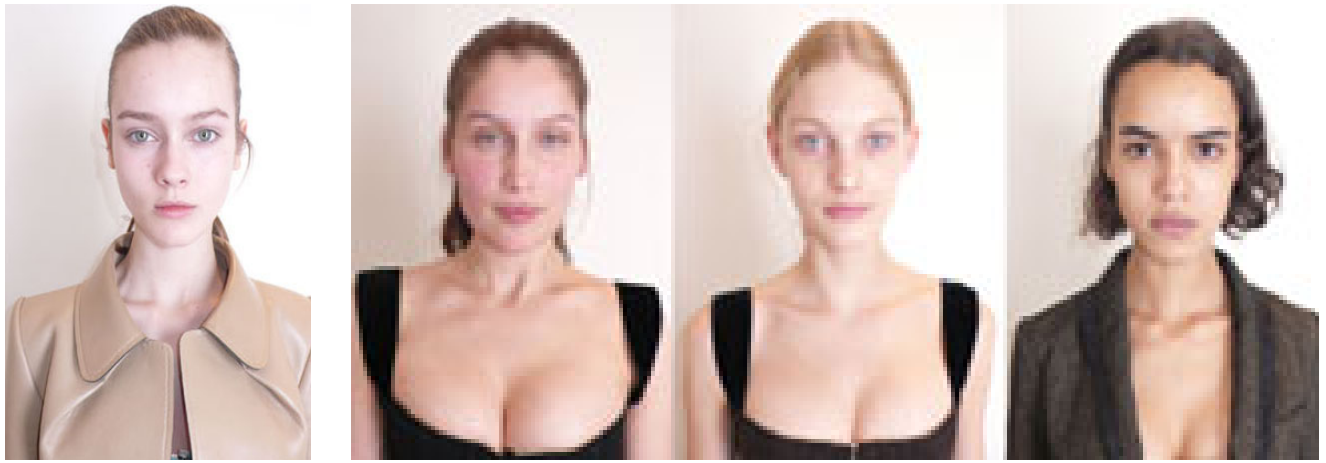
Very complicated due to pose, illumination, and expression compensation

Aim is to extract mathematical features which match identity. No physical measurements of face are generally used!

Holy grail of biometrics, but generally considered to be unreliable compared to iris and fingerprint

# Problem: Matching unfamiliar faces

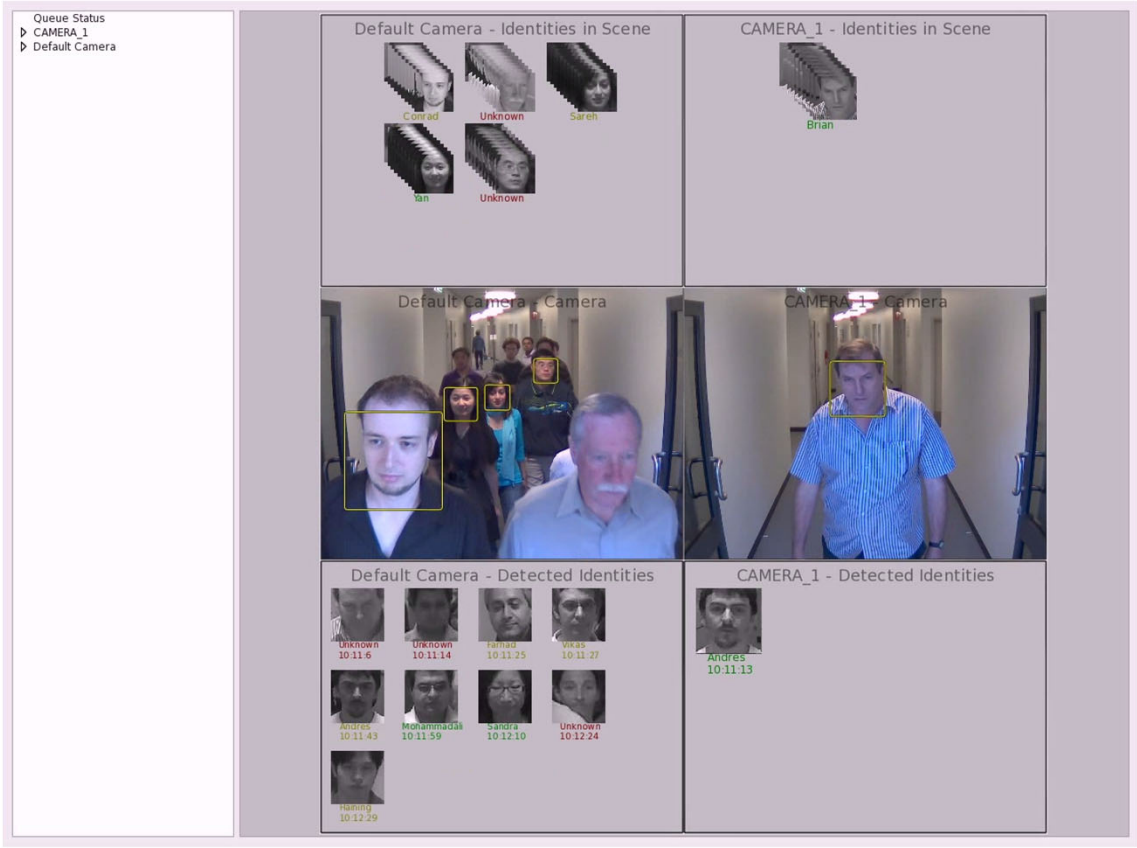
# is not as easy as it sounds



# Facial Feature Detection for Alignment

IEEE Trans. Image Processing, Nov. 2002. Moon, Chellappa and Rosenfeld

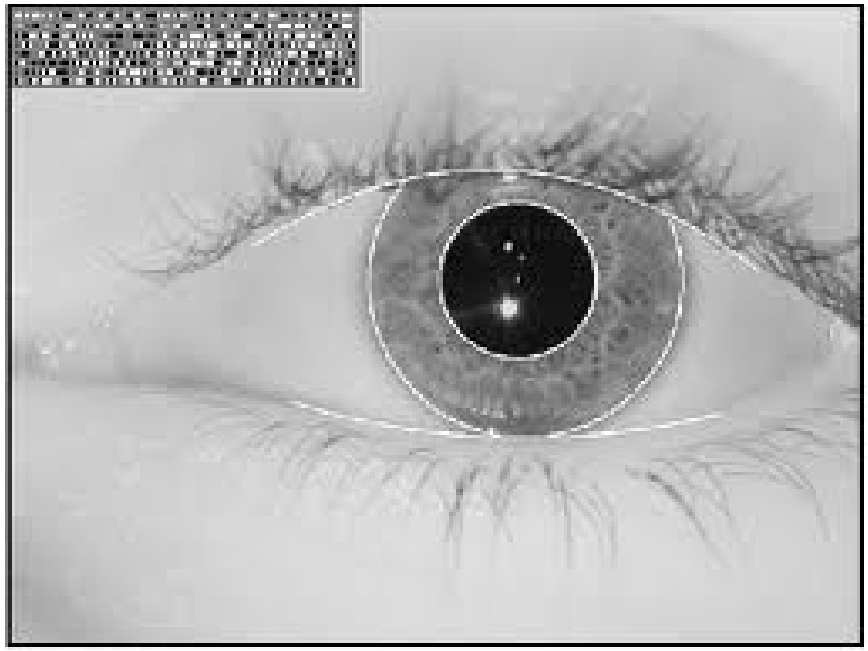
# Video: CCTV Face Search in Operation



# Iris Recognition

- Often considered to be the most accurate biometric technology
- Very low false accept (alarm) rates
- New technologies such as **iris in motion** allow collection from up to 1m (40”) standoff. Can process up to 50 persons per minute.
- Can tell twins apart
- Can be uncooperative though usually detectable

# Principle of Operation



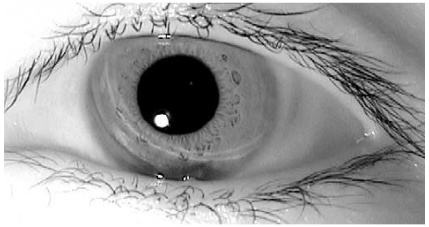
Produces mathematical code from texture of the iris under near infrared illumination

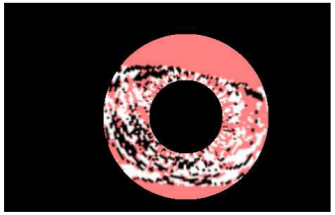
Can match both left and right eyes

Very good recognition performance

# Summary of Iris in Motion

- For
  - Very reliable and fast recognition performance
  - Touch free and continuous operation
  - No need to remove glasses
  - Works in a variety of lighting conditions
  - Enrolment on the move
- Against
  - Requires new infrastructure in addition to CCTV
  - Identity based on iris unable to be verified by human
  - Can have problems with contact lenses including possibility of identity fraud via printed lenses
  - Collection of yet another biometric database (iris)





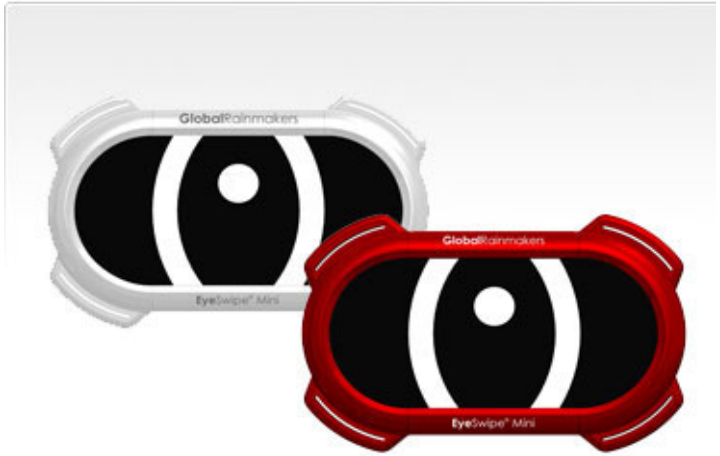
- May be overcome by combining with cctv face technology

# Fusion of Face and Iris in Motion

Iris in Motion technology as developed for the CIA

Winner of 2009 Frost & Sullivan Best Practice Award


Very reliable and fast (50 per minute) recognition of people. Fuse with uncooperative face recognition for more powerful system.



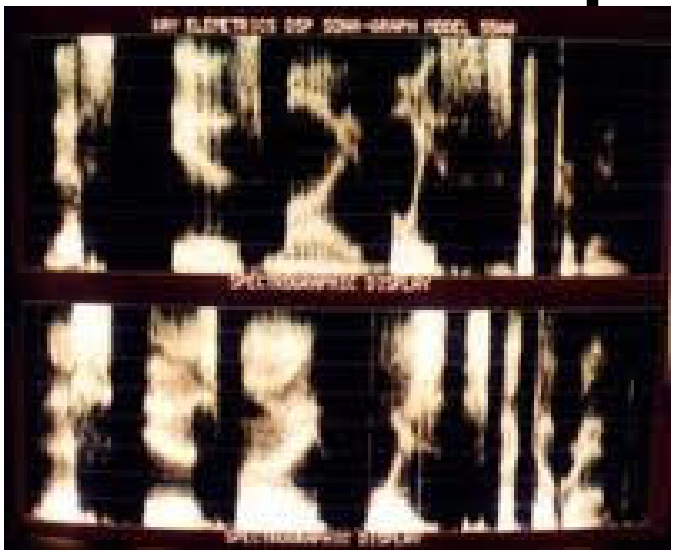

HBOX in NICTA Demo Room

# Video: Iris in Motion in Operation

# Voice Identification

- Low accuracy
- Mostly short distance capture
- Difficult to capture in **noisy public environments**
- Affected by common colds and flu
- Probably least suitable for border control
- Better suited to investigation
- Can be uncooperative and undetectable

# Principle of Operation



Perform frequency analysis of voice to determine resonances of head cavities which indicate identity

Fairly unreliable

Mostly used for verification rather then recognition

# Typical Applications

- Face
  - border control, investigative, drivers licences, Smartgate
- Iris
  - border control, forensic (horse ID, labour control)
- Fingerprint
  - USA border control, forensic
- Voice
  - Investigative, telephone intercepts

# Implementation Issues

- Accuracy
- Recognition performance on large galleries
  - Performance always drops with gallery size
- Performance against demographics
  - (HP face recognition accused of racism)
- Control of capture environment
  - Face: Pose, illumination, expression, glasses etc
  - Iris: Pose, eye blink, gaze angle
  - Fingerprint: correct print technique
  - Voice: background noise, quality of channel
- Can result be verified by human operator?
  - Ok for Face, not for others

# Implementation Issues

- Attended vs unattended mode
  - All can operate in unattended mode to some extent
- Language and Cultural Considerations
  - Face is difficult to capture for women in Islamic Countries
  - Fingerprint is associated with criminals and has low public acceptance
  - Hygiene is an issue for contact based technologies
- Most systems are used in verification mode
  - In this case false reject rate is the major practical issue
  - Often false accept rate must be unacceptably high to keep false reject levels low defeating a prime aim of biometric technology
  - E.g. Manchester Airport where husband swapped passport with wife

# Cultural and Social Issues

- Fingerprints are associated with criminals
- Face recognition can be difficult with dark skin
- Faces are covered in Islamic societies
- Mass use of biometrics raises security concerns for mass biometric databases –need for cancellable biometrics
- Biometric systems can be fooled
  - Photos of faces, videos of faces
  - Iris contact lenses
  - Fingerprint tape
  - Voice manipulation
- To prevent biometric defeats, may need to run system in attended mode

# Private Sector Trends

- Biometrics such as fingerprint and face used as convenient alternatives to passwords
- Face and fingerprint biometric appearing on mobile devices
- Typically encourage voluntary adoption of biometrics for convenient and fast security checks
- Disneyland uses fingerprints to manage large scale ticketing systems.
- Bank of America deploying iris on the move internally
- Iris used to detect racehorse substitution (Fine Cotton Affair)

# Government Uses of Biometrics

- Border Control
  - Face, Iris, Fingerprint
- Driver's Licence
  - Face Recognition to prevent false licence issuance
  - Australian Digital Licence Project
- Enforcement of Disbarment
  - The United Arab Emirates checks irises of Third Country National labour (mostly Indian and Pakistani) to enforce disbarment at the borders

# Questions