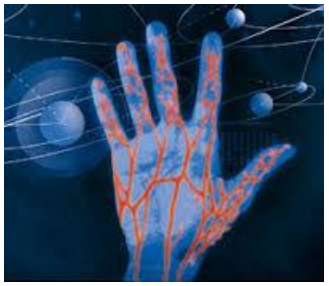
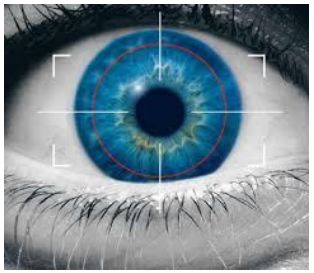
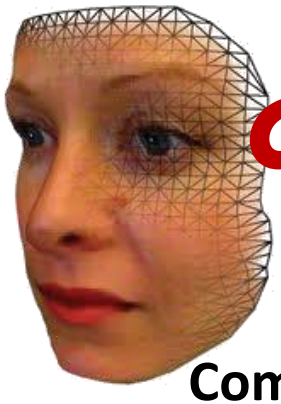




Biometrics – *Our Past, Present, and Future Identity*



Syed Abd Rahman Al-Attas, Ph.D.

Associate Professor

Computer Vision, Video, and Image Processing Research Lab

Faculty of Electrical Engineering,

Universiti Teknologi Malaysia

Outline

- General Information on Biometrics
- Why Biometrics
- Market Trends
- How it works
- Examples of Biometrics Modalities
- Standards
- Concluding Remarks

What is Biometric

- Biometric literally means life measurement.
- Measurement of an individual for either:
  - Identification – who you are (one to many)

  - Authentication (Verification) – you are who you are (one to one).

What is Biometric

- Biometric is the key.

- Biometric System is the lock

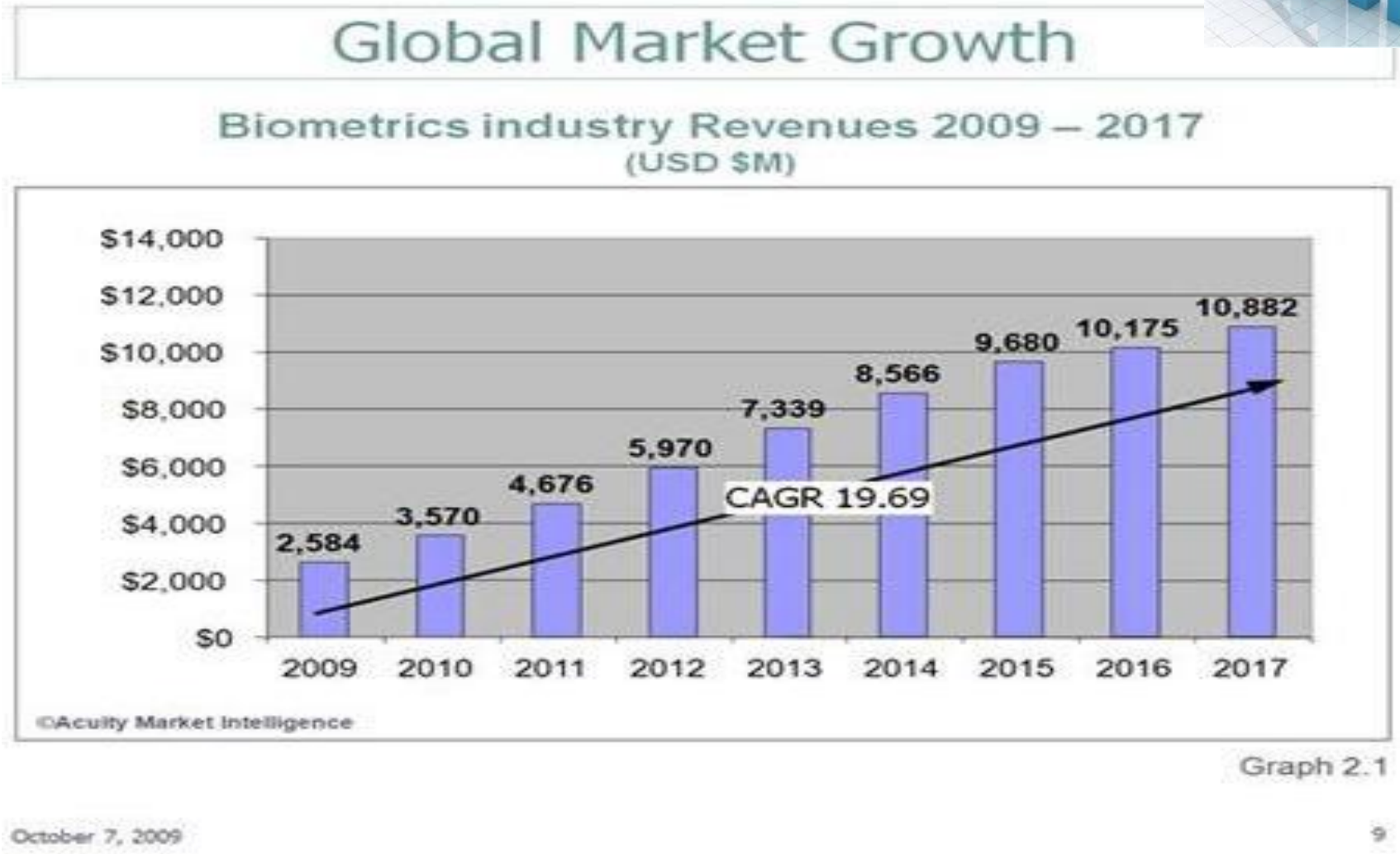
Types of Biometrics

Physiological	Behavioral
• Fingerprint • Face • Iris • DNA • Finger Vein • Palm Print • Hand Geometry	• Voice • Signature • Typing Rhythm • Gait

Why Biometrics

- Harder to fake unlike identity cards or passports.
- Can’t be guessed unlike a password
- Can’t be misplaced/loss unlike an access card or ID cards.
- Can’t be forgotten unlike password

Market Trend



http://fingerchip.pagesperso-orange.fr/biometrics/applications.htm

Market Trend

USD 23.3 Billion by 2019

- 2013 – 2019
- Transparency Market Research

USD 23.54 Billion by 2020

- 201 4 – 2020
- Markets and Markets

Market Trend

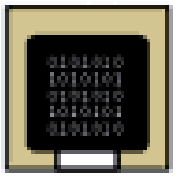
BIOMETRICS MARKET BREAKDOWN

FINGERPRINT
FOR AUTHENTIFICATION
2003 $198 MILLION
2008 $1,493 MILLION

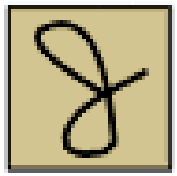
IRIS
2003 $36 MILLION
2008 $366 MILLION

VOICE
2003 $23 MILLION
2008 $225 MILLION

FACE
2003 $50 MILLION
2008 $802 MILLION

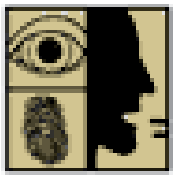


MIDDLEWARE
2003 $48 MILLION
2008 $397 MILLION

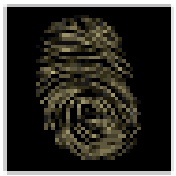


SIGNATURE
2003 $9 MILLION
2008 $107 MILLION

HAND GEOMETRY
2003 $43 MILLION
2008 $154 MILLION



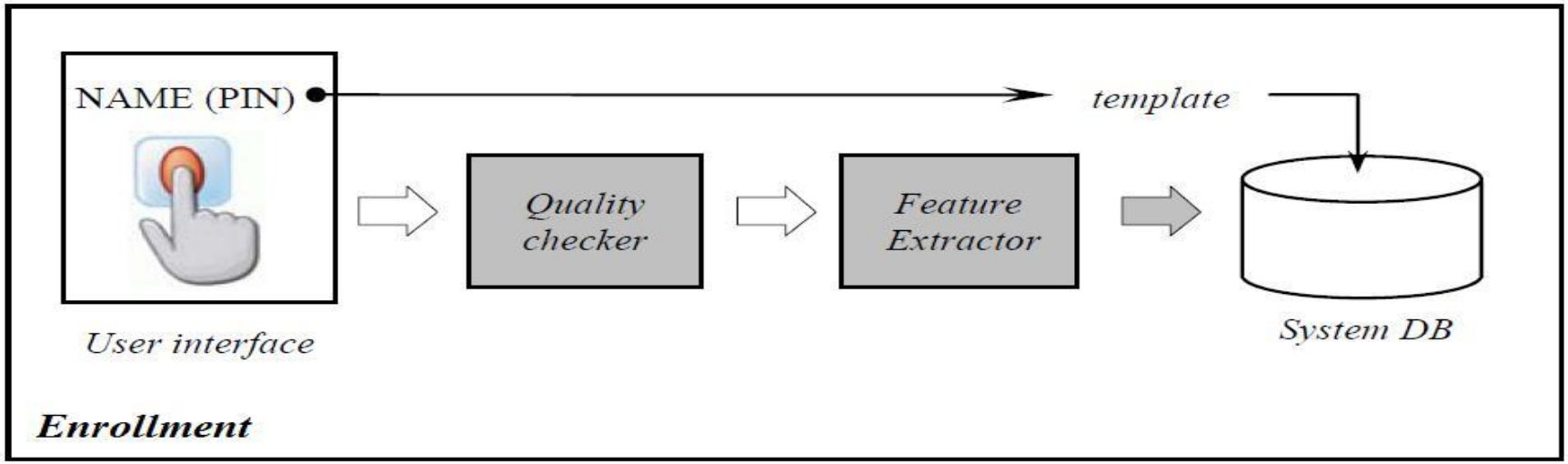
MULTIMODAL
2003 $11 MILLION
2008 $220 MILLION



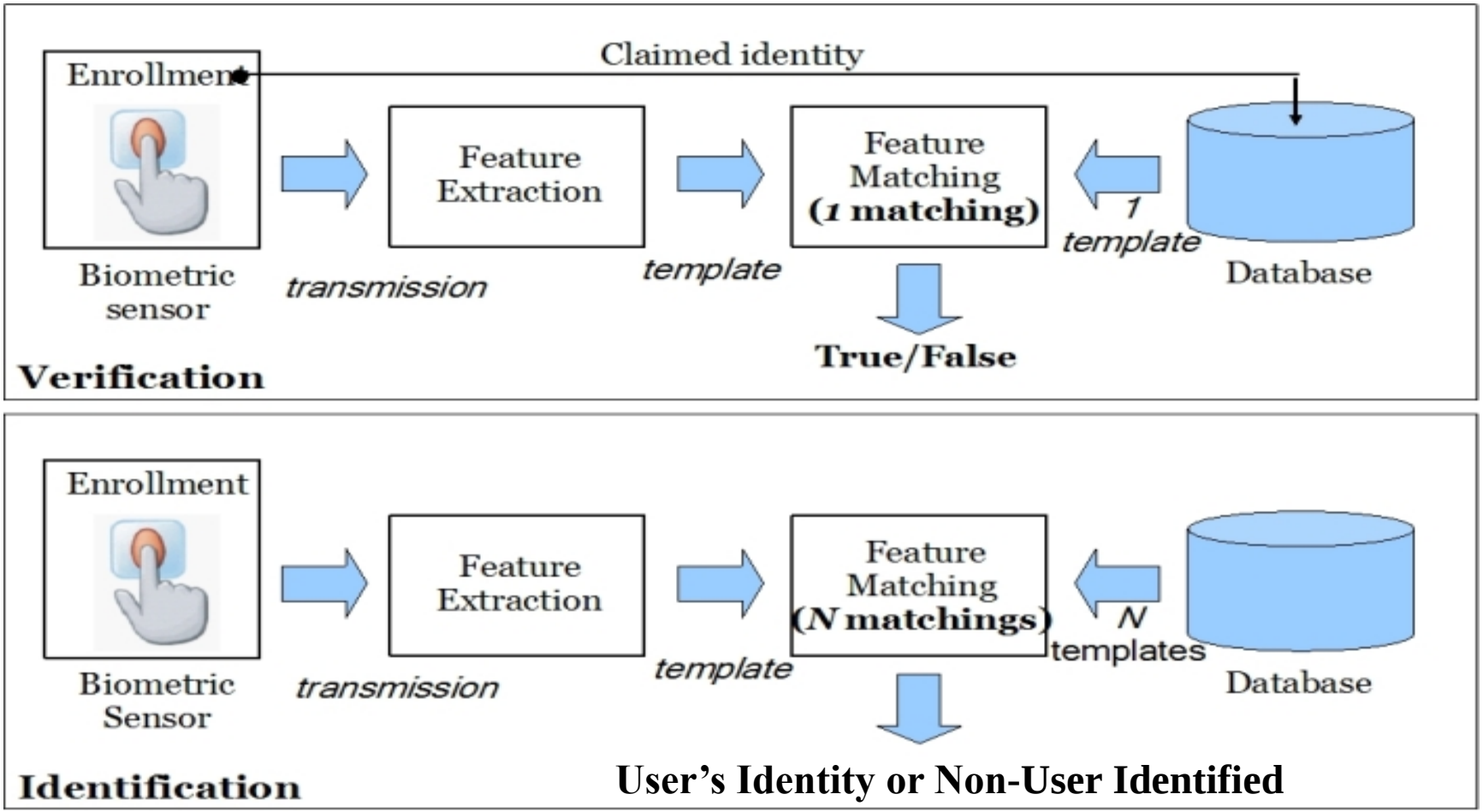
FINGERPRINT
FOR CIVIL/CRIMINAL ID
2003 $312 MILLION
2008 $1,095 MILLION

http://www.prism-magazine.org/oct04/briefings.htm

How Biometric Works



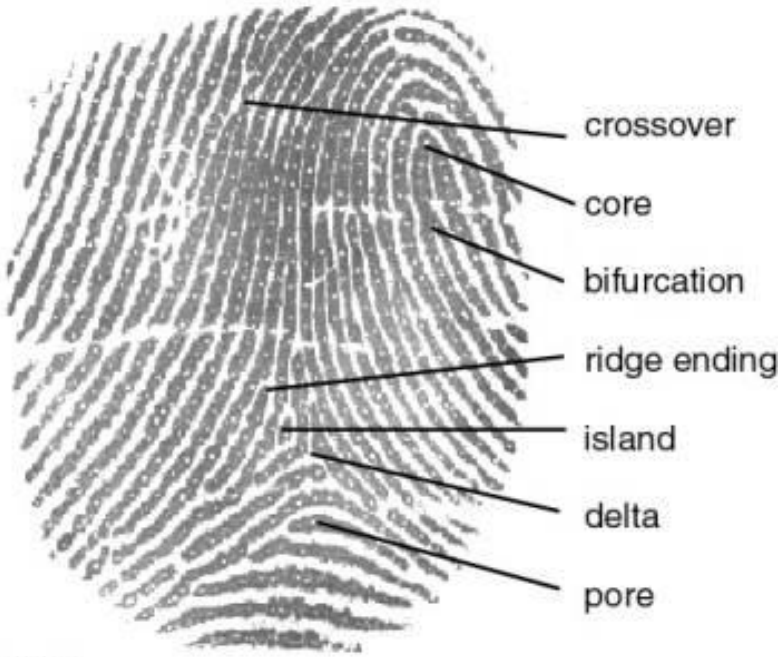
How Biometric Works



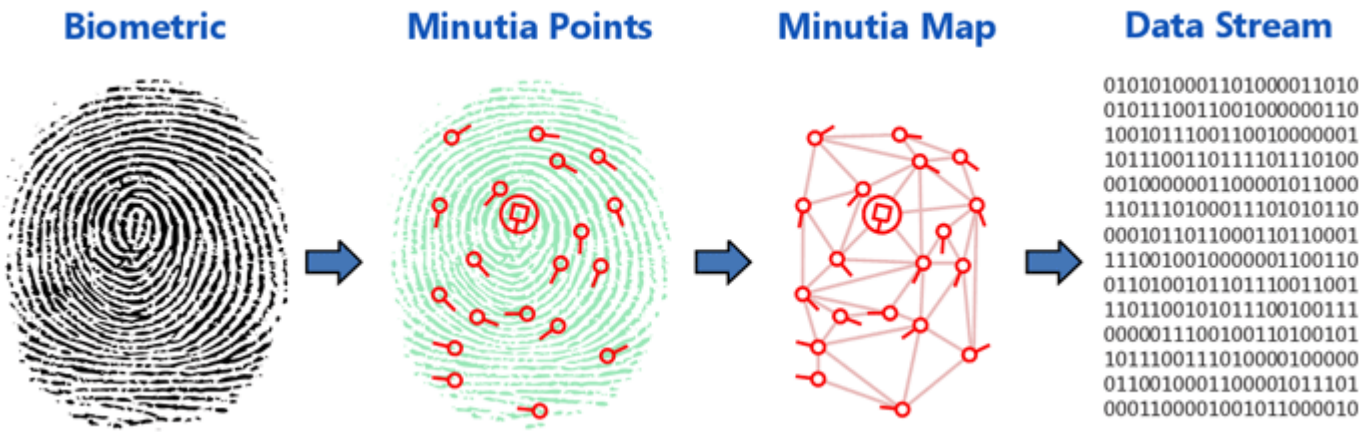
Fingerprint

- Most widely used
- Very established
- Matching techniques
  - Minutiae-based – most popular
  - Correlation-based – eg. Phase information
  - Graph-based – based on minutiae topology

Fingerprint



Fingerprint



Fingerprint

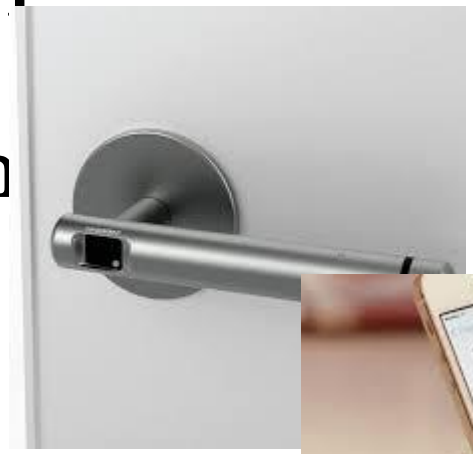
- Types of Sensors
  - Optical sensors with CCD or CMOS cameras
  - Ultrasonic sensors – not common, big size, deer
  - Solid state temperature sensors
  - Solid state capacitive sensors - smartphone
  - RF sensors (Latest)
- Types of Reader/Sensing
  - Static fingerprint reader
  - Swipe fingerprint reader

Fingerprint

- Thanks to the smartphone industries
  - 2013 first smartphone shipped with fingerprint scanner (Iphone 5s) followed by Samsung S5
- In 2020 the market will be $14.35 billion

Fingerprint

- Current Application
  - Entry Access
  - Device Access
  - Security
  - Control Access

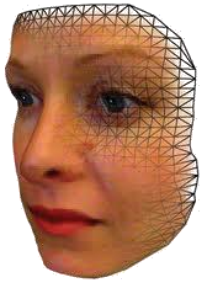


Fingerprint

- Advantages
  - Very high accuracy.
  - Is the most economical biometric PC user authentication technique.
  - It is one of the most developed biometrics
  - Easy to use.
  - Small storage space required for the biometric template, reducing the size of the database memory required
  - It is standardized.

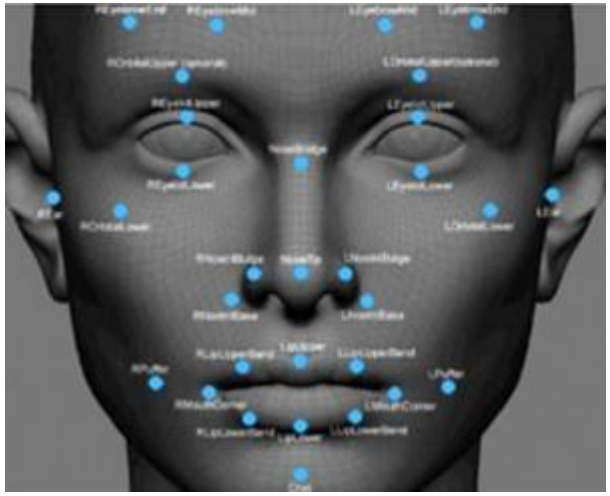
Fingerprint

- Disadvantages
  - Very intrusive to some people - related to criminal identification.
  - Error prone for dry or dirty finger skin.
  - Aging effect - not appropriate with children..
  - Large memory for higher resolution. For a 500 dpi fingerprint image at 8 bits per pixel requires approximately 240 Kbytes → Compression required (a factor of 10 approximately).



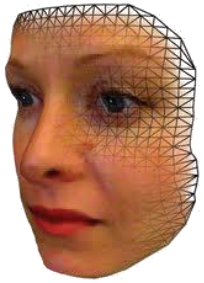
Face

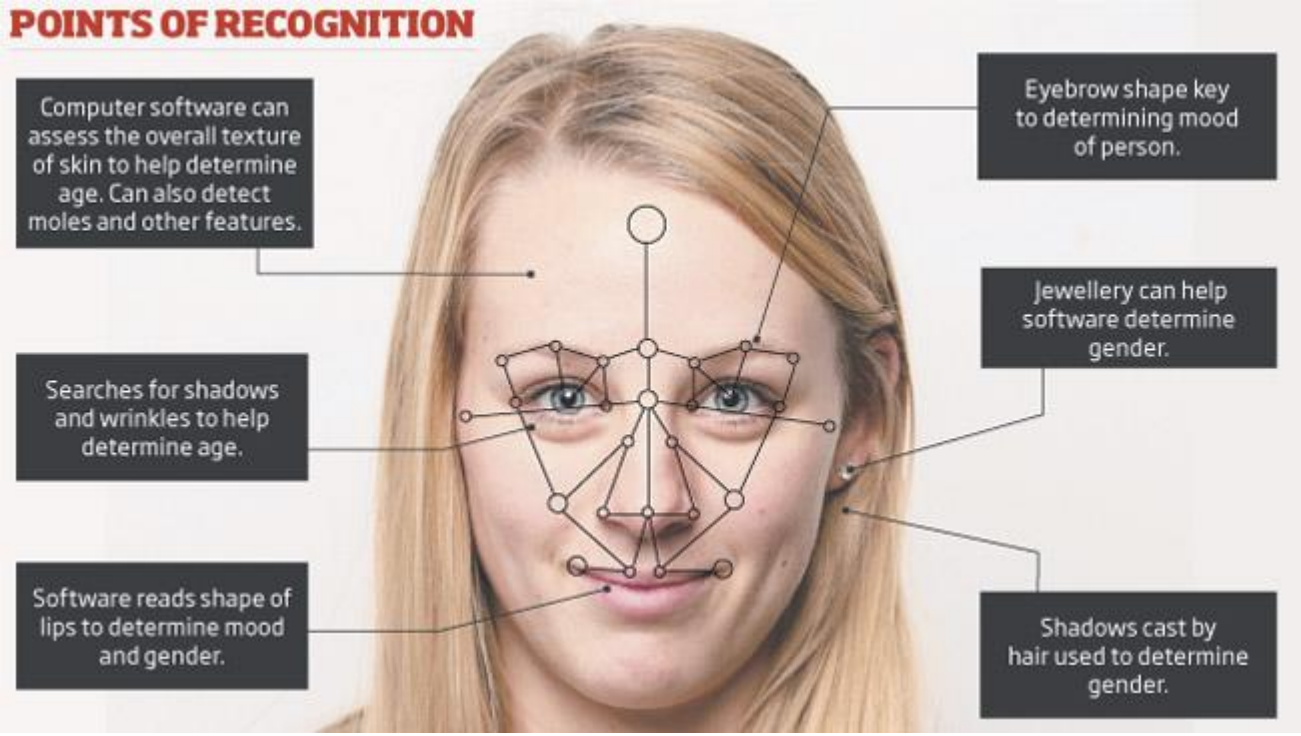
- Based on some facial features or landmarks known as nodal points
- Each face has about 80 nodal points – some of them
  - Distance between the eyes
  - Width of the nose
  - Depth of the eye sockets
  - The shape of the cheekbones
  - The length of the jaw line



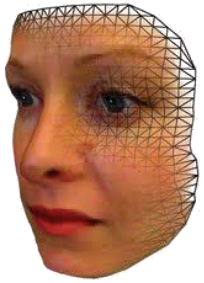
- These nodal points will create a numerical code called faceprint and stored in the database.

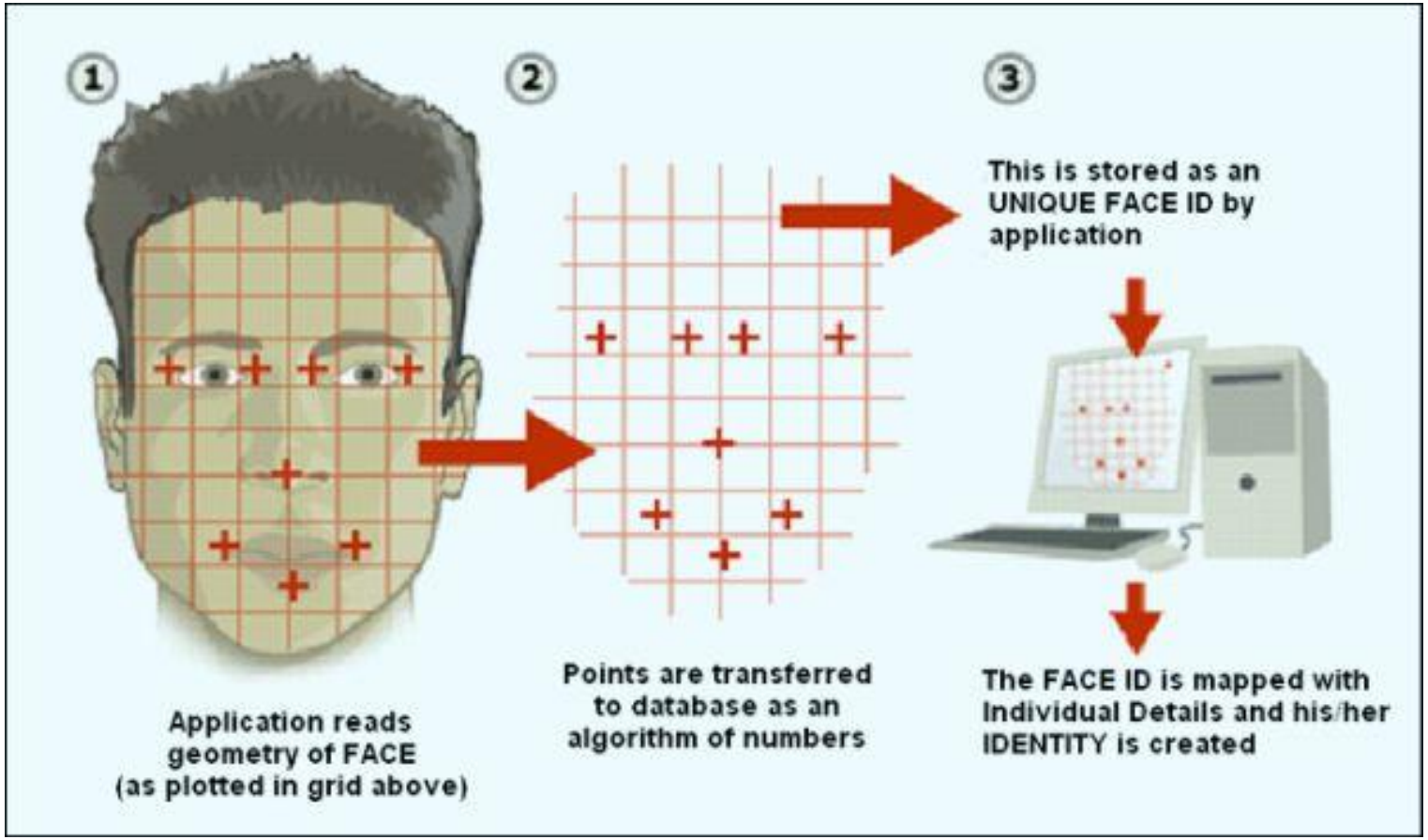
Face




POINTS OF RECOGNITION
Computer software can assess the overall texture of skin to help determine age. Can also detect moles and other features.
Searches for shadows and wrinkles to help determine age.
Software reads shape of lips to determine mood and gender.
Eyebrow shape key to determining mood of person.
Jewellery can help software determine gender.
Shadows cast by hair used to determine gender.

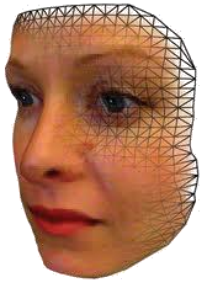
Face





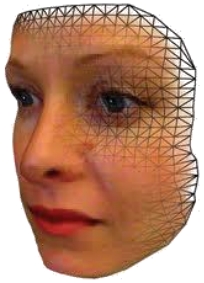
http://atmega32-avr.com/how-facial-recognition-systems-work/

Face



- New technology
  - 3D face scanner
  - Biometric face recognition – surface skin texture
- Problems
  - Significant glare on eyeglasses
  - Hair obscuring central part of the face
  - Poor lighting that causes the face to be over- or under-exposed
  - Lack of resolution (face too far from camera)
  - Head pose, illumination, facial expression, cosmetic
  - Still low accuracy for in the wild environment.

Face

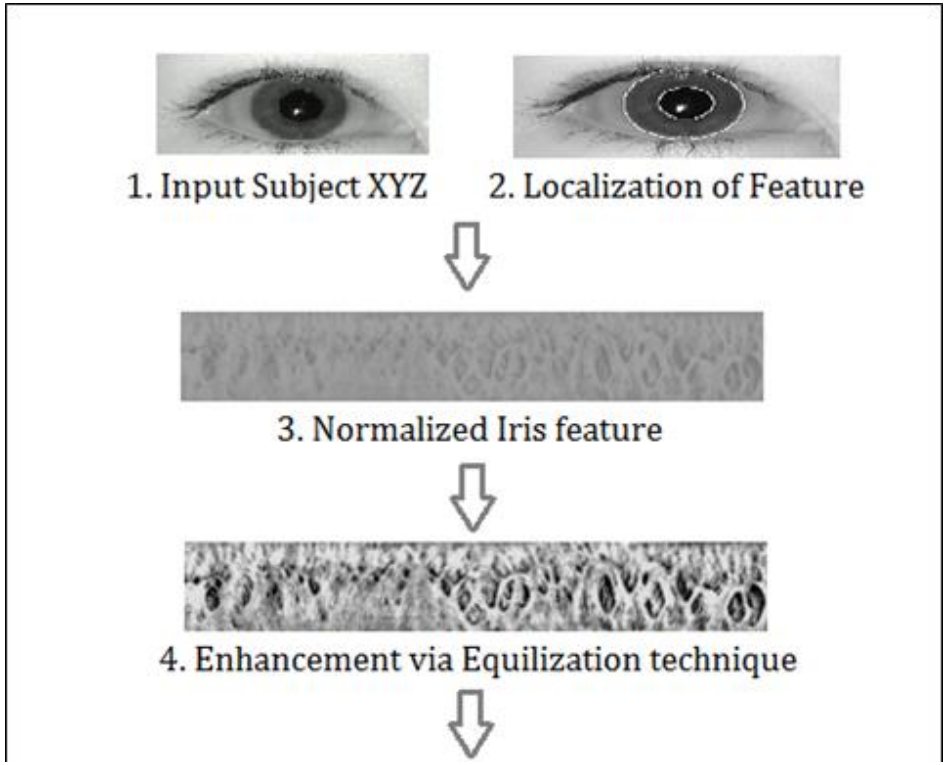


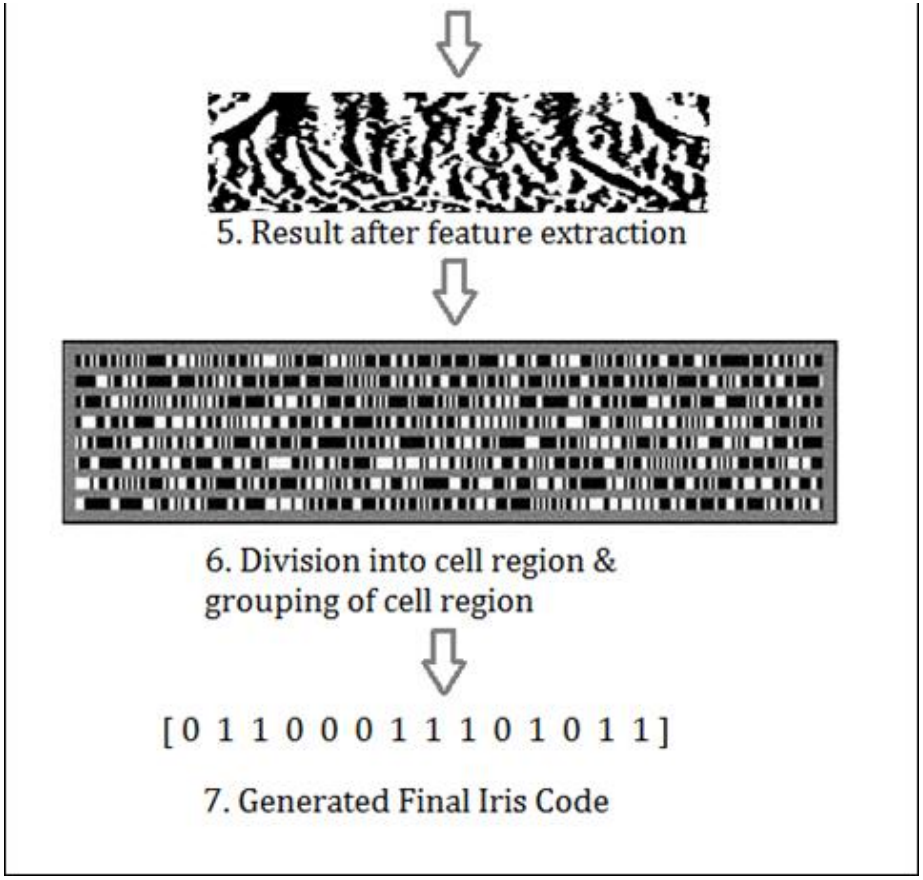
- Users
  - Law Enforcment
  - Custom & Immigration

Iris

- Not a retinal scan
- Relatively new technology
- Fast response
- Based on “Iris Code” – collected from at least 200 points – rings, furrow, freckles, corona etc

Iris

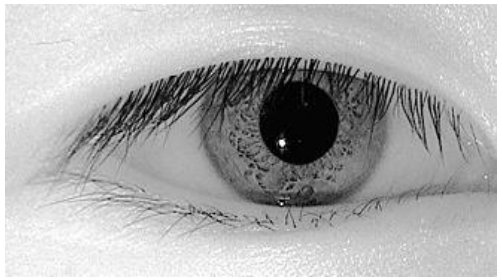




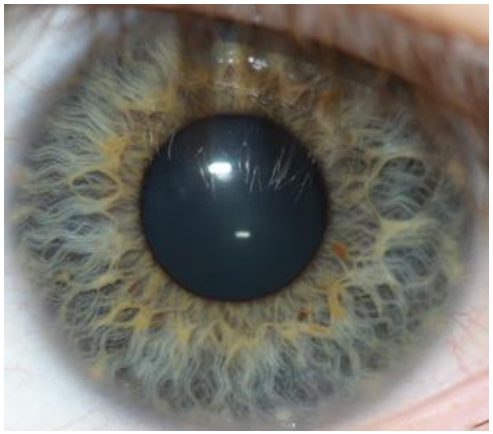
http://resources.infosecinstitute.com/notes-biometric-template-security/

Iris

- Scanners
  - Near Infrared wavelength – dark brown eyes



  - Visible wavelength



Iris

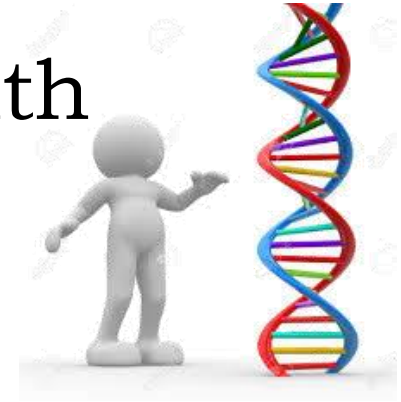
- Currently more expensive than other biometric scanning systems.
- Mainly used at some European airports for frequent travelers, and UAE

Iris

- Advantages
  - Stable - remains unchanged throughout one's lifetime
  - Unique - the probability of two rises producing the same code is nearly impossible
  - Flexible - easily integrates into existing security systems or operates as a standalone
  - Reliable - not susceptible to theft, loss or compromise
  - Non-Invasive - non-contact and quick, offering excellence accuracy from distances as far as 3" to 10"

DNA

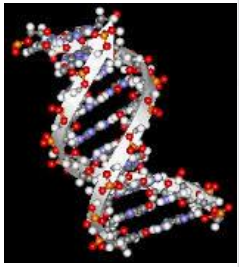
- DNA - Deoxyribonucleic acid with double helix shape



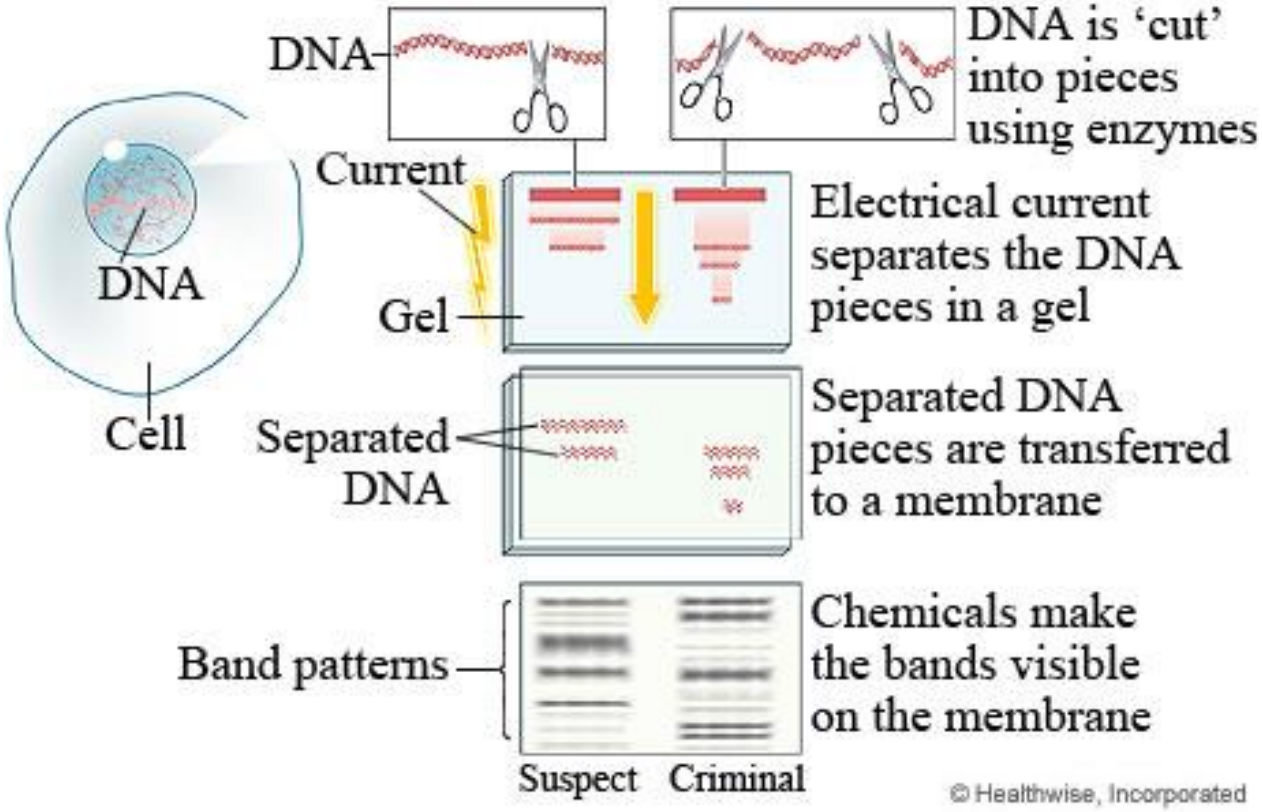
- Very unique – impossible to fake (actually 99.9% similar, only 0.1% is different.

- Longer processing time with intricate procedures

DNA



- DNA Fingerprinting process



DNA

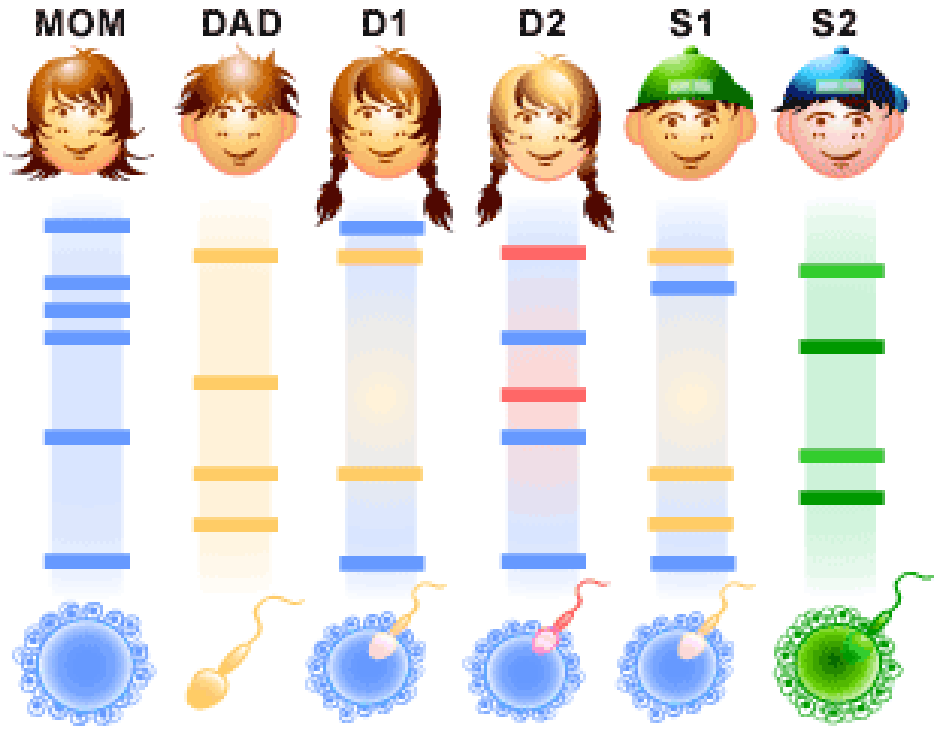
- Mainly used to
  - Find out who a person's parent or siblings are – family tree.

  - Solve crimes in finding the criminal

  - Identify a body especially if badly decomposed

DNA

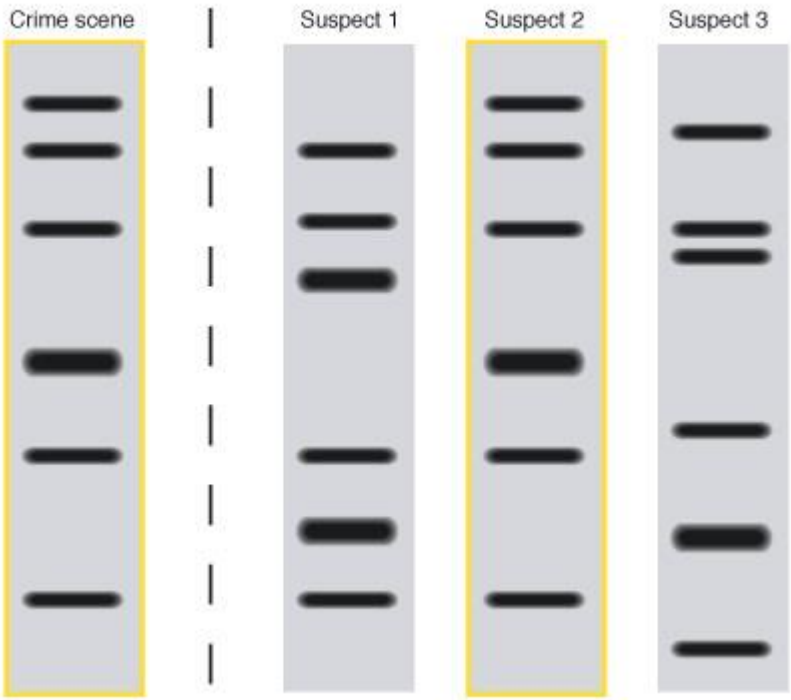
- Parent/Sibling Matching



http://www.scq.ubc.ca/a-brief-tour-of-dna-fingerprinting/

DNA

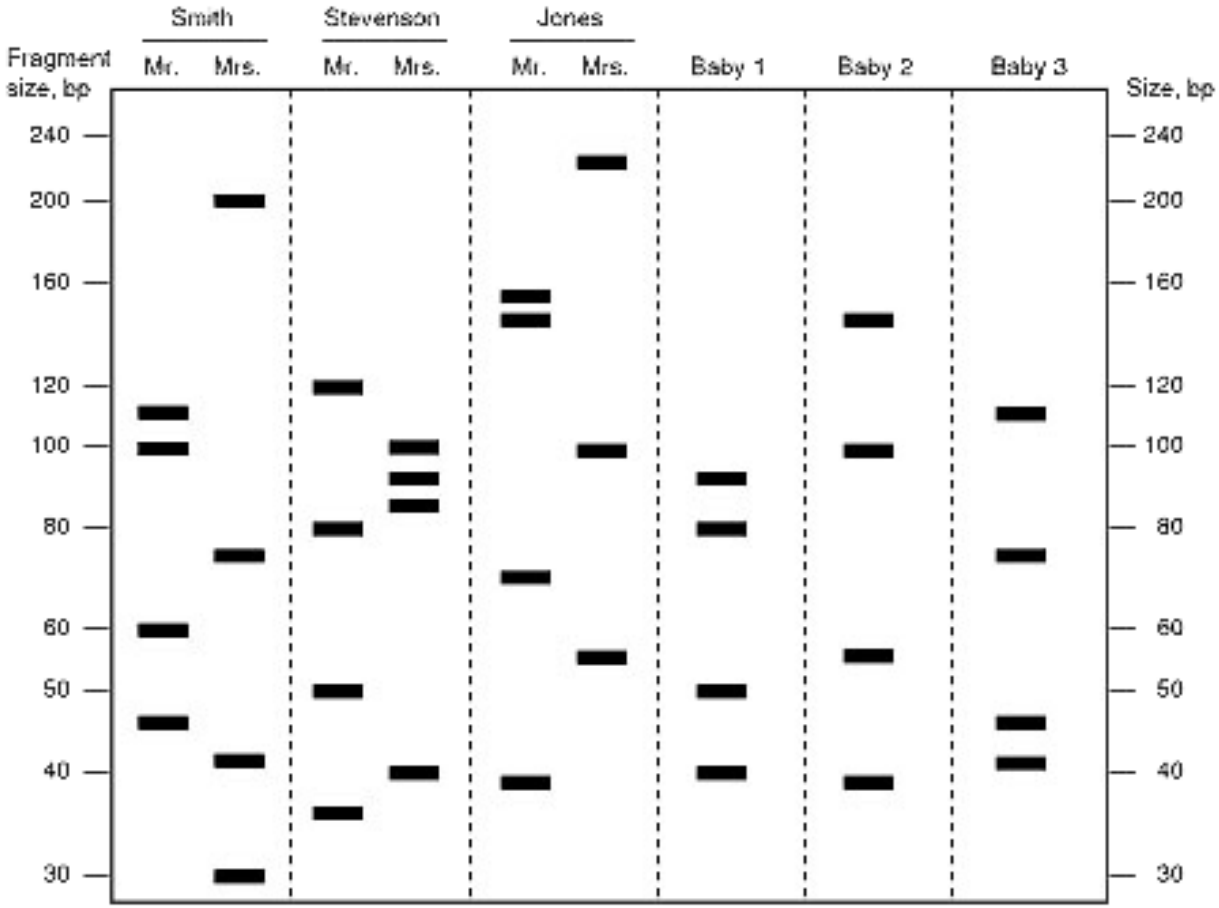
- Criminal Search



http://geneed.nlm.nih.gov

DNA

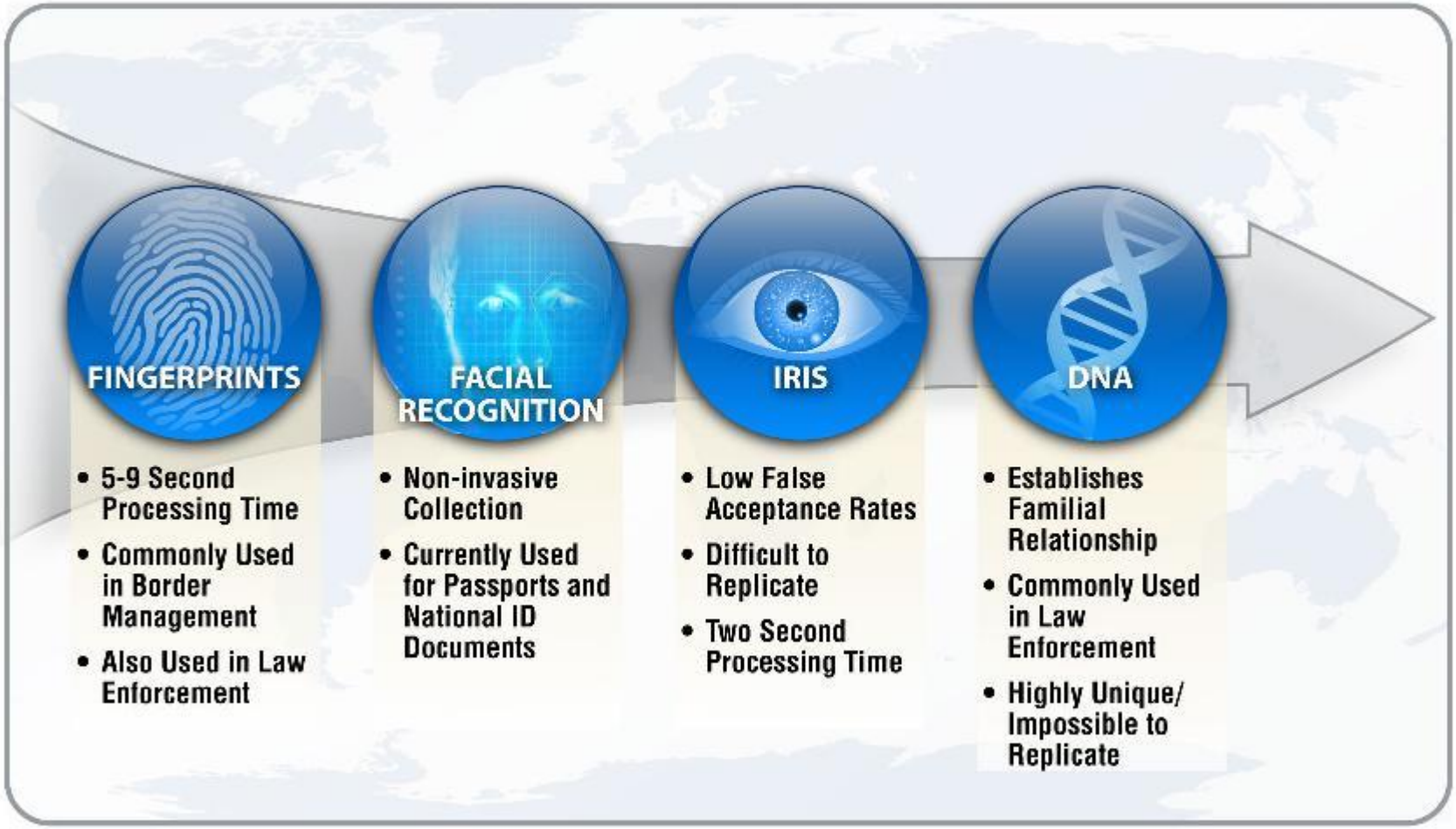
- Who's baby?



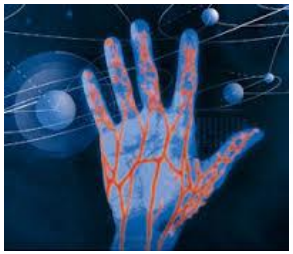
DNA

- Limitations
  - Possibility of incorrect results due to errors such as cross-contamination of samples.
  - DNA profiles can only offer statistical probability (for example, one in a million), rather than absolute certainty.
  - DNA evidence is easily planted at a crime scene.

Comparison

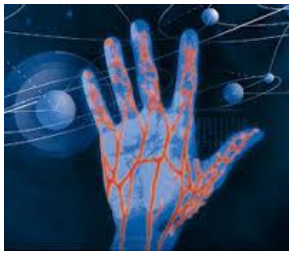

FINGERPRINTS
• 5-9 Second Processing Time
• Commonly Used in Border Management
• Also Used in Law Enforcement
FACIAL RECOGNITION
• Non-invasive Collection
• Currently Used for Passports and National ID Documents
IRIS
• Low False Acceptance Rates
• Difficult to Replicate
• Two Second Processing Time
DNA
• Establishes Familial Relationship
• Commonly Used in Law Enforcement
• Highly Unique/ Impossible to Replicate

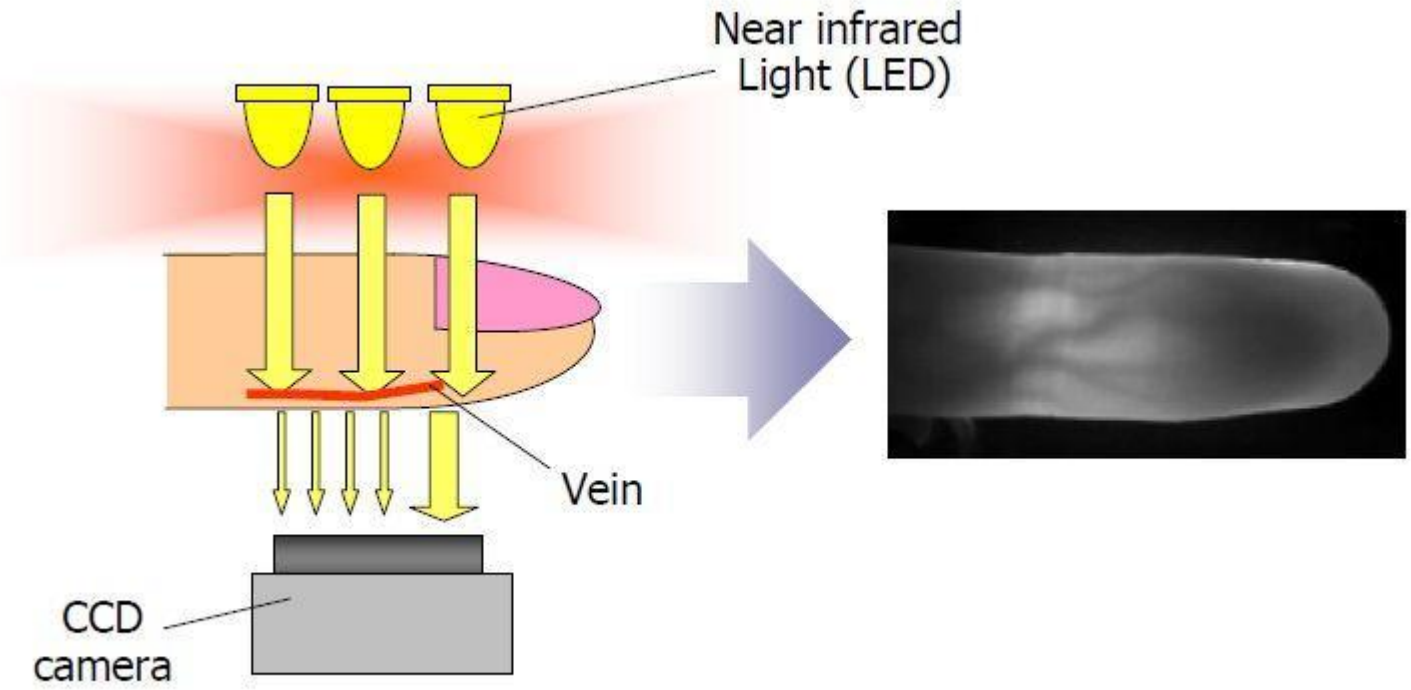
Finger Vein

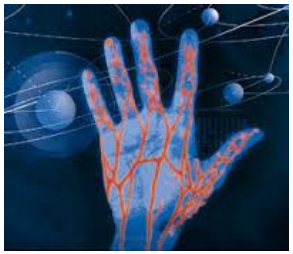


- Exploit the hidden structure of vein pattern or vein network.
- Either from one finger or entire palm

Finger Vein

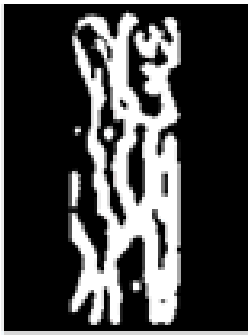




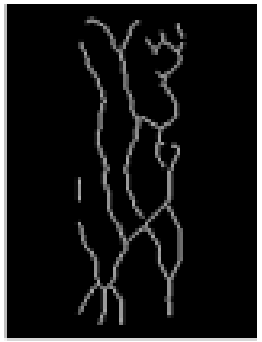


Finger Vein

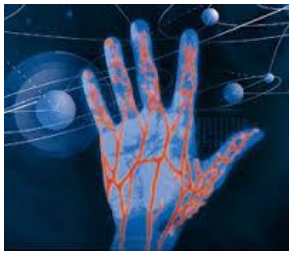
Vein image



Feature Point extraction

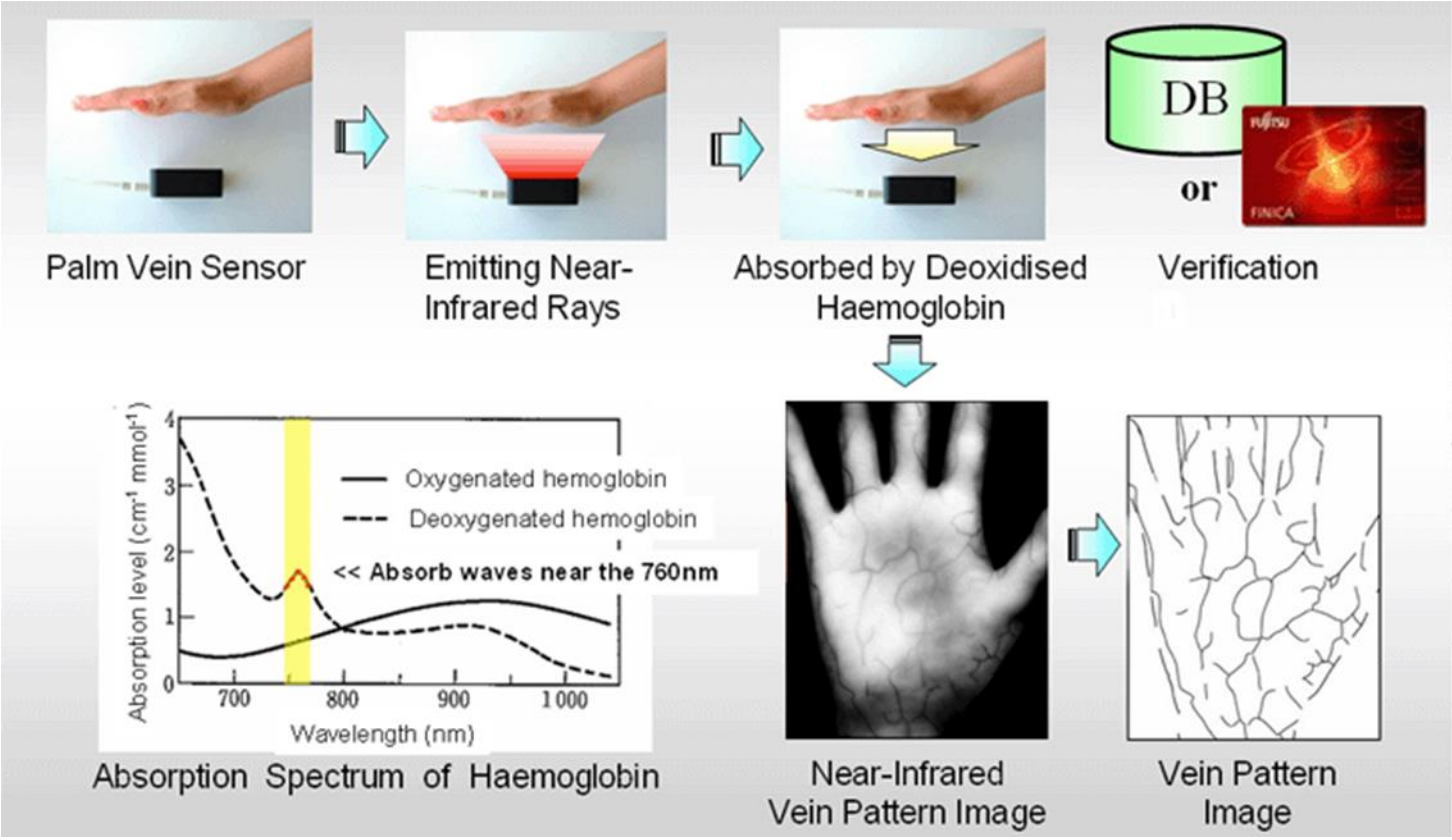


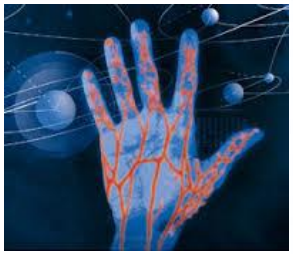
Vein pattern



Finger Vein

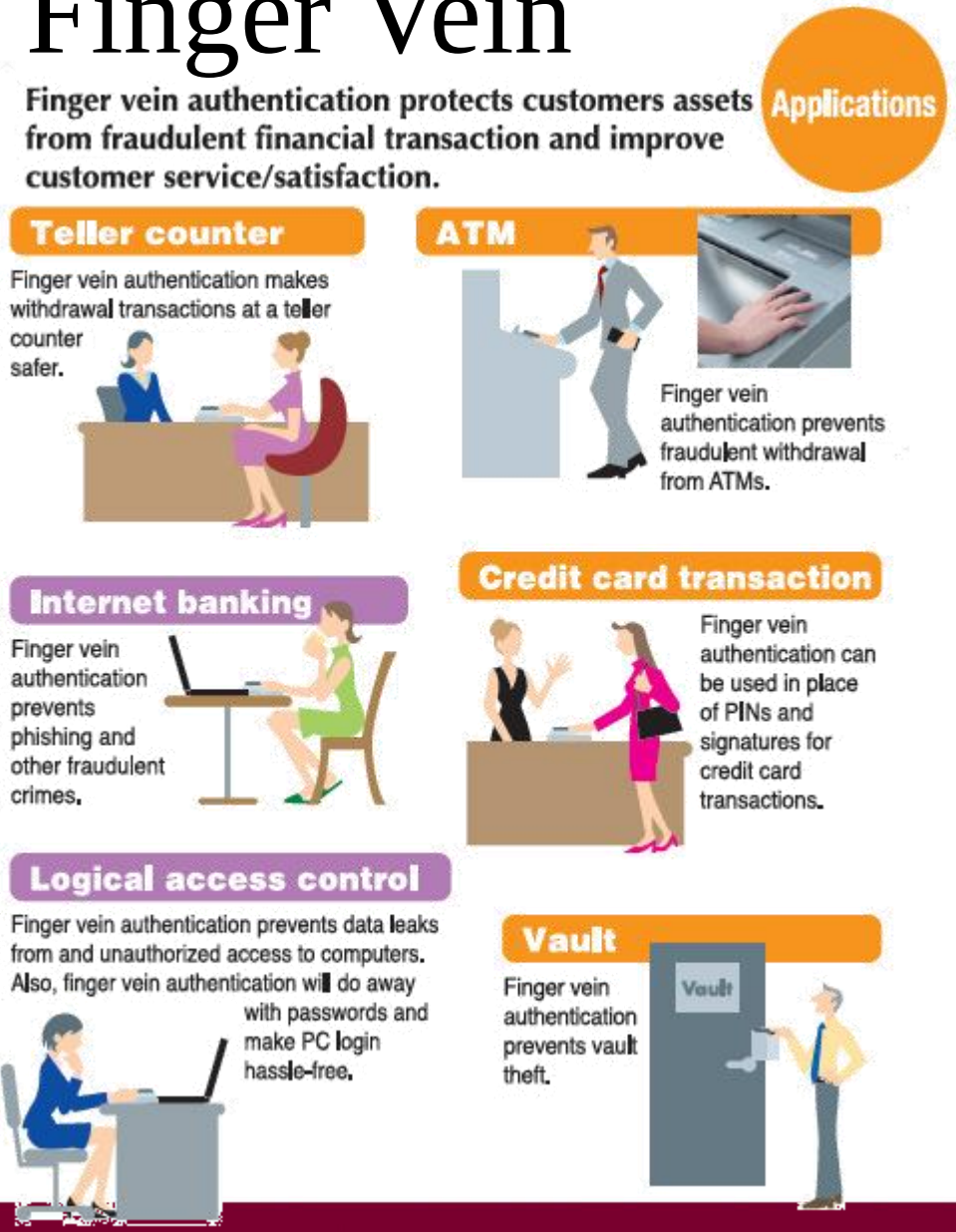
- Capturing Palm vein





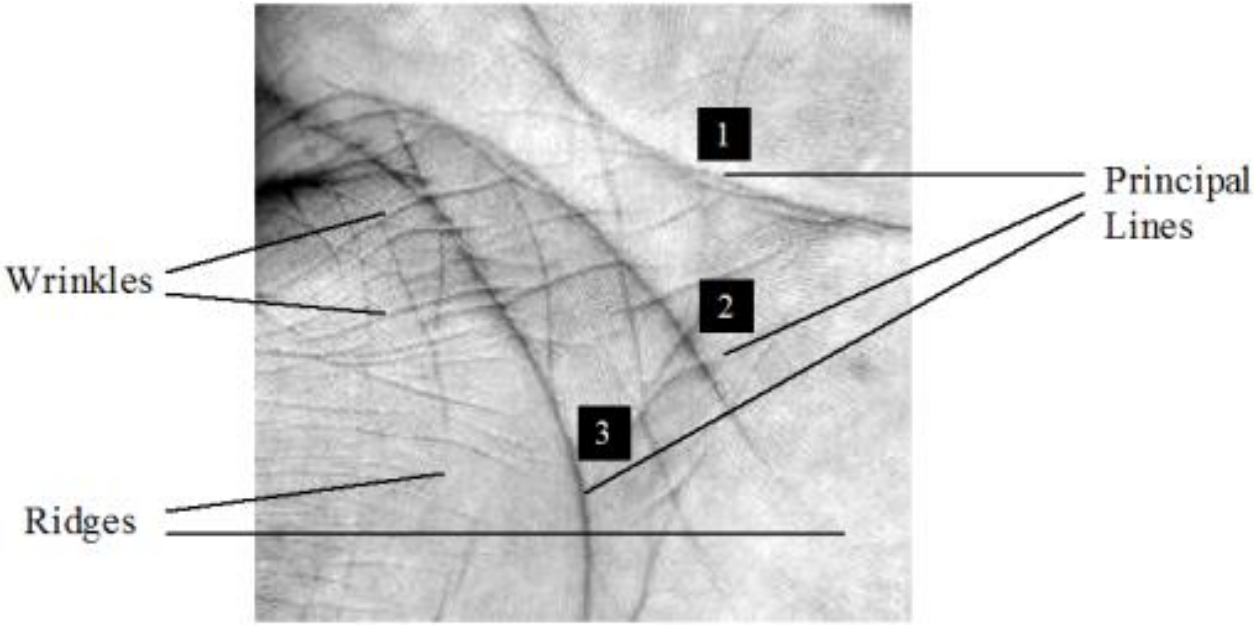
Finger Vein

- Applications



Palm Print

- based on the aggregate of information presented in a friction ridge impression



Palm Print

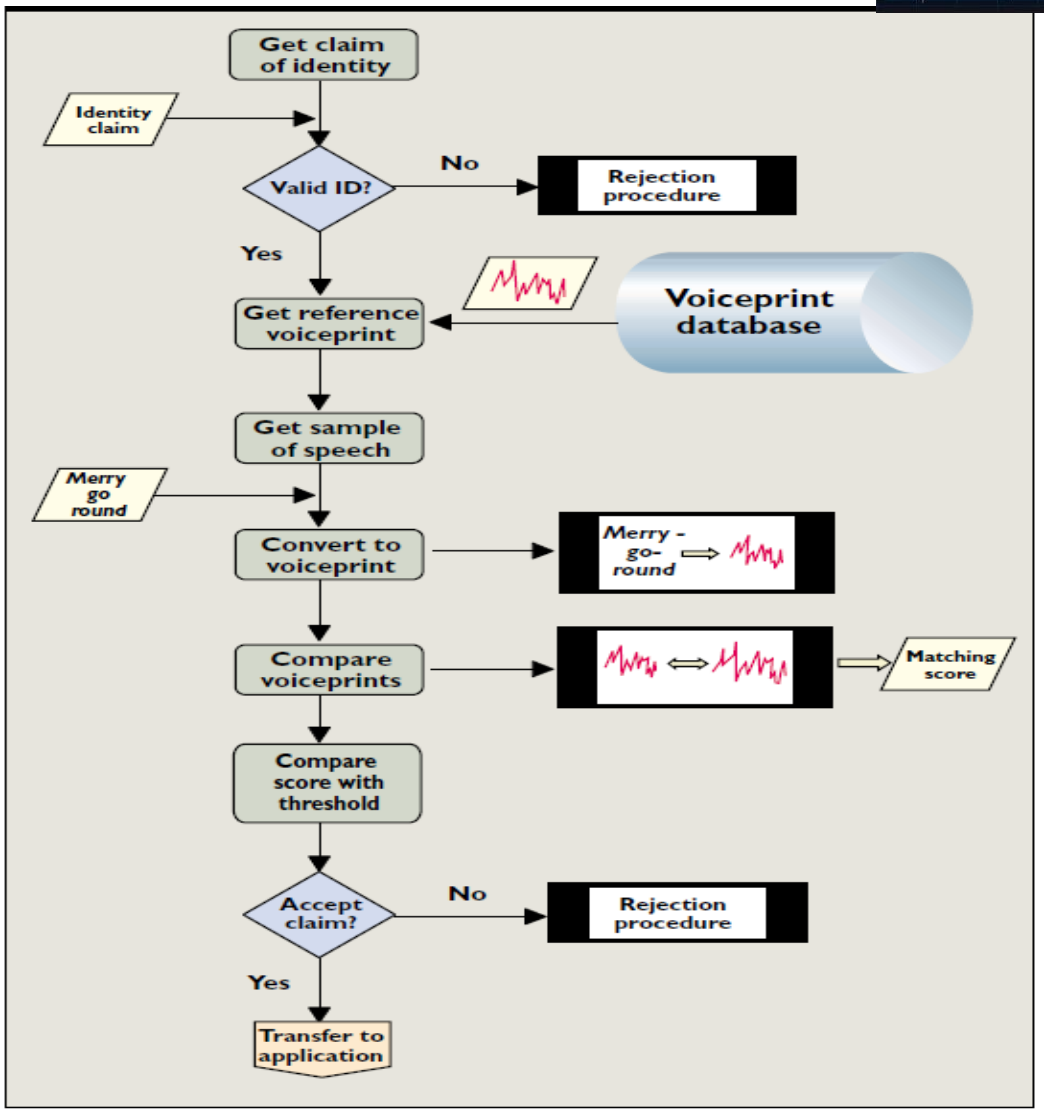
- Matching technique
  - Minutiae-based – most widely used
  - Correlation-based – template matching
  - Ridge-based matching – used ridge pattern landmark features and geometric characteristic – alternative to minutiae.

Voice

- Process acoustic information rather than image – frequency and pitch.
- 2 type of voice biometric
  - Speaker Verification
  - Speaker Identification
- Combines voice biometric and speech recognition
- Reference voice – voice prints

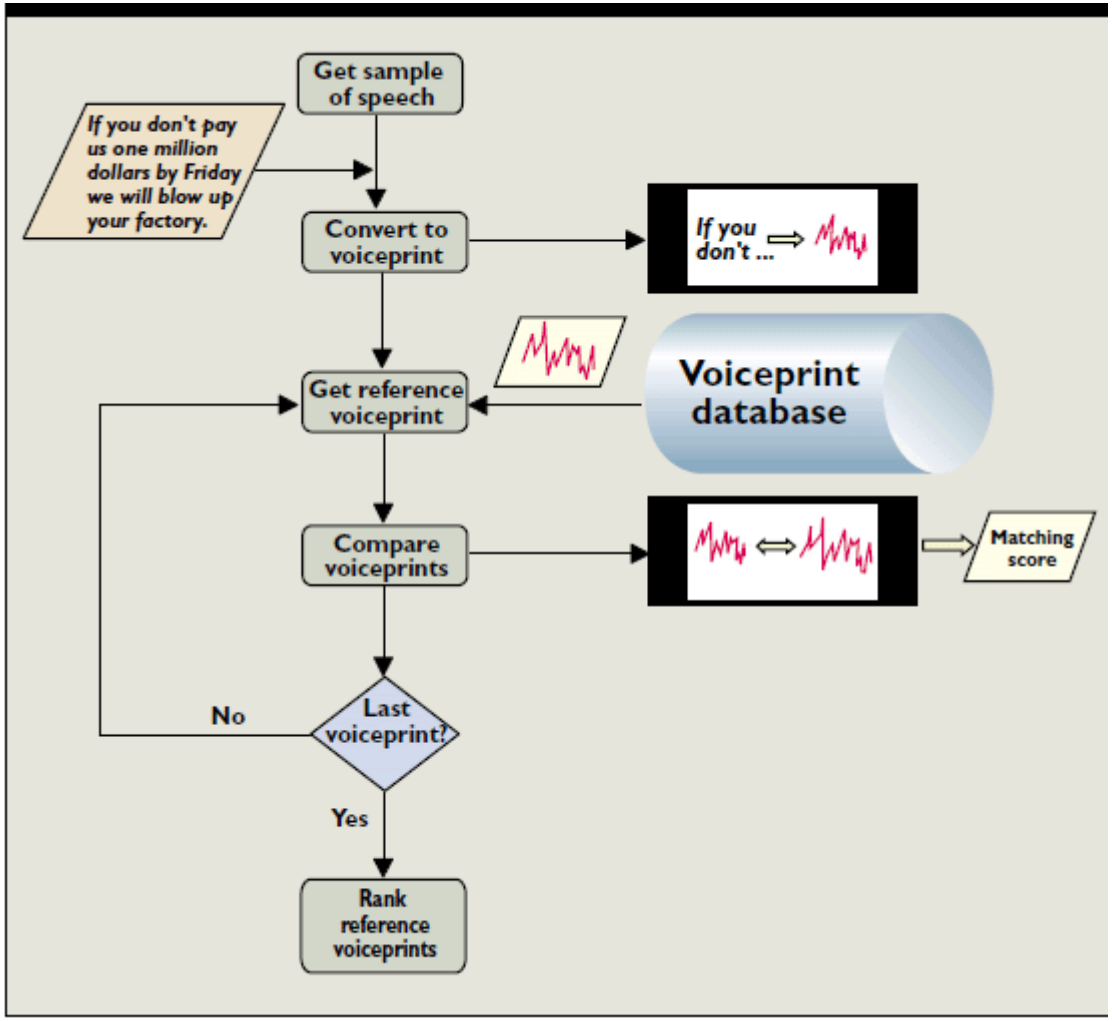
Voice

- Speaker Verification



Voice

- Speaker Identification



http://www.rapidsoftsystems.com/mobile-voice-biometrics-platform.html

Voice

- Problems
  - Human voices do not stay the same all the time e.g a person with a cold has a different voice
  - Quality of microphones
  - Background noise
  - Can be easily recorded and used for unauthorized PC or network
  - Low accuracy

Signature

- Online or Dynamic
  - Analyze shape, speed, stroke, pen pressure and timing information during the act of signing.
  - Only the original signer can recreate the changes in timing and X, Y, and Z (pressure).
  - Needs special pen and tablet.
- Offline or Static
  - Use image processing technique.
  - Look for certain features in the signature.

Signature


Dynamic singals of signature
Start and end of individual
Pressure
Time
Speed
Pressure levels
Static signature data
Crossing
Punctuation
Curves and loops
Closed areas

Signature

- Strength
  - High level of resistance to imposters - although it is quite easy to forge a signature, it is very difficult to “mimic” the behavioral patterns associated with the signature.
  - Noninvasive tool.
  - Unlike physiological biometrics, signature can be changed in case of stolen template

Signature

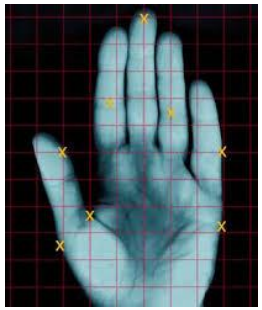
- Weakness
  - Inconsistency – prone to increase the error.
  - Inconveniency of using tablet – increase error.

Other Biometrics

- Gait - Style of walking

- Typing Rhythm

- Hand geometry



- Multimodal Biometrics

Standards

- Important from 2 aspects

1. Manufacturers
   - Compatibility
   - Sustainability
2. End Users
   - Portability
   - Reliability

Standards

- Involves
  - Framework of the System
  - Format of the Data
  - Testing of System
  - Data Quality

Standards

- Under ISO/IEC SC37 (Data Part)
  - Part 1 – Framework
  - Part 2 – Finger Minutiae
  - Part 3 – Finger Pattern Spectral Data
  - Part 4 – Finger Image
  - Part 5 – Face Image
  - Part 6 – Iris
  - Part 7 – Signature/Sign Time Series

Standards

- Under ISO/IEC SC37 (Data Part)
  - Part 8 – Finger Pattern Skeletal
  - Part 9 – Vascular Image
  - Part 10 – Hand Geometry Silhoutte
  - Part 11 – Signature/Sign Processed Dynamic
  - Part 12 –
  - Part 13 – Voice Data
  - Part 14 – DNA

Future of Biometric

- Will be the future form of identification
- Technology will make biometric more matured.
- Sophisticated algorithms will be fast with high accuracy and little chance to spoof.
- Hardware devices will be smaller but able to work afar.
- However, the system won't be perfect and constraints by limitations

Thank You
For
Your Attention