



Fingerprints and Human recognition

Jaroslav Siroic
Jayant Nehra



Agenda

- Introduction
- History of fingerprints
- Fingerprint acquisition
- Types of algorithms
- Sensor and algorithm integration
- Algorithm comparison
- Other biometric features
- Conclusion





Introduction

Biometrics

The term “biometrics” is derived from the Greek words “bio” (life) and “metrics” (to measure).

Due to significant advances in the field of computer processing, automated biometric systems have become available over the last few decades.

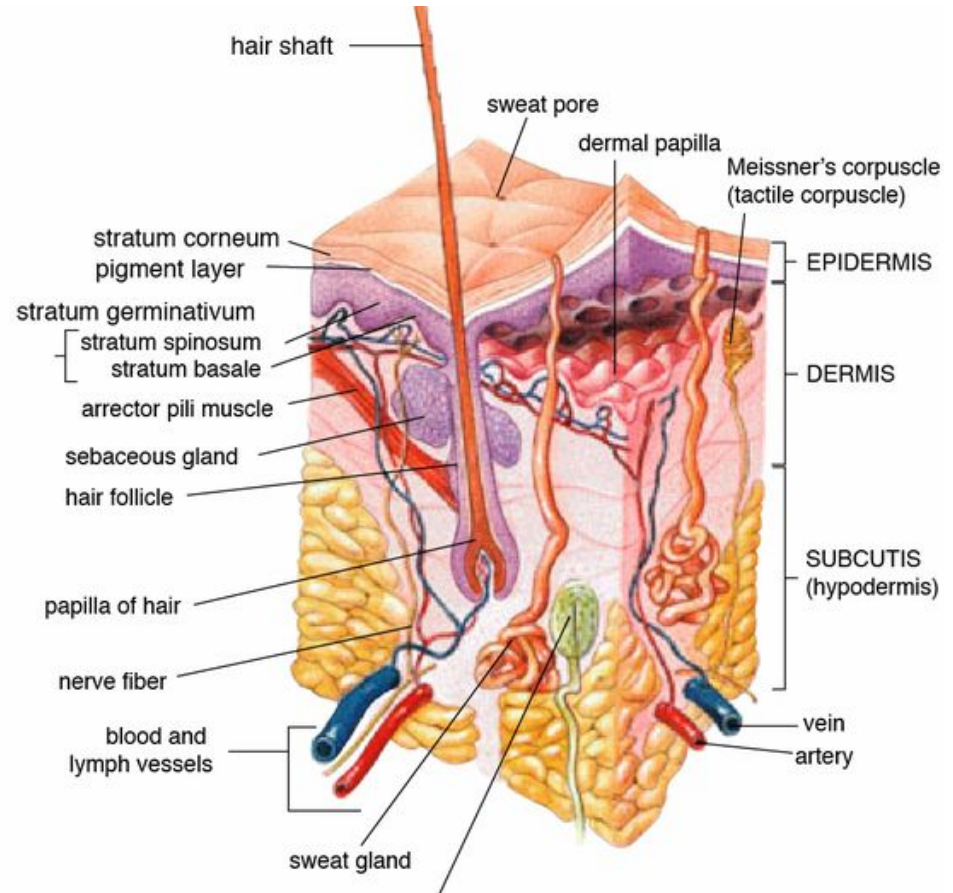
Many of these new automated techniques, however, are based on ideas that were originally conceived hundreds, even thousands of years ago.

One of the oldest and most basic examples of a characteristic that is used for recognition by humans is the face.

The concept of human-to-human recognition is also seen in behavioral-predominant biometrics such as speaker and gait recognition.

What is fingerprint?

A **fingerprint** is an impression left by the friction ridges of a human finger.



Formation of Fingerprint

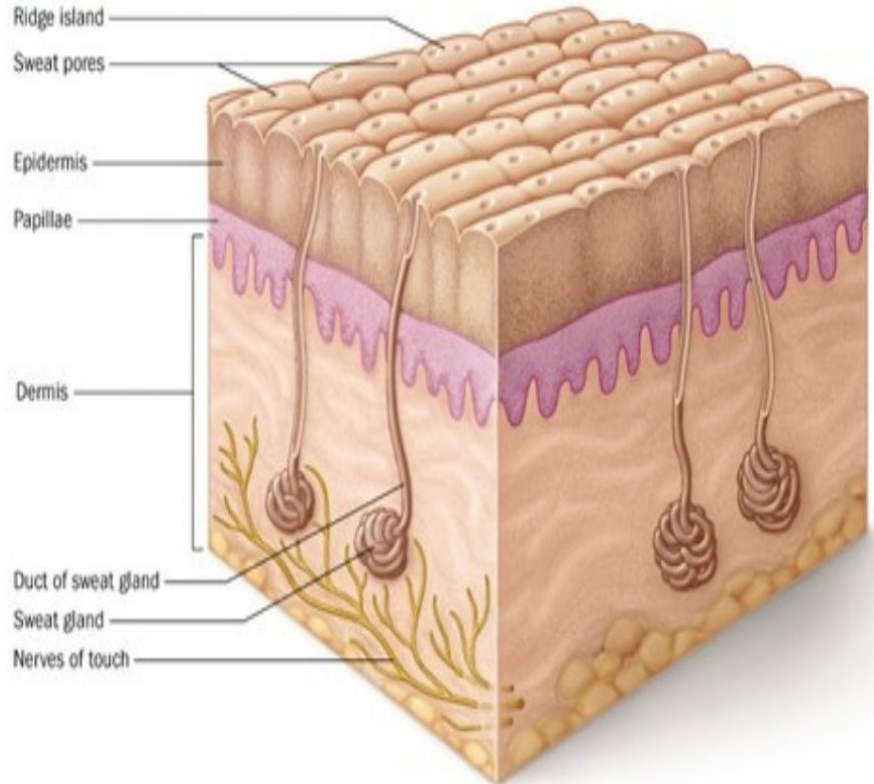
Skin consists of :

1. Inner Layer : dermis
2. Outer Layer : epidermis
3. Basel Layer in between

Basel layer grows faster than others.

It collapses and folds to form intricate shapes.

These folds and pores create unique patterns even amongst identical twins.



Types of fingerprint



LOOPS



WHORLS



ARCHES

Double Loop



Peacock's eye



Tented Arch





History of fingerprints

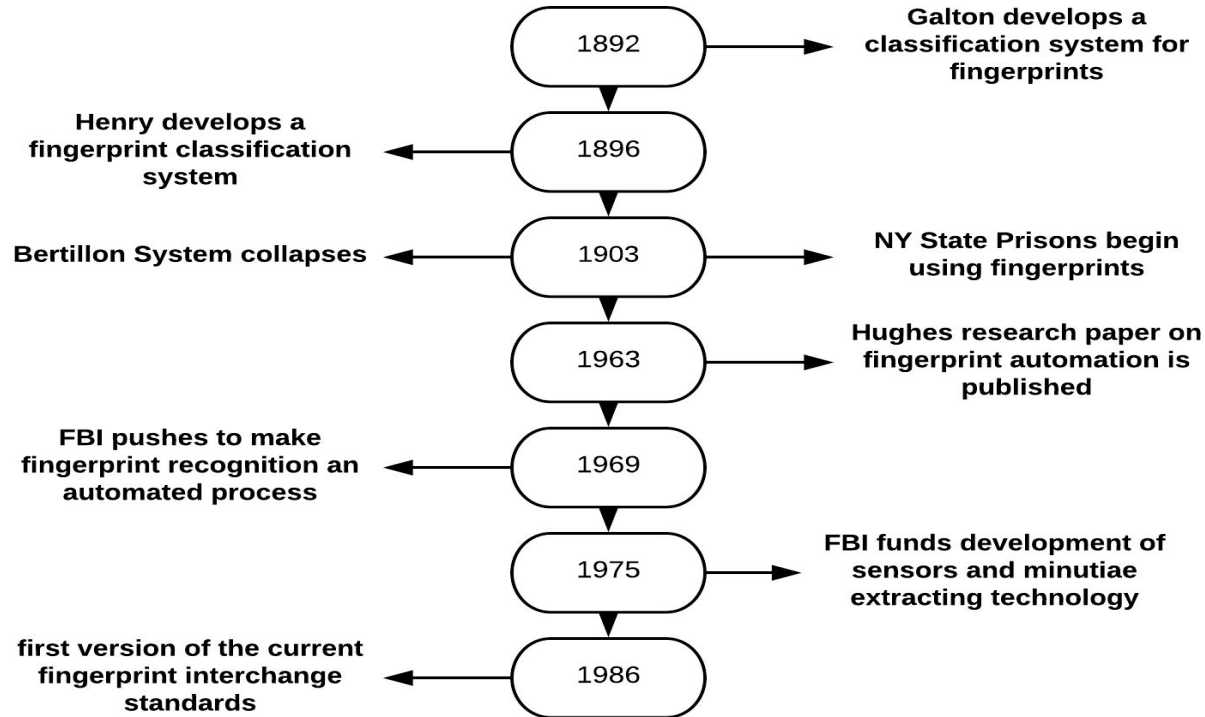
Fingerprints Historical Uses

- Person's mark as early as 500 B.C. "Babylonian business transactions are recorded in clay tablets that include fingerprints."
- Early Chinese merchants used fingerprints to settle business transactions.
- In 1684 Dr. Nehemiah Grew published friction ridge skin observations in "Philosophical Transactions of the Royal Society of London" paper.
- In 1686, Marcello Malpighi, an anatomy professor at the University of Bologna, noted fingerprint ridges, spirals and loops in his treatise.
- The first of two approaches was the Bertillon system of measuring various body dimensions, which originated in France.
- The other approach was the formal use of fingerprints by police departments. This process emerged in South America, Asia, and Europe.



- By the late 1800s a method was developed to index fingerprints that provided the ability to retrieve records.
- The first such robust system for indexing fingerprints was developed in India by Azizul Haque for Edward Henry, Inspector General of Police, Bengal, India. This system, called the Henry System, and variations on it are still in use for classifying fingerprints.
- True biometric systems began to emerge in the latter half of the twentieth century, coinciding with the emergence of computer systems.

Timeline of Fingerprint Biometrics





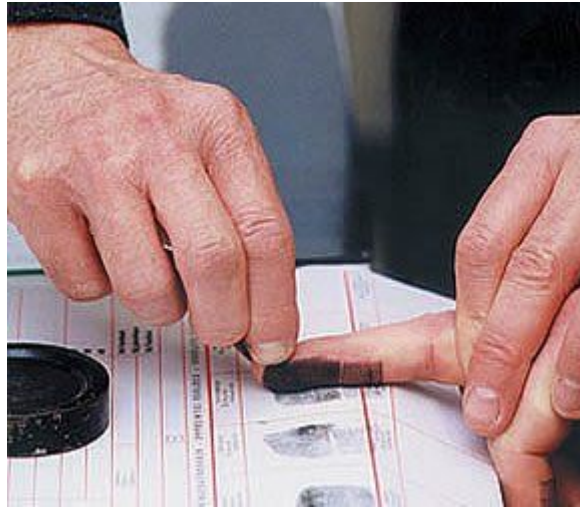
Fingerprint Acquisition

Old acquisition technologies

Chinese records from the Qin Dynasty (221-206 BC) include details about using handprints as evidence during burglary investigations



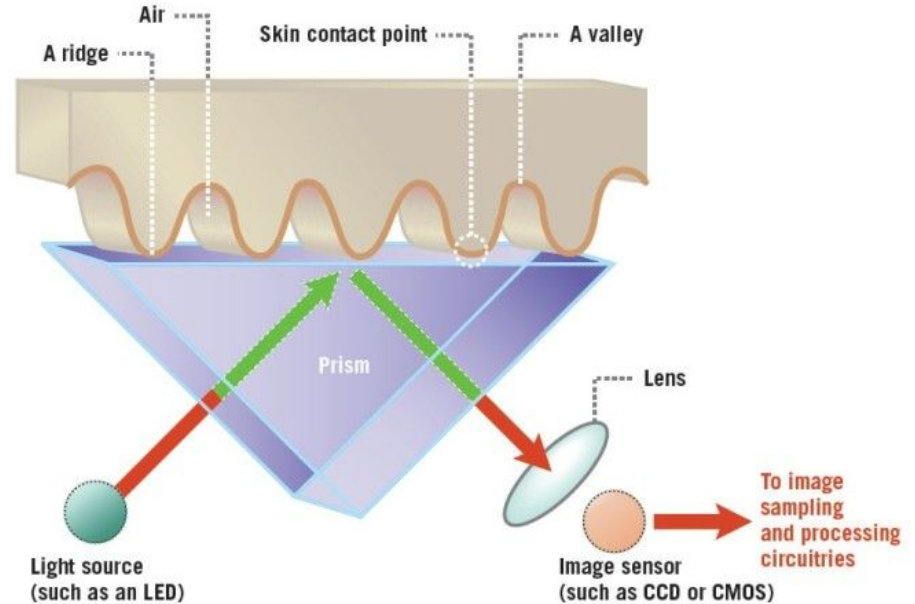
Rolled fingerprinting in police application using ink & paper.



Clay bullae from Greek and Roman periods

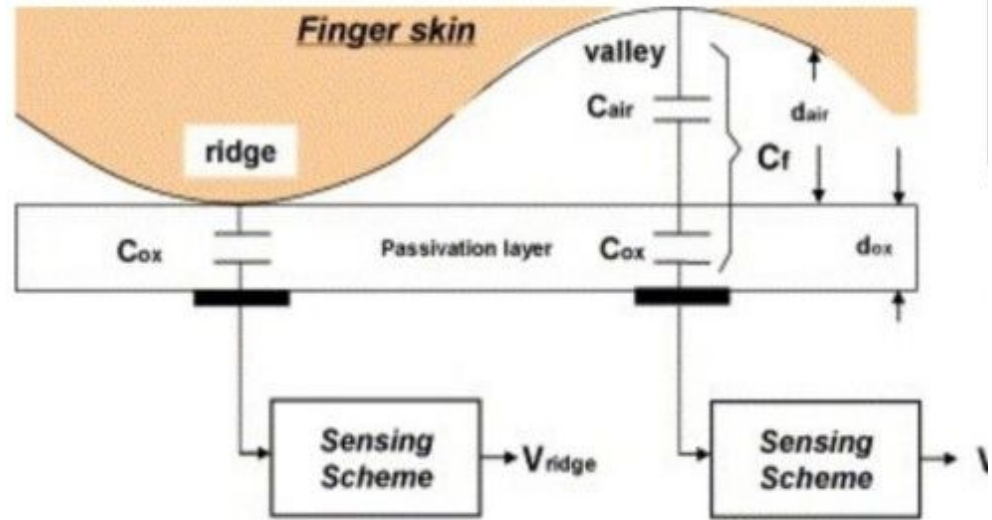
Optical sensor

Optical fingerprint scanners are the oldest method of capturing and comparing fingerprints. As the name suggests, this technique relies on capturing an optical image, essentially a photograph, and using algorithms to detect unique patterns on the surface, such as ridges or unique marks, by analysing the lightest and darkest areas of the image



Capacitive scanner

As capacitors can store electrical charge, connecting them up to conductive plates on the surface of the scanner allows them to be used to track the details of a fingerprint. The charge stored in the capacitor will be changed slightly when a finger's ridge is placed over the conductive plates, while an air gap will leave the charge at the capacitor relatively unchanged. An op-amp integrator circuit is used to track these changes, which can then be recorded by an analogue-to-digital converter.



Optical Vs Capacitive

Capacitive Sensors

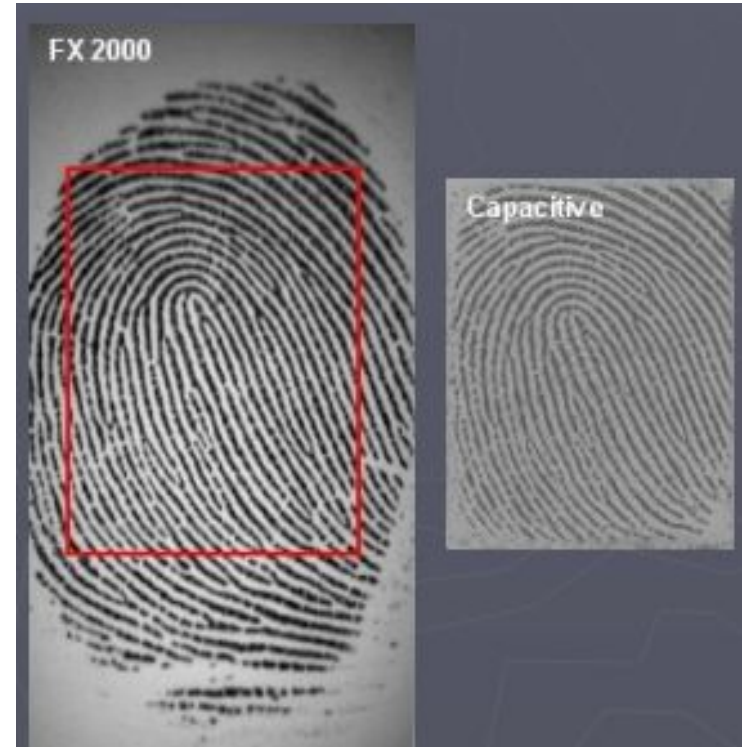
1. Greater miniaturization
2. Newer technology
3. Can be embedded into small devices
4. Prone to dirt etc. since finger touches silicon
5. Relatively cheap

Optical Sensors

1. Larger sensing area since manufacturing large pure silicon chips is expensive
2. More robust. Longer life
3. More expensive
4. Better image quality and higher resolution

Factors affecting the scan

- Image quality
 - Sharpness
 - Contrast
 - Distortion
- Resolution – higher is better
 - Too low and we cannot detect the minutiae
- Sensing area
 - Average fingerprint is about 0.5" x 0.7"
 - Large area (1.0" x 1.0") ensures that overlap effects (leading to false rejections) are reduced



Ultrasonic scanner

To actually capture the details of a fingerprint, the hardware consists of both an ultrasonic transmitter and a receiver. An ultrasonic pulse is transmitted against the finger that is placed over the scanner. Some of this pulse is absorbed and some of it is bounced back to the sensor, depending upon the ridges, pores and other details that are unique to each fingerprint.





Fingerprint Comparison Methods



1. Direct Correlation

In Earlier times two fingerprint images were matched manually but automated methods are widely used now.

Not efficient for large databases.















2. General shape of the fingerprint

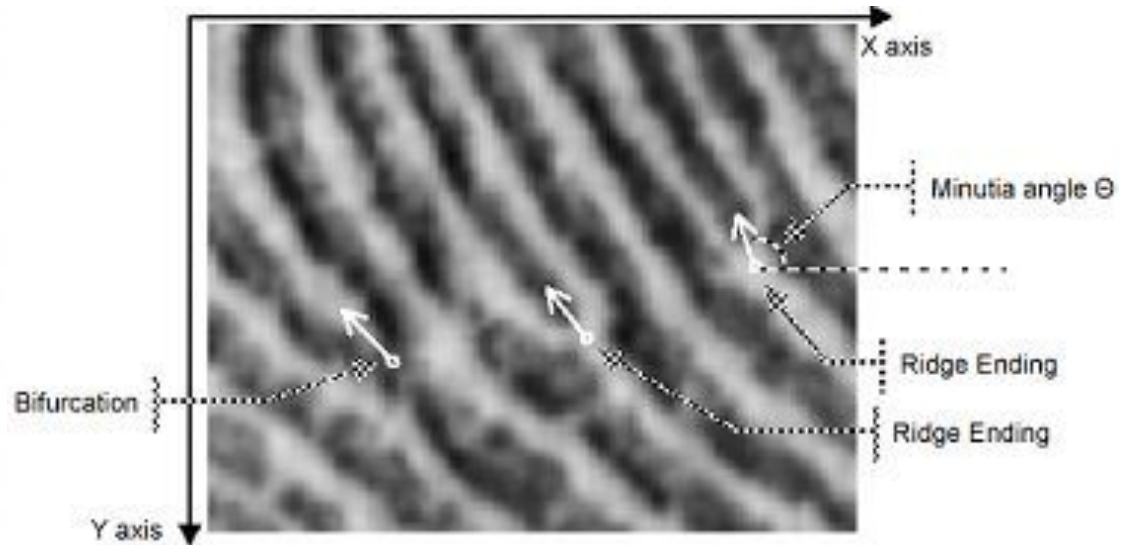
The general shape of the fingerprint is used to pre-process the images, and reduce the search in large databases. This uses the general directions of the lines of the fingerprint, and the presence of the core and the delta. Several categories have been defined in the Henry system: whorl, right loop, left loop, arch, and tented arch.



3. Minutiae-based comparison

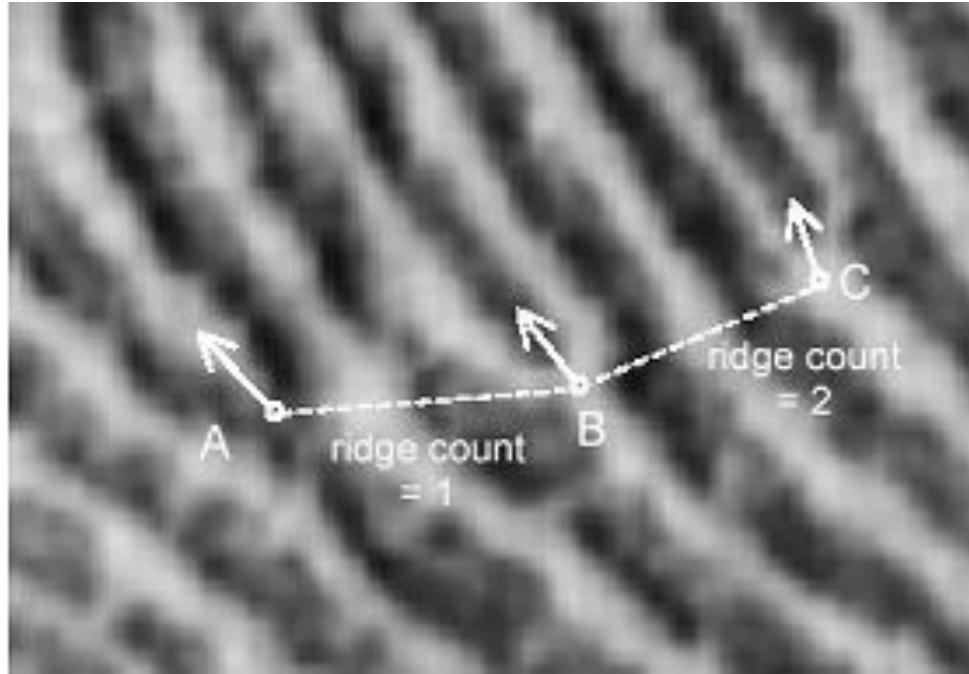
Most algorithms are using minutiae, the specific points like ridges ending, bifurcation... Only the position and direction of these features are stored in the signature for further comparison.

| Minutiae | Example | Minutiae | Example |
|----------------------|---|----------------------------------|---|
| ridge ending |  | bridge |  |
| bifurcation |  | double bifurcation |  |
| dot |  | trifurcation |  |
| island (short ridge) |  | opposed bifurcations |  |
| lake (enclosure) |  | ridge crossing |  |
| hook (spur) |  | opposed bifurcation/ridge ending |  |



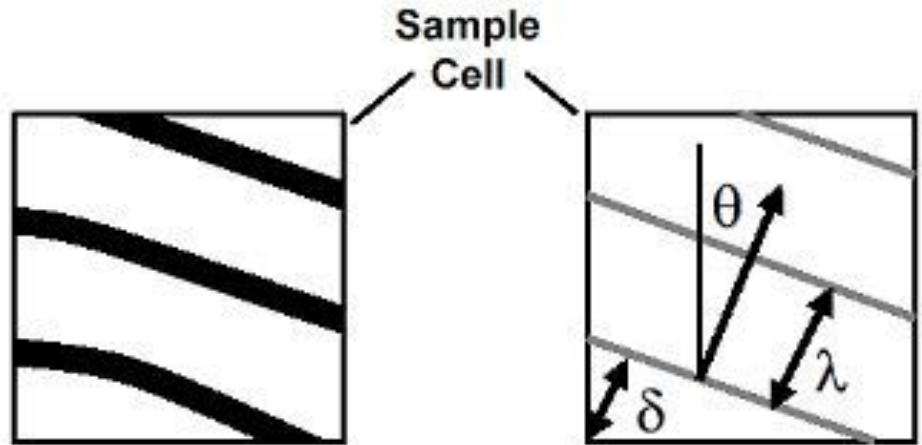
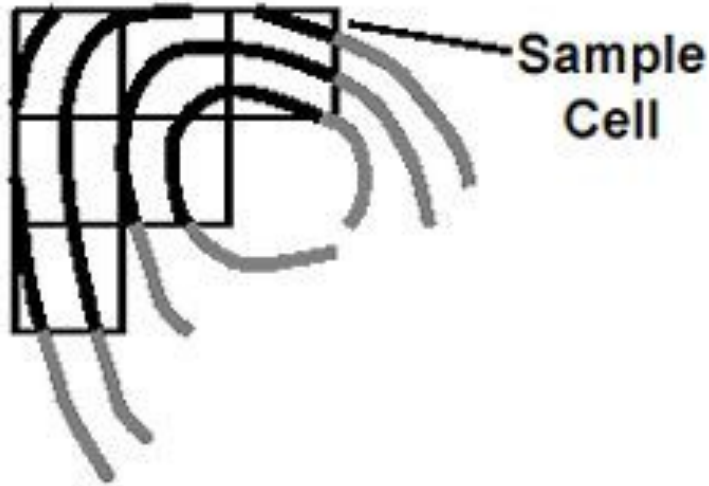
4. Compare the number of ridges

Some algorithms counts the number of ridges between particular points, generally the minutiae, instead of the distances computed from the position.



5. Pattern matching

Pattern matching algorithms are using the general shape of the ridges. The fingerprint is divided in small sectors, and the ridge direction, phase and pitch are extracted and stored.





Algorithms

Minutiae-based matching algorithms

The most popular matching approach for fingerprint identification is usually based on lower-level features determined by singularities in finger ridge patterns called minutiae. In general, the two most prominent used features are **ridge ending** and ridge **bifurcation**.



a)



b)

Example of a) ridge ending and b) bifurcation.

MINUTIAE EXTRACTION

Typically each detected minutiae m_i is described by four parameters:

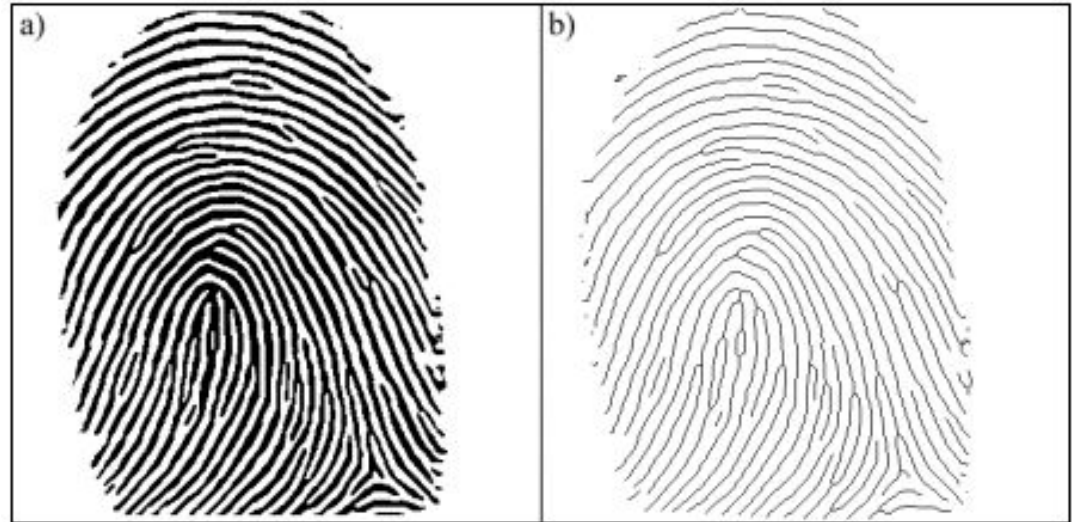
$$m_i = (x_i, y_i, \theta_i, t_i)$$

where:

- x_i, y_i – are coordinates of the minutiae point,
- θ_i – is minutiae direction typically obtained from local ridge orientation,
- t_i – is type of the minutiae point (ridge ending or ridge bifurcation),

MINUTIAE EXTRACTION - RIDGE THINNING METHOD

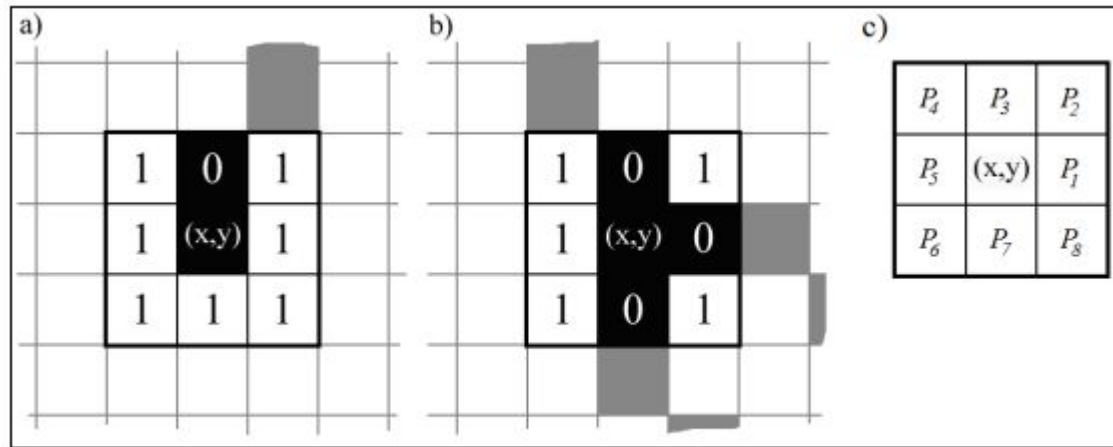
The most commonly used method of minutiae extraction is the **Crossing Number (CN)** concept. The binary ridge image needs further processing, before the minutiae features can be extracted. The first step is to binarize and further to thin the ridges, so that they are single pixel wide



Fingerprint image a) binarization and b) skeletonization.

MINUTIAE EXTRACTION - RIDGE THINNING METHOD

The minutiae points are determined by scanning the local neighbourhood of each pixel in the ridge thinned image, using a 3×3 window



a) Ridge ending and b) bifurcation in c) 3×3 window.

MINUTIAE EXTRACTION - RIDGE THINNING METHOD

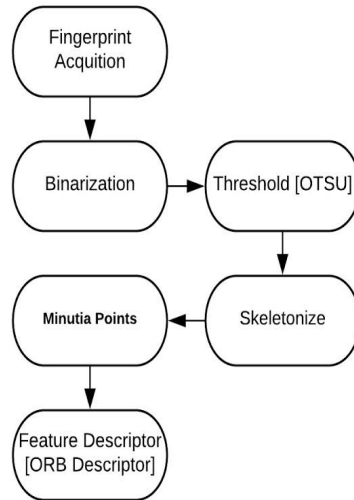
The CN value is then computed, which is defined as half the sum of the differences between pairs of neighbouring pixels p_i and p_{i+1}

$$CN_{(x,y)} = \frac{1}{2} \sum_{i=1}^8 |p_i - p_{i+1}|, \quad p_1 = p_9$$

| CN | Property |
|----|---------------------|
| 0 | Isolated point |
| 1 | Ridge ending |
| 2 | Continuing ridge |
| 3 | Bifurcation |
| 4 | Crossing |

Properties of the *Crossing Number*.

Our Feature Extraction Pipeline



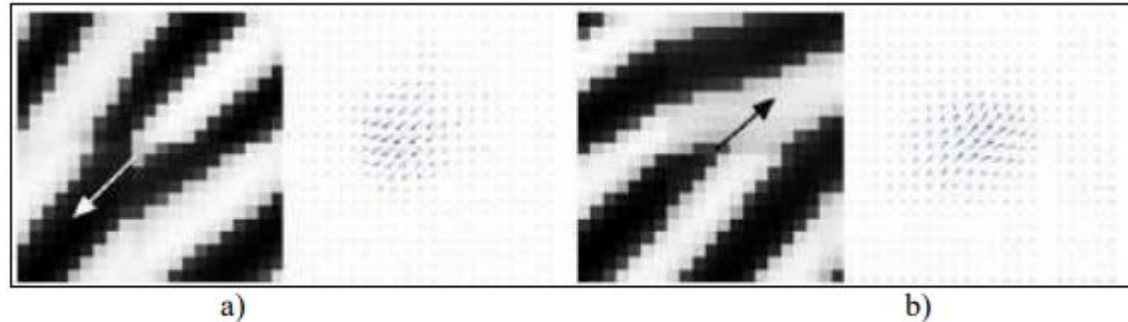
MINUTIAE EXTRACTION - DIRECT GRAYSCALE METHOD

Minutiae extraction approaches, that work directly on the grey-scale images, without binarization and thinning, was induced by these consideration:



- enhancement algorithms are time-consuming
- a significant amount of information may be lost during the binarization process
- skeletonization may introduce a large number of false minutiae
- unsatisfactory results when applied to low quality images

DIRECT GRAYSCALE METHOD - LINEAR SYMMETRY

Nilsson and Bigun proposed using Linear Symmetry (LS) filter in the minutiae extract approach, based on the concept that minutiae are local discontinuities of the LS vector field. Two types of symmetries - parabolic symmetry and linear symmetry are adapted to model and locate the points in the grayscale image, where there is lack of symmetry.



Symmetry filter response in the minutiae point. a) ridge bifurcation, b) ridge ending



Sensor and Algorithm Integration

System On Chip

1. 1998, May HP OB3000 laptop prototype with integrated Thomson-CSF (now Atmel) FingerChip + logon from Cogent demonstrated at the CTST'98 in Orlando.
2. 2002, Jan Trek's Thumbdrive Touch G3 128MB, using the Sony sensor.
3. 2002, Nov The HP iPAQ h5450 is the first PDA with a built-in fingerprint sensor, the FingerChip from Atmel.
4. 2004, Oct IBM ThinkPad T42 integrates the sweep fingerprint sensor from Upek/ST.

Around 2005 system with built-in sensors took off for all kinds of consumer products.

Apple Touch ID

Touch ID is built into the home button. It features a stainless steel detection ring to detect the user's finger without pressing it. The feature does not work without contact with this ring.

The sensor uses **capacitive touch** to detect the user's fingerprint. Apple says it can read sub-epidermal skin layers, and it will be easy to set up and will improve with every use. Up to 5 fingerprint maps can be stored in the Secure Enclave.



Synaptics Clear ID Optical In-Display Fingerprint

Designed to enable smartphones with infinity displays, Synaptics' Clear ID in-display fingerprint sensors are placed in a natural location directly in the OLED touchscreen, eliminating the need for buttons and bezels. A fingerprint icon in the display guides the user and disappears upon authentication. Clear ID is faster than alternative biometrics such as 3D facial, and very convenient with one-touch biometric authentication





Spooofing

Types of attack

- Brute force
- Latent print
- Replay
- Trojan Horses
- Fake feature
- Dead feature
- Other (software leaks, bad security policies etc)

Fake Fingerprint





Comparison to other biometric features

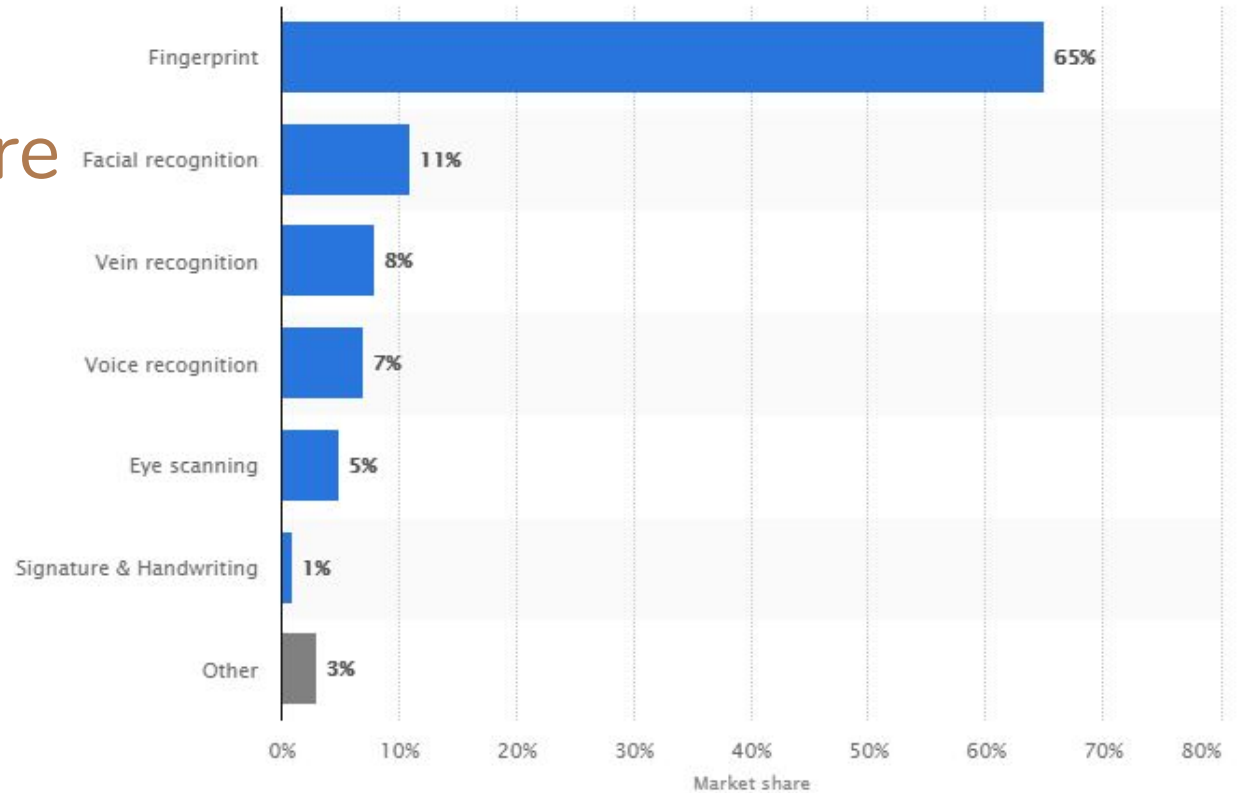
Comparison Metric

- **Universality** (availability) - “failure to enroll” rate.
- **Distinctiveness** - False Match Rate (FMR).
- **Permanence** (robustness) - False Non-Match Rate (FNMR).
- **Collectability** (accessible) - “throughput rate” of the system.
- **Performance** - recognition accuracy, speed, and the resources required to the application.
- **Acceptability** - measured by “Resistance to Circumvention”.

| Biometric characteristic | Universality | Distinctiveness | Permanence | Collectability | Performance | Acceptability | Circumvention |
|---------------------------------|---------------------|------------------------|-------------------|-----------------------|--------------------|----------------------|----------------------|
| Facial thermogram | H | H | L | H | M | H | L |
| Hand vein | M | M | M | M | M | M | L |
| Gait | M | L | L | H | L | H | M |
| Keystroke | L | L | L | M | L | M | M |
| Odor | H | H | H | L | L | M | L |
| Ear | M | M | H | M | M | H | M |
| Hand geometry | M | M | M | H | M | M | M |
| Fingerprint | M | H | H | M | H | M | M |
| Face | H | L | M | H | L | H | H |
| Retina | H | H | M | L | H | L | L |
| Iris | H | H | H | M | H | L | L |
| Palmprint | M | H | H | M | H | M | M |
| Voice | M | L | L | M | L | H | H |
| Signature | L | L | L | H | L | H | H |
| DNA | H | H | H | L | H | L | L |

Market share

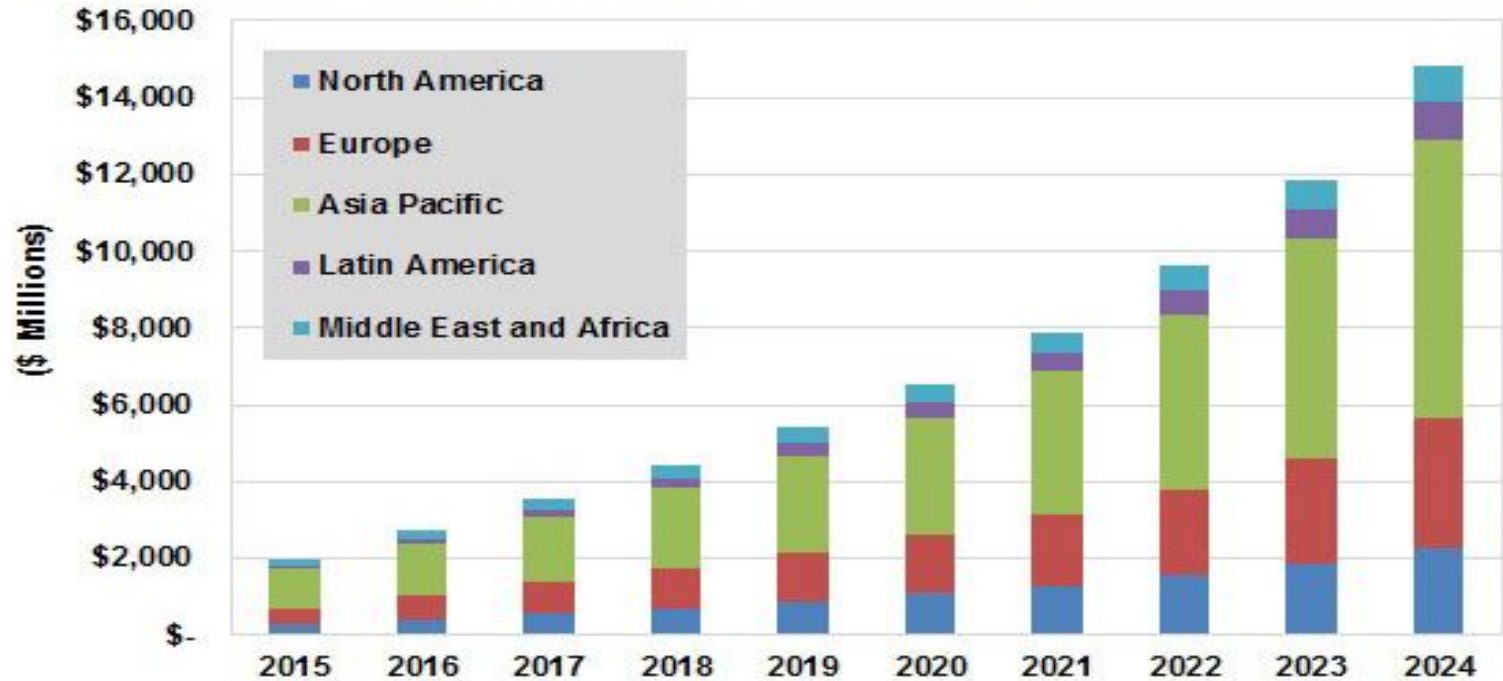
This statistic represents the global biometric market in 2015



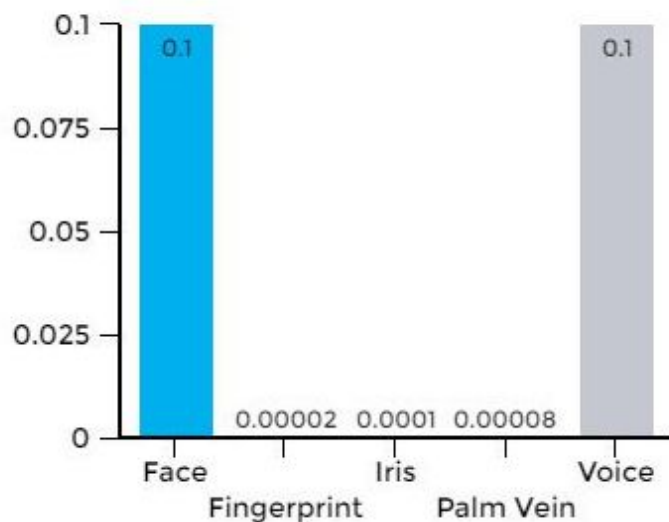
Global fingerprint sensor volume vs. ASP from year 2014 to 2020 (estimated)



Annual Biometric Revenue by Region

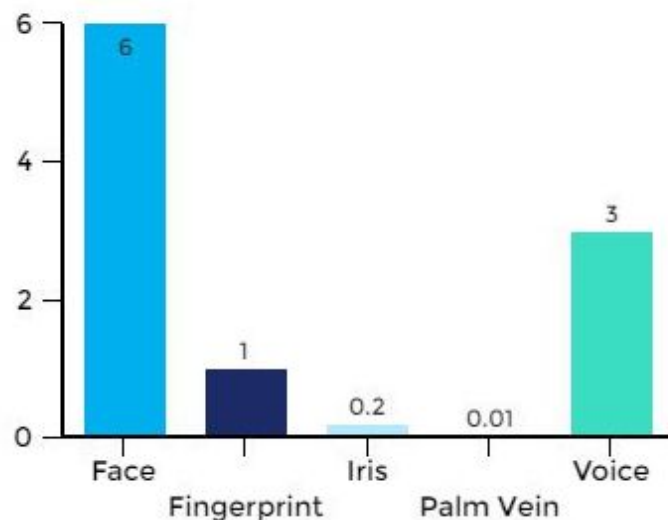


FAR/FRR





False Acceptance Rate

FAR is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.



False Rejection Rate

False rejection rate (FRR) is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user.



Future of fingerprint technology

Future of Fingerprint Technology

- A new fingerprint technique that has been developed by Sheffield Hallam University, in partnership with West Yorkshire Police.
- The technique is based around **mass spectrometry**, an analytical technique that ionises chemicals and sorts the ions based on their mass-to-charge ratio.
- In practical terms this means that authorities will be able to detect, via a fingerprint sample, whether that individual has, for example, handled a condom, consumed alcohol or drugs, whether the subject is male or female and even the brand of hair gel they use.

Mass spectrometry

Mass spectrometry is an analytical technique that can find traces of a substance within the ridges of a fingerprint.

It then vaporises the sample and fires it through an electric and magnetic field inside a vacuum – this causes the particles to behave differently meaning that different molecules can be identified.

What can mass spectrometry detect?

- Gender, Blood (human or animal), Drugs (specifically cocaine, marijuana, cannabis, heroin, amphetamine),
- Hair, Cleaning products / cosmetics, Condom lubricants (down to brand) , Food and drink

Future of Biometric Systems

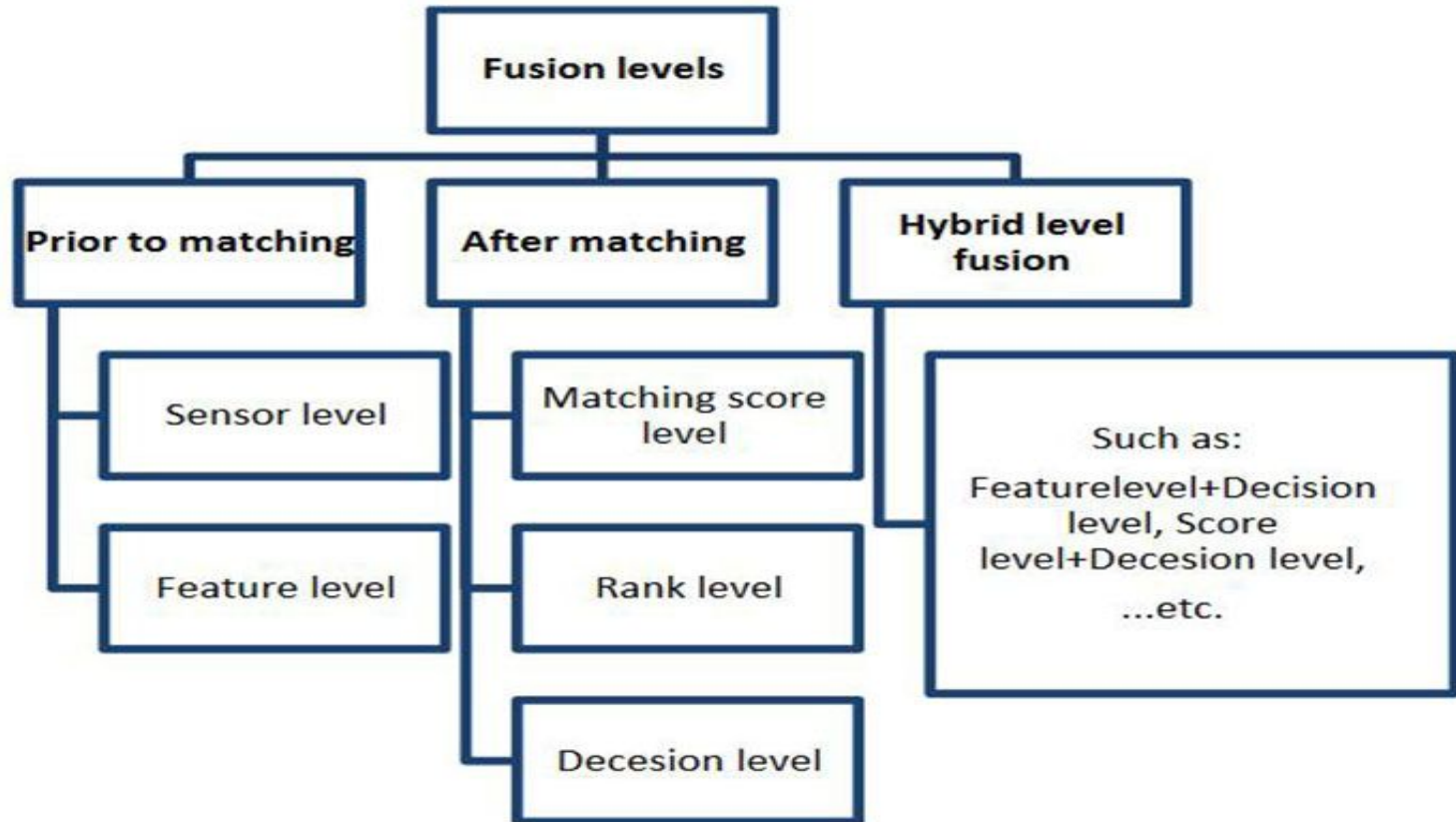
- Social Penetration of technology has been astonishing in the past few decades.
- Smartphones, personal digital assistants, wearables and smart devices are digitizing most aspects of our lives.
- Hand in hand with smartphones and other portable computing devices, biometrics has also sneaked in our life, changing the way how devices in your possession recognize you.
- Started with flagship and high-end devices, this trend of putting a fingerprint sensor on smartphones has now made it to inexpensive devices as well.

Integration Scenarios in Multi-Biometric Systems

Since multi-biometric systems are designed to use more than one or multiple sample from one biometric trait, they use one of the following integration scenarios to capture and process biometric characteristics:

- **Multi-sensor systems**
- **Multi-modal systems**
- **Multi-instance systems**
- **Multi-sample systems**
- **Multi-algorithm systems**
- **Hybrid systems**

Fusion Levels



Fingerprint Role in Multi-Biometric Fusion Techniques



M2-FuseID™ Advanced Fingerprint Reader

- captures a high-quality, 500 dpi fingerprint image.
- captures the unique finger vein pattern inside your finger
- Liveness Detection.
- Spoofing Detection.





Conclusion

- 
- When it comes to security, fingerprint authentication is a more secure means of authentication than a four-digit PIN, and user doesn't have to remember it.
 - The rapid increase of smartphones with fingerprint technology has made biometrics part of our daily lives.
 - On the negative side, two of the biggest drawbacks of biometrics over the years—high costs and privacy concerns—are still issues.
- 

Bibliography

- <https://www.androidauthority.com/how-fingerprint-scanners-work-670934/>
- <http://www.ancientpages.com/2016/03/04/fascinating-ancient-history-of-fingerprints/>
- <https://www.statista.com/statistics/736629/worldwide-biometric-market-distribution-by-technology/>
- <https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/>
- A MINUTIAE-BASED MATCHING ALGORITHMS IN FINGERPRINT RECOGNITION SYSTEMS:
http://www.keia.ath.bielsko.pl/sites/default/files/publikacje/11-BIO-41-lukaszWieclawMIT_v2_popr2.pdf
- https://thesai.org/Downloads/Volume6No6/Paper_18-Multi_Biometric_Systems_A_State.pdf
- <http://www.m2sys.com/wp-content/uploads/pdf/M2-FuseID-web-flyer.pdf>
- <https://www.bayometric.com/global-biometric-market-analysis/>
- <http://handlines.blogspot.com/2005/09/do-you-have-unusual-fingerprints.html>
- Fingerprint Sensing Techniques, Devices and Applications Rahul Singh kingtiny@cs.cmu.edu 30th April 2003