Fingerprint Recognition

Part of the content is based on the tutorial by Annalisa Franco (IAPR/IEEE Winter School on Biometrics 2020)

BiDA Lab
Biometrics & Data Pattern Analytics Lab

UAM
Universidad Autónoma de Madrid

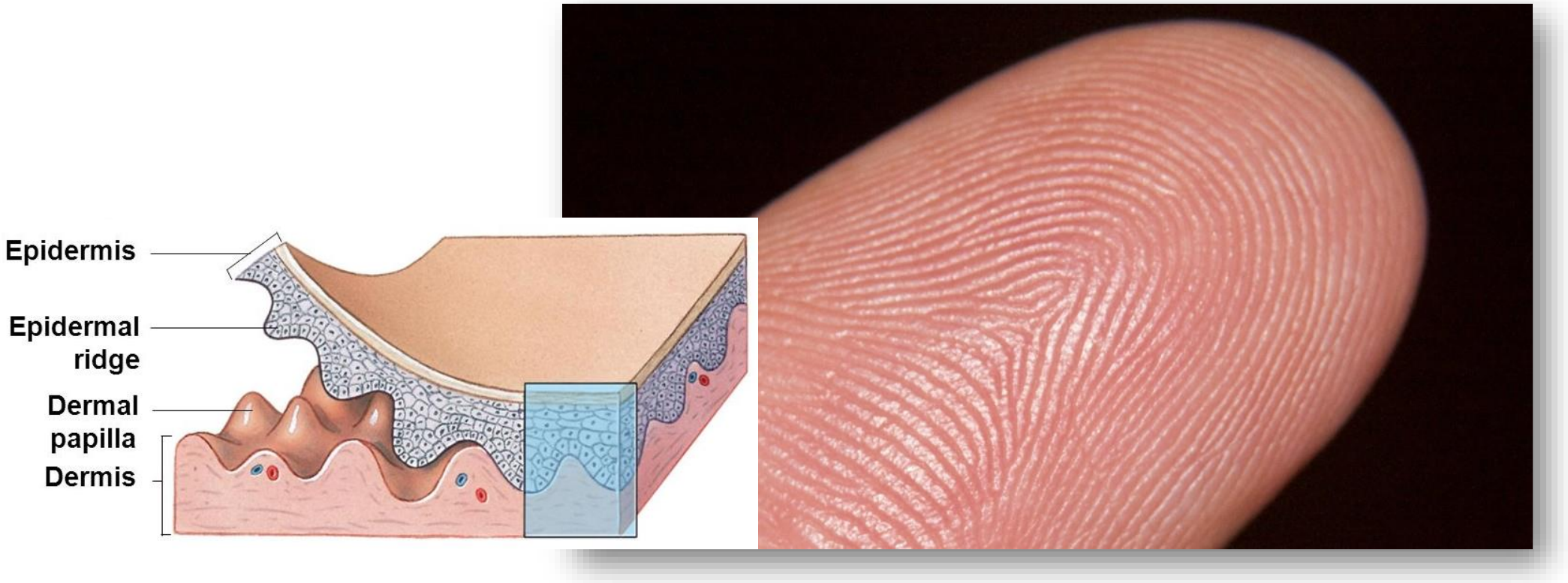
What is it?

It is an impression left by the friction ridges and valleys of a human finger.

- A. K. Hrechak, and J. A. McHugh, “Automated fingerprint recognition using structural matching,” Pattern Recognition, 23(8), 893-904, 1990.
- D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition. Springer Science & Business Media, 2009.

Why Do We Have Fingerprints?

The dermal papillae causes the ridges and valleys developed on the surface of the epidermis (in hands and feet).



- A. K. Hrechak, and J. A. McHugh, “Automated fingerprint recognition using structural matching,” Pattern Recognition, 23(8), 893-904, 1990.
- D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition. Springer Science & Business Media, 2009.

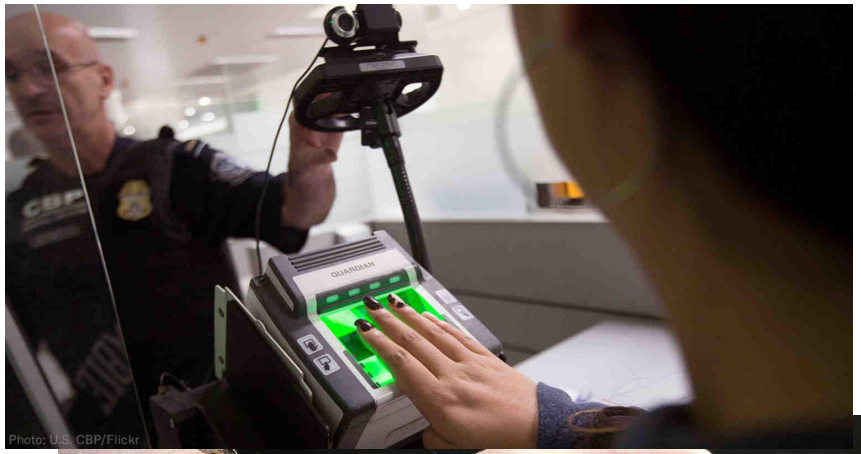
Patterns?

Small body region with a lot of high discriminant information

- A. K. Hrechak, and J. A. McHugh, “Automated fingerprint recognition using structural matching,” Pattern Recognition, 23(8), 893-904, 1990.
- D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition. Springer Science & Business Media, 2009.

Why is it so Popular?

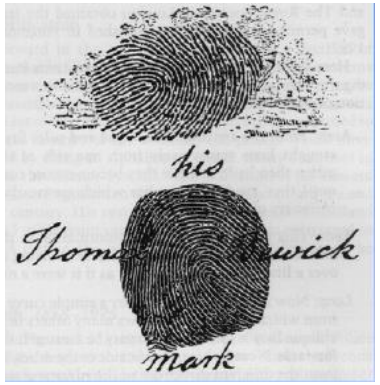
Fingerprint is arguably the most commonly used physiological biometric feature.



- A. K. Jain, K. Nandakumar, and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities.” Pattern Recognition Letters, 79, 80-105, 2016.

Why is it so Popular?

- Ancient biometric identification technique.
- Highly distinctive and unique.
- Do not change during the lifetime of a person.
- Publicly accepted as reliable (evidence in a court of law).
- Identical twins have different fingerprints.



- A. K. Jain, K. Nandakumar, and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities.” Pattern Recognition Letters, 79, 80-105, 2016.

Milestones in Fingerprint Recognition

- ~1000-2000 B.C.: Fingerprints for business transactions in ancient Babylon.
- 3rd Century B.C.: Thumbprints used on clay seals in China to "sign" documents.
- 14th Century: Official government documents in Persia have fingerprint impressions.
- 1686: Professor Marcello Malpighi (Bologna) notes the common characteristics of spirals, loops and ridges in fingerprints
- 1823: J. E. Purkinje published a thesis detailing full nine different fingerprint patterns.
- 1880: Dr. Henry Faulds published an article proposing fingerprints for personal identification. Also in 1880, Faulds sent a description of his fingerprint classification system to Sir Charles Darwin. Darwin, aging and in poor health, declined to assist Dr. Faulds in the further study of fingerprints, but forwarded the information on to his cousin, British scientist Sir Francis Galton.

Milestones in Fingerprint Recognition

- 1883: “Life on the Mississippi,” a novel by Mark Twain, tells the story of a murderer who is identified by the use of fingerprints. His later book "Pudd'n Head Wilson” includes a courtroom drama involving fingerprint identification.

- 1888: Sir Francis Galton’s began his study of fingerprints during the 1880s. Galton became the first to provide scientific evidence that no two fingerprints are exactly the same, and that prints remain the same throughout a person’s lifetime.

- 1892: Juan Vucetich (Argentine police official) made the first criminal fingerprint identification.

- 1902: Alphonse Bertillon, director of the Bureau of Identification of the Paris Police, is responsible for the first criminal identification of a fingerprint without a known suspect.

- 1903: Fingerprinting technology comes into widespread use in the United States.

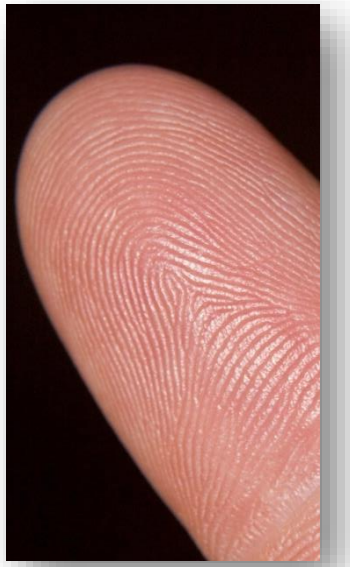
- 1909: Dr. Federico Olóriz Aguilera introduced the fingerprint science in Spain.

Milestones in Fingerprint Recognition

- 1924: The U.S. Congress acts to establish the Identification Division of the F.B.I. By 1946, the F.B.I. had processed 100 million fingerprint cards; that number doubles by 1971.
- 1990s: AFIS, or Automated Fingerprint Identification Systems, begin widespread use around the country.
- 2010: IAFIS processed more than 61 million ten-print submissions during Fiscal Year 2010.
- Nowadays: fingerprint is everywhere...

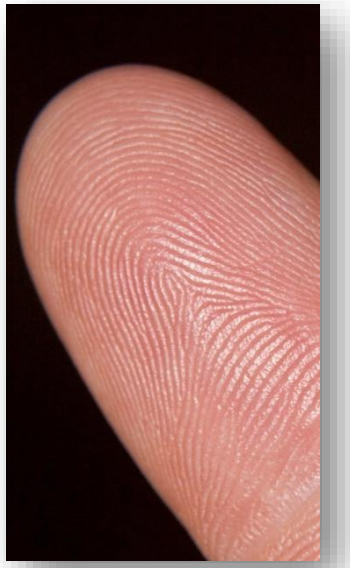
Types of Fingerprints

- Natural: Observed directly on the finger (e.g., taking a picture).



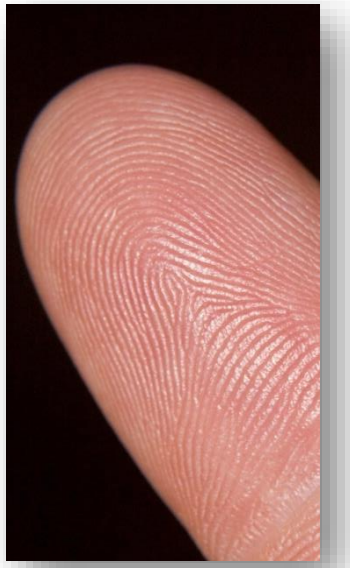
Types of Fingerprints

- Natural: Observed directly on the finger (e.g., taking a picture).
- Latent: transmitted over the contact with a surface.



Types of Fingerprints

- Natural: Observed directly on the finger (e.g., taking a picture).
- Latent: transmitted over the contact with a surface.
- Digital: graphic reproduction of a natural fingerprint (e.g., using sensors).



Ink vs. Digital

- Ink: Manual acquisition process following the traditional forensic techniques. Latent fingerprints are lifted during real prosecutions.

Lower Quality

Ink vs. Digital

- Ink: Manual acquisition process following the traditional forensic techniques. Latent fingerprints are lifted during real prosecutions.

- Digital: acquired with dedicated sensors. Resolution up to 1000 dots per inch (dpi).

Lower Quality

Higher Quality

Rolled vs. Plain

- Rolled: obtained by rolling a finger from one side to the other (nail-to-nail) in order to capture the whole fingerprint pattern. Rolled fingerprints have larger size and contain more information.

Rolled

Rolled vs. Plain

- Rolled: obtained by rolling a finger from one side to the other (nail-to-nail) in order to capture the whole fingerprint pattern. Rolled fingerprints have larger size and contain more information.

- Plain: the fingers are pressed down on a flat surface, but not rolled. Plain fingerprints contain less information than rolled prints but they have clearer ridge structure and do not present the distortions generated by the rolling of the finger.

Rolled

Plain

Rolled vs. Plain

- Rolled: obtained by rolling a finger from one side to the other (nail-to-nail) in order to capture the whole fingerprint pattern. Rolled fingerprints have larger size and contain more information.

- Plain: the fingers are pressed down on a flat surface, but not rolled. Plain fingerprints contain less information than rolled prints but they have clearer ridge structure and do not present the distortions generated by the rolling of the finger.

Rolled

Plain

Rolled and plain impressions are obtained either by scanning the inked impression on paper, or by directly using livescan devices

Automatic Fingerprint Recognition: Architecture

Input Fingerprint

Automatic Fingerprint Recognition: Architecture

Input Fingerprint

Presentation Attack Detection

Real or **Fake**?

Automatic Fingerprint Recognition: Architecture

Input Fingerprint

Presentation Attack Detection

Real or **Fake**?

Feature Extraction

Automatic Fingerprint Recognition: Architecture

Input Fingerprint

Presentation Attack Detection

Real or Fake?

Feature Extraction

Matching

Identity
Match/Non-match

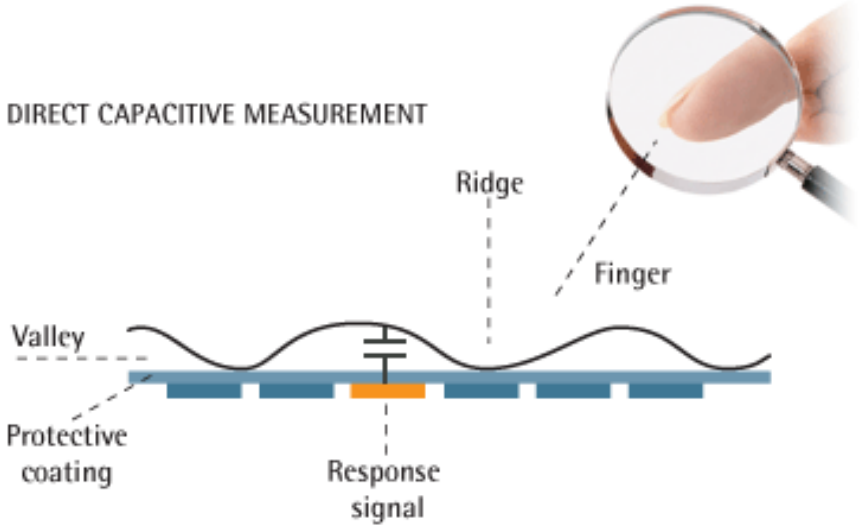
Database

Automatic Fingerprint Recognition: Architecture

Input Fingerprint

Fingerprint Sensors

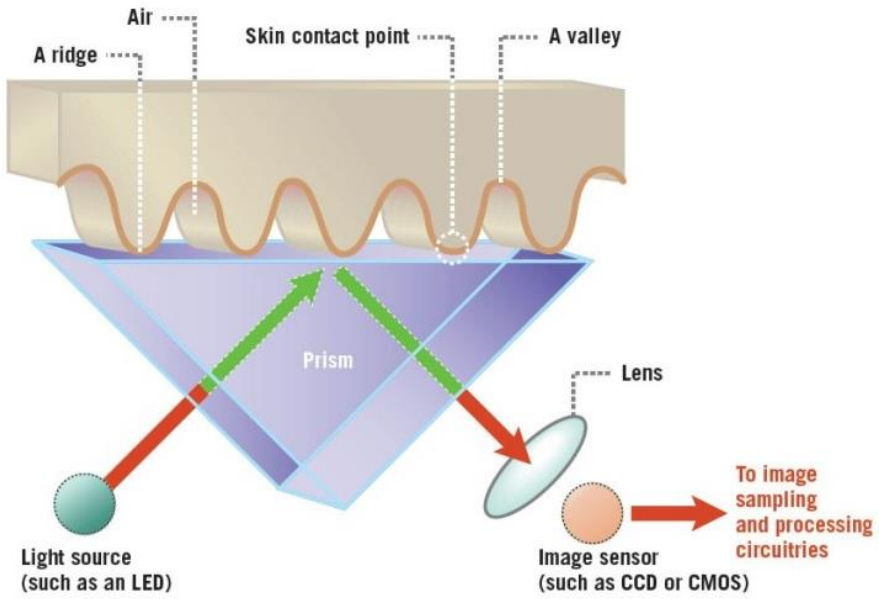
Capacitance: Capacitance sensors use principles associated with capacitance in order to form fingerprint images. In this method of imaging, the sensor array pixels each act as one plate of a parallel-plate capacitor, the dermal layer (which is electrically conductive) acts as the other plate, and the non-conductive epidermal layer acts as a dielectric. It is the simplest type of fingerprint sensor.



Fingerprint Sensors

Optical: Optical fingerprint imaging involves capturing a digital image of the print using visible light. This type of sensor is, in essence, a specialized digital camera.

They capture a 2D image of the fingerprint.

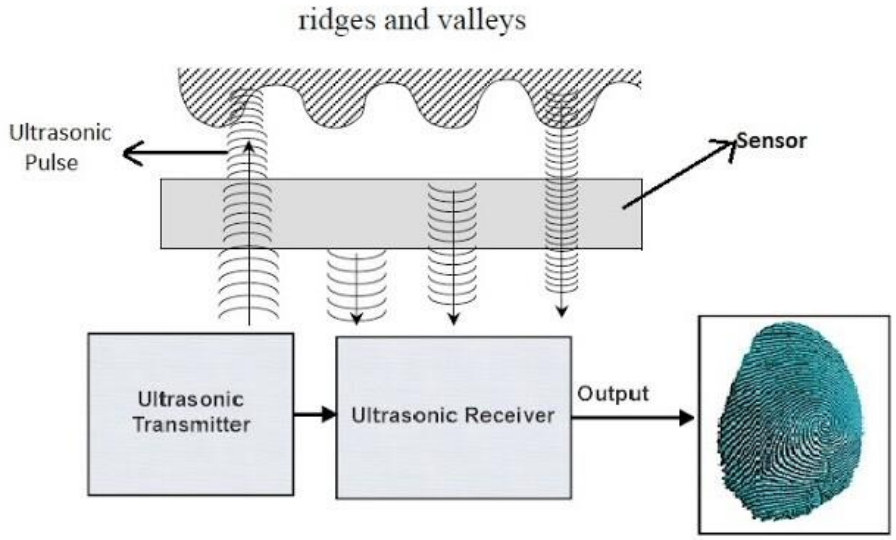


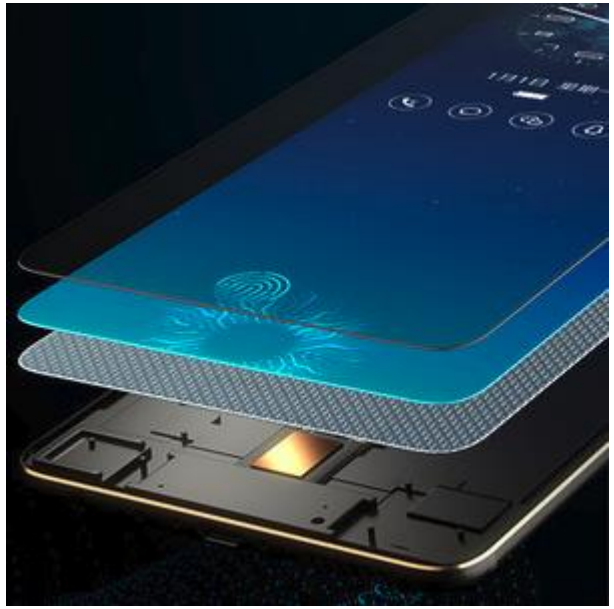
Xiaomi, Oppo, Huawei, etc.

Fingerprint Sensors

Ultrasonic: Ultrasonic sensors make use of the principles of medical ultrasonography in order to create visual images of the fingerprint. Unlike optical imaging, ultrasonic sensors use very high frequency sound waves to penetrate the epidermal layer of skin.

They capture a 3D image of the fingerprint.





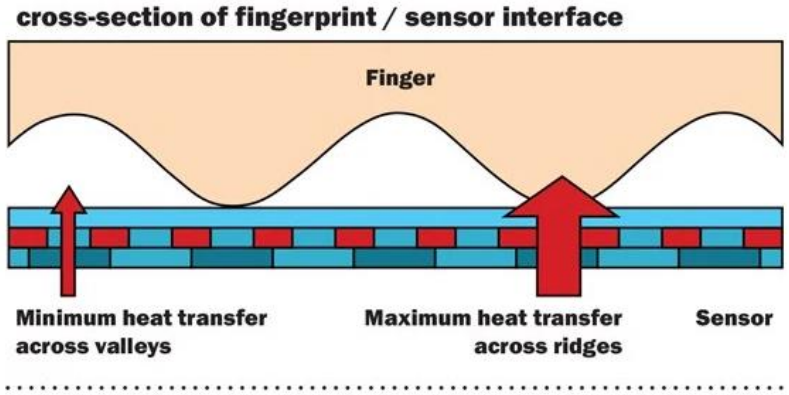
Samsung Galaxy S10 (Qualcomm sensor)

Fingerprint Sensors

Thermal: Thermal fingerprint sensors measure the temperature differential between the sensor pixels that are in contact with the ridges and those under the valleys, that are not in contact.

It is difficult to spoof using fake fingerprints.

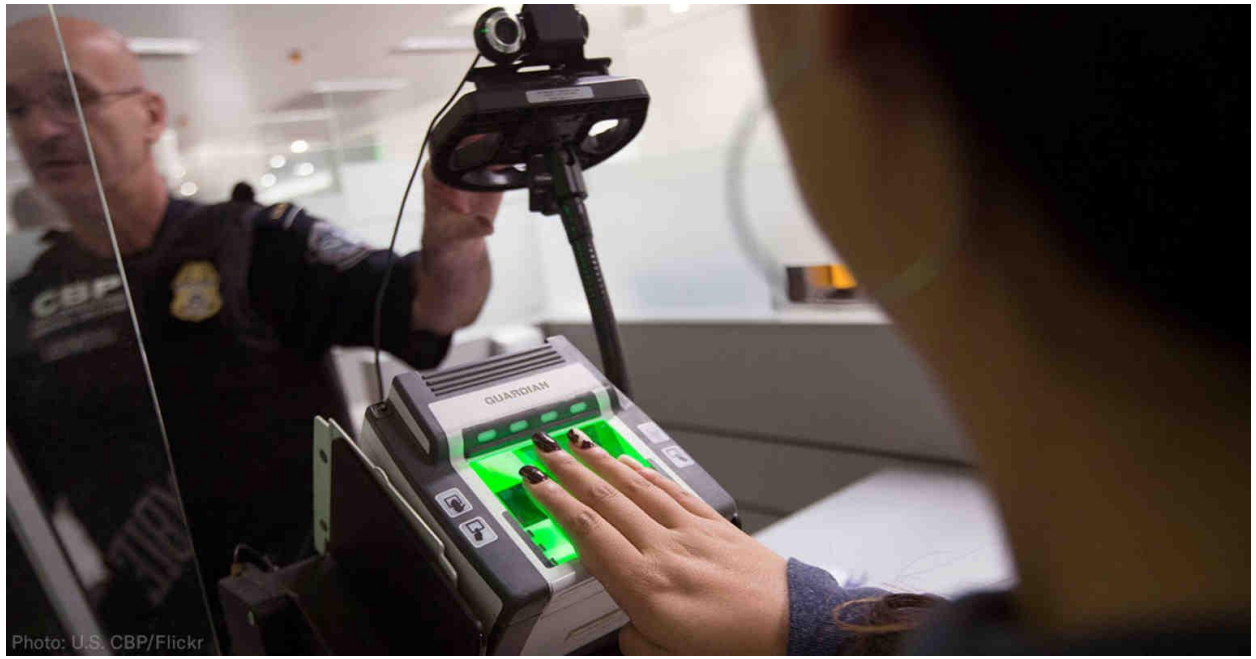
Limitations: the image disappears very quickly. The image vanishes because the finger and the pixel array have reached thermal equilibrium.



Atmel AT77C101B

Sensor Technologies

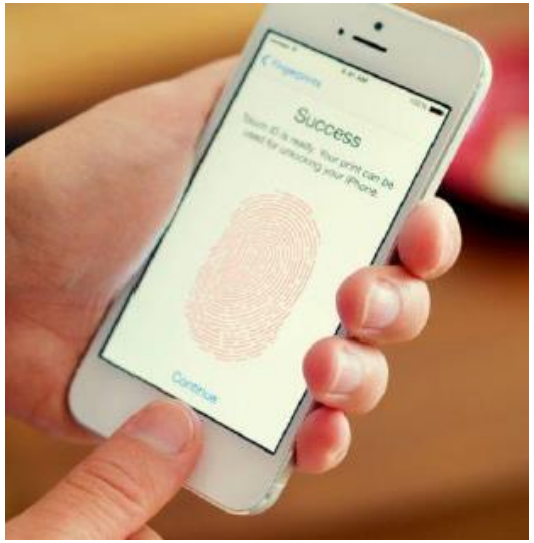
AFIS/APIS: Automatic Fingerprint/Palmprint Identification Systems enable creating, storing and functioning of electronic databases of fingerprint, palmprint and latent records.

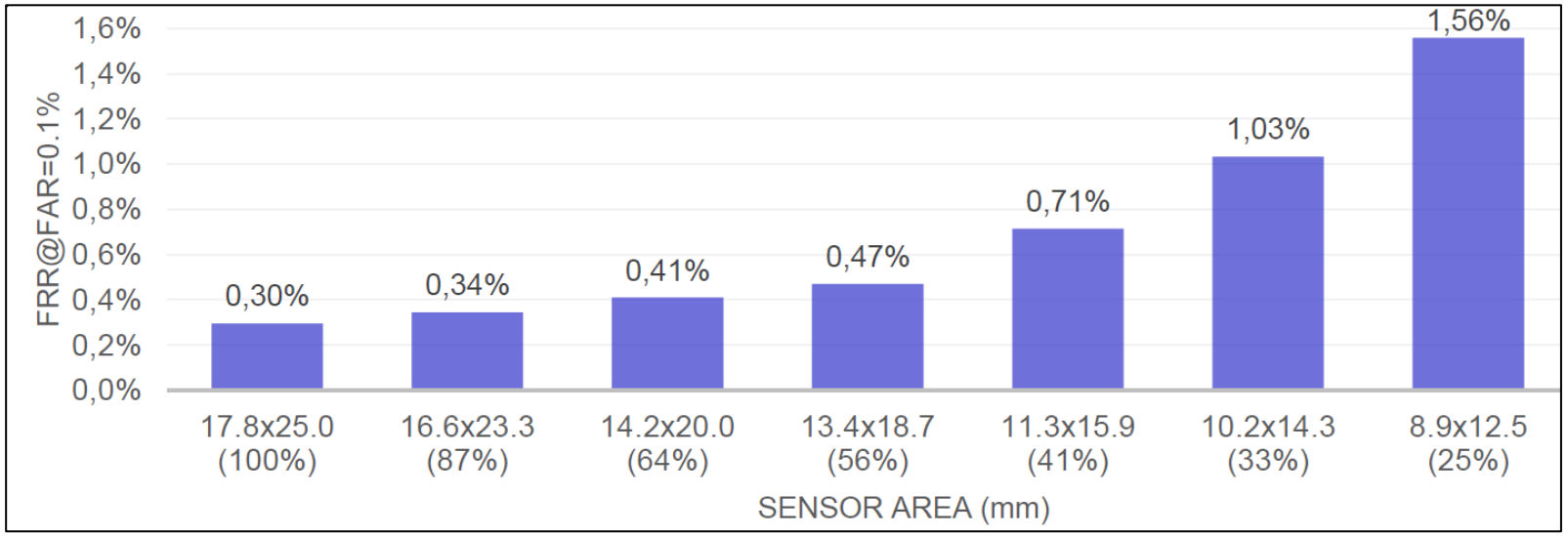


Law enforcement, border control and criminal investigation.

Fingerprint Sensors

Problems with small area sensors: Comparing small patches increases the risk of false matches.





- A. K. Hrechak, and J. A. McHugh, “Automated fingerprint recognition using structural matching,” Pattern Recognition, 23(8), 893-904, 1990.
- A. Roy, N. Memon and A. Ross, “Masterprint: Exploring the vulnerability of partial fingerprint-based authentication systems” IEEE Transactions on Information Forensics and Security, 12(9), 2013-2025, 2017.

Image Quality

Low quality fingerprints:

- Scarcely prominent ridge lines (manual workers, elderly people).
- Too dry or wet fingerprints.

Good Quality

Dry Fingerprint

Wet Fingerprint

Intrinsically low quality image

Image Quality

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Fingerprint Image Quality (NFIQ) is the *facto standard* to quantify fingerprint quality (open source).

- NFIQ (1.0): assigns to a fingerprint a value in {1,2,3,4,5} which is in inverse proportion with its quality.

Image Quality

National Institute of Standards and Technology
U.S. Department of Commerce

Quality/Accuracy Tradeoff:

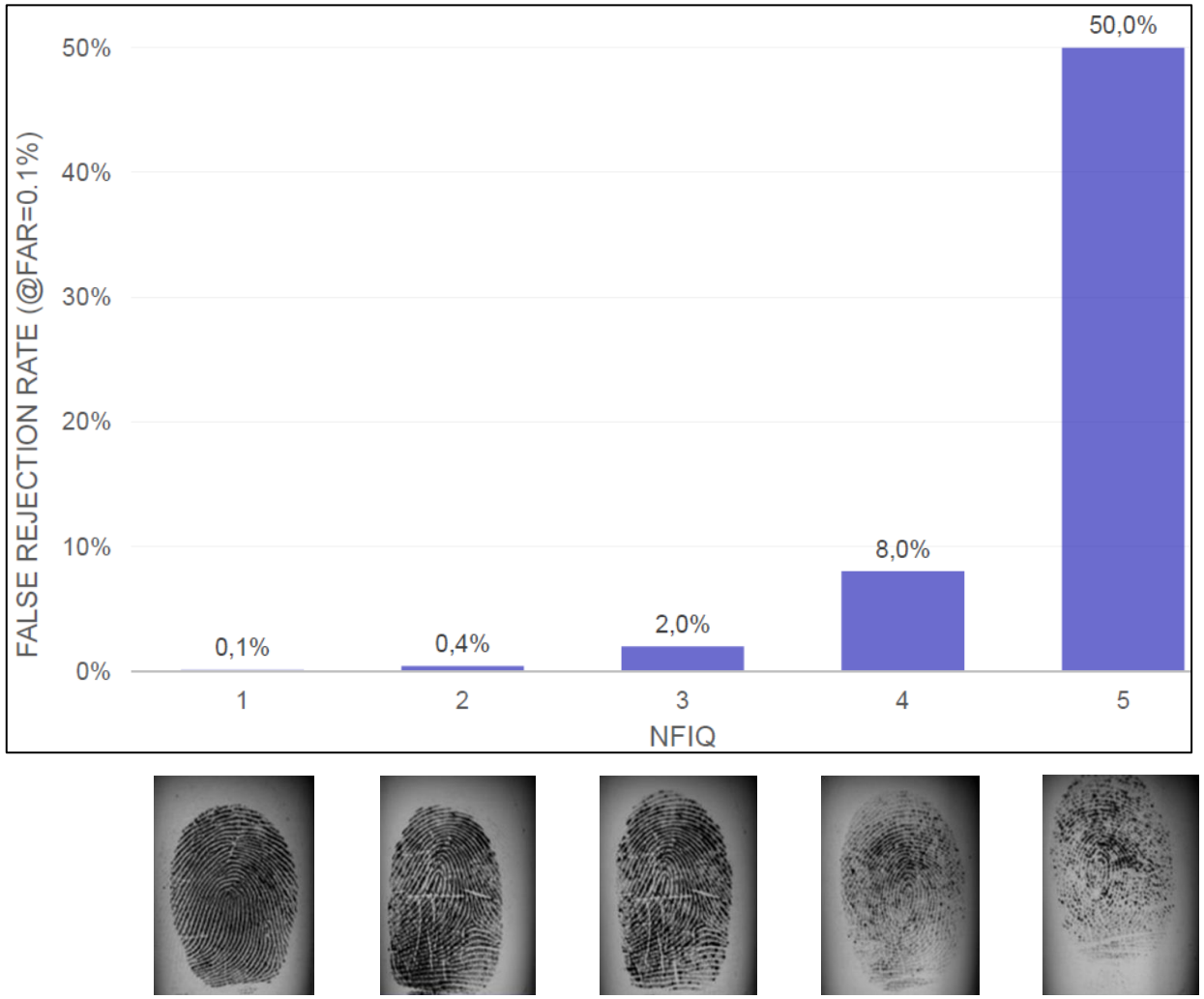
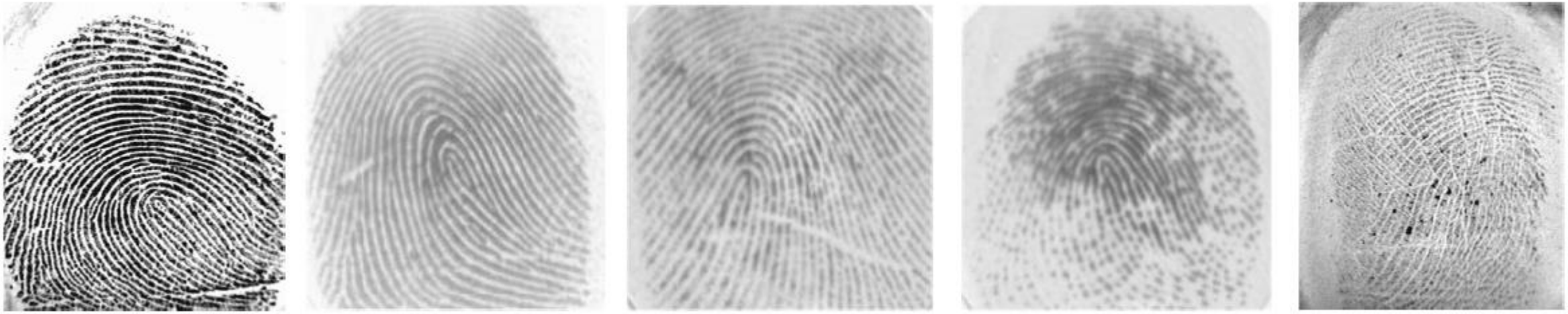


Image Quality

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Fingerprint Image Quality (NFIQ) is the *facto standard* to quantify fingerprint quality (open source).

- NFIQ (2.0): assigns to a fingerprint a value in [0...100] which is in direct proportion with its quality.
  - Quality features: 155 evaluated, 14 selected (e.g., orientation, ridge valley uniformity, etc.).



- Code: https://www.nist.gov/services-resources/software/development-nfiq-20

Automatic Fingerprint Recognition: Architecture

Input Fingerprint

Presentation Attack Detection

Real or **Fake**?

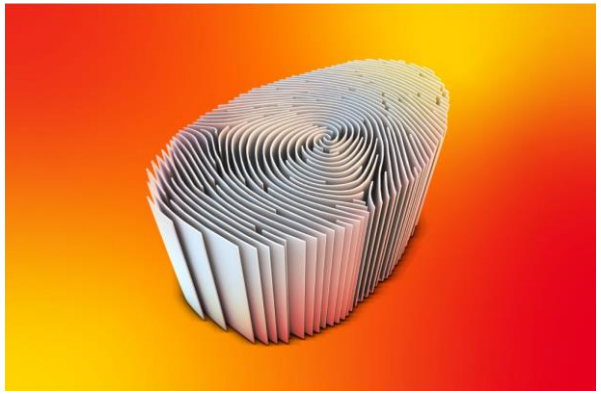
Presentation Attack Detection

Samsung Galaxy S10 fingerprint sensor defeated by a $450 3D printer

Need to fool a 3D fingerprint sensor? Use a 3D printer.

RON AMADEO - 4/8/2019, 5:24 PM

3D Fingerprint model!



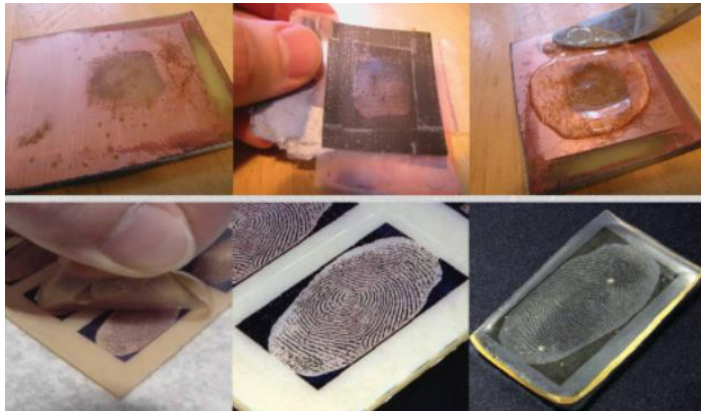
- URL: https://arstechnica.com/gadgets/2019/04/samsung-galaxy-s10-fingerprint-sensor-defeated-by-a-450-3d-printer/

Presentation Attack Detection

Detection of attacks from real fingerprints.

Gelatin

Residual fingerprint using PCV



Latex

Photo/Scanning

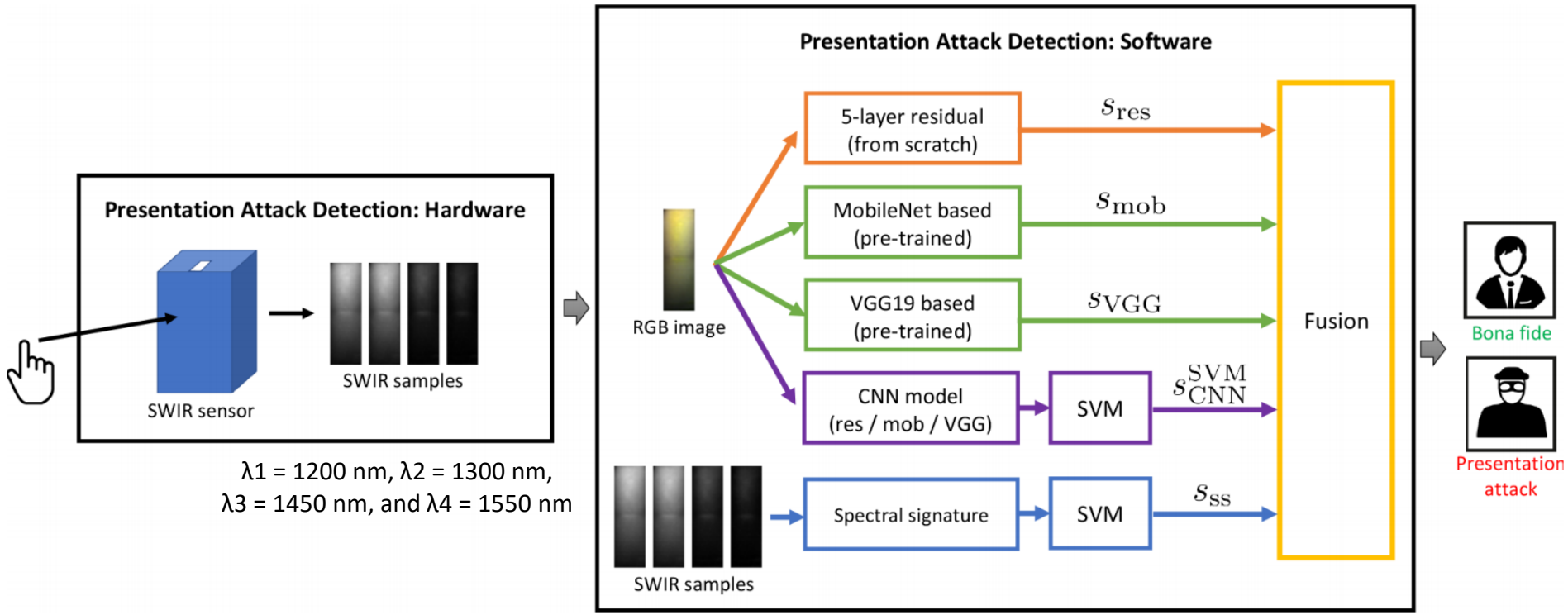
- R. Tolosana, M. Gomez-Barrero, C. Busch and J. Ortega-Garcia, “Biometric presentation attack detection: Beyond the visible spectrum”, IEEE Transactions on Information Forensics and Security, vol 15, pp. 1261-1275, 2019.
- C. Sousedik and C. Busch, “Presentation attack detection methods for fingerprint recognition systems: a survey", IET Biometrics, vol. 3, pp. 219–233, 2014.
- E. Marasco and A. Ross, “A survey on antispoofing schemes for fingerprint recognition systems", ACM Computing Surveys, 2015

Presentation Attack Detection

BiDA Lab
Biometrics & Data Pattern Analytics Lab

Beyond the visible spectrum: Short-Wave Infrared Sensor.

- Detection of skin and non-skin materials.



- R. Tolosana, M. Gomez-Barrero, C. Busch and J. Ortega-Garcia, "Biometric presentation attack detection: Beyond the visible spectrum", IEEE Transactions on Information Forensics and Security, vol 15, pp. 1261-1275, 2019.

Presentation Attack Detection

BiDA Lab
Biometrics & Data Pattern Analytics Lab

Attacks (PAI): 35 types

PAI Group	PAI Species
Dragon Skin	Finger, conductive, conductive nanotips white, graphite
Latex	Finger
Overlay	Conductive silicone, monster latex, glue, silicone, urethane, wax, dragon skin
Playdoh	Black, blue, green, orange, pink, purple, red, teal, yellow
Printed	2D photograph/matte paper, 3D normal/Ag paint,
Silicone	Barepaint coating, finger flesh/yellow, graphite, normal, coating
Silly Putty	Glow in the dark, normal, metallic
Wax	Finger

Unseen attacks (not considered for training)

- R. Tolosana, M. Gomez-Barrero, C. Busch and J. Ortega-Garcia, “Biometric presentation attack detection: Beyond the visible spectrum”, IEEE Transactions on Information Forensics and Security, vol 15, pp. 1261-1275, 2019.

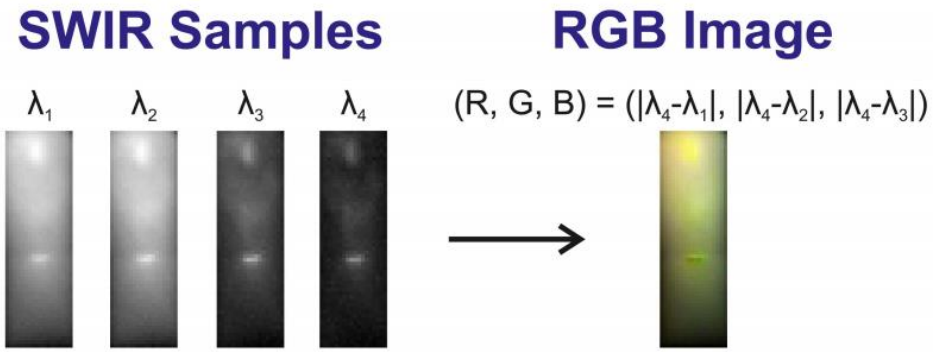
Presentation Attack Detection

BiDA Lab
Biometrics & Data Pattern Analytics Lab

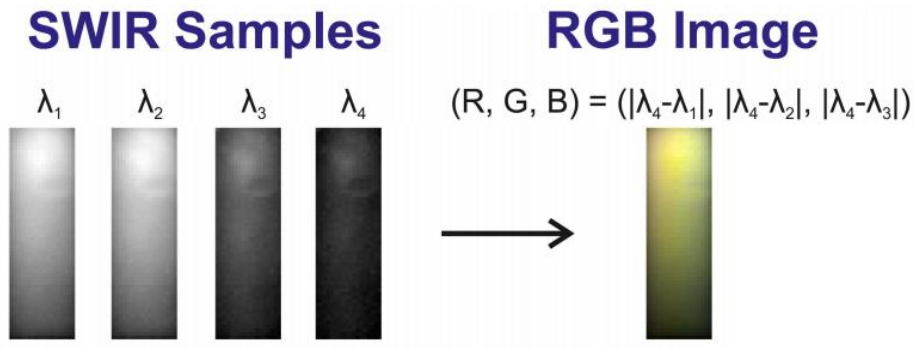
Attacks (PAI): 35 types

PAI Group	PAI Species
Dragon Skin	Finger, conductive, conductive nanotips white, graphite
Latex	Finger
Overlay	Conductive silicone, monster latex, glue, silicone, urethane, wax, dragon skin
Playdoh	Black, blue, green, orange, pink, purple, red, teal, yellow
Printed	2D photograph/matte paper, 3D normal/Ag paint,
Silicone	Barepaint coating, finger flesh/yellow, graphite, normal, coating
Silly Putty	Glow in the dark, normal, metallic
Wax	Finger

Unseen attacks (not considered for training)



Real Fingerprint



Attack: Playdoh

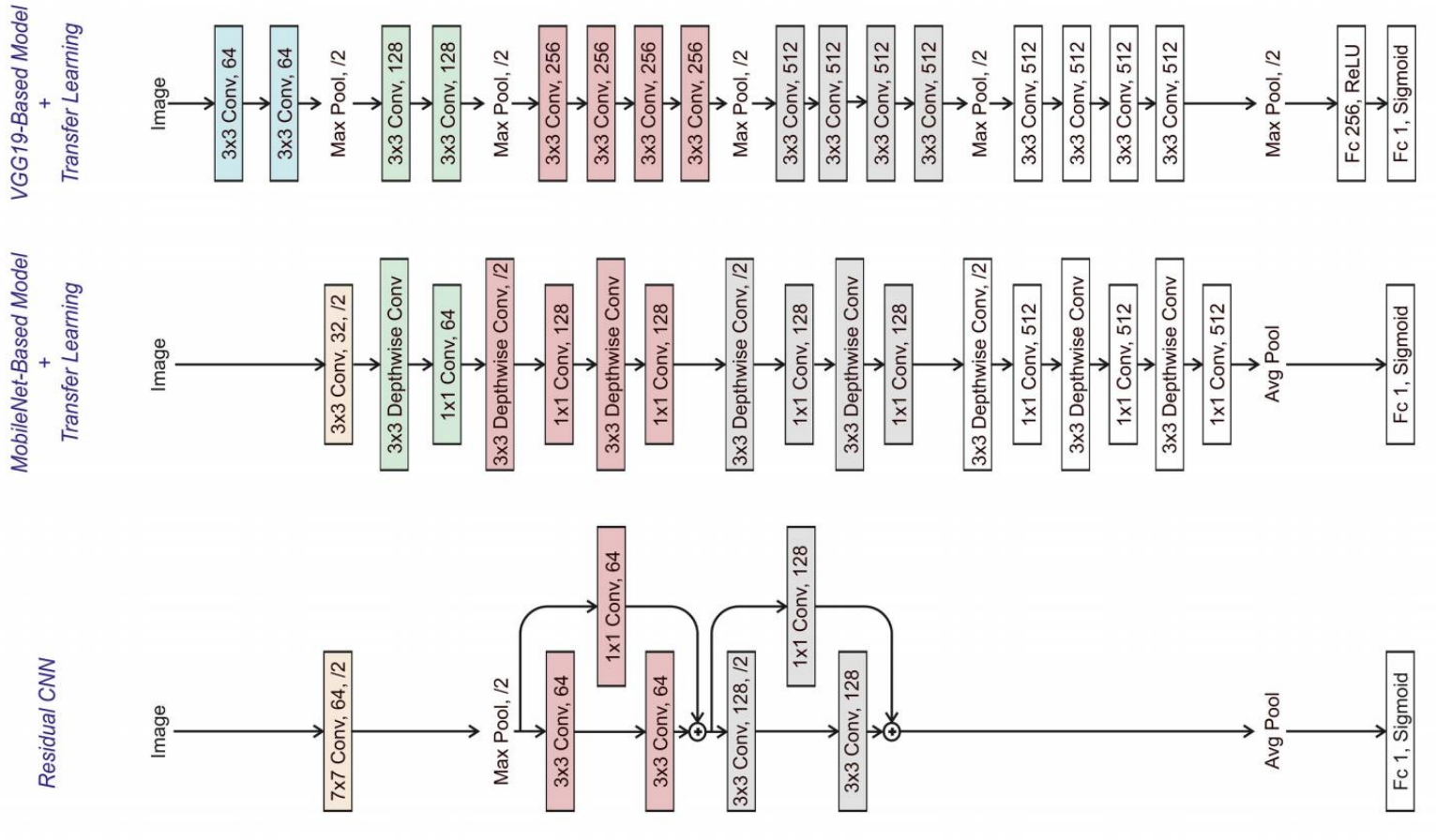
- R. Tolosana, M. Gomez-Barrero, C. Busch and J. Ortega-Garcia, "Biometric presentation attack detection: Beyond the visible spectrum", IEEE Transactions on Information Forensics and Security, vol 15, pp. 1261-1275, 2019.

Presentation Attack Detection

BiDA Lab
Biometrics & Data Pattern Analytics Lab

Presentation Attack Detection System.

- Handcrafted features (pixel normalized values + SVM).
- Deep learning features:
  - Trained from scratch and using pre-trained models (ImageNet) + transfer learning.

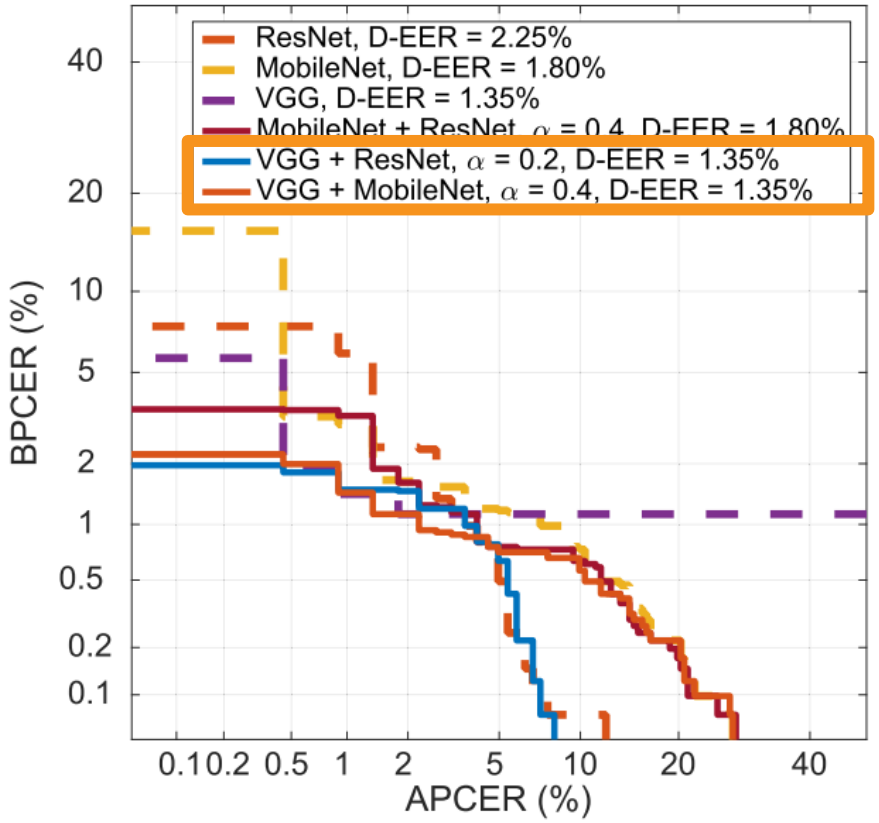


Presentation Attack Detection

BiDA Lab
Biometrics & Data Pattern Analytics Lab

Results on BATL research project (USA IARPA):

- Error results close to 1% (even considering unknown attacks!).



- R. Tolosana, M. Gomez-Barrero, C. Busch and J. Ortega-Garcia, “Biometric presentation attack detection: Beyond the visible spectrum”, IEEE Transactions on Information Forensics and Security, vol 15, pp. 1261-1275, 2019.

Automatic Fingerprint Recognition: Architecture

Input Fingerprint

Presentation Attack Detection

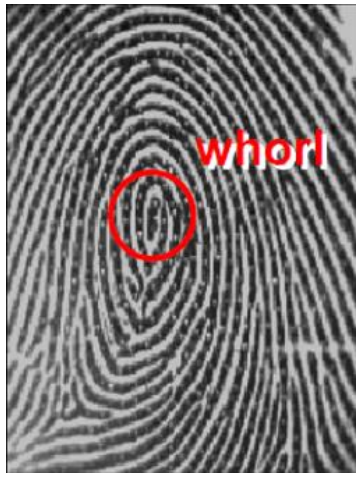
Real or **Fake**?

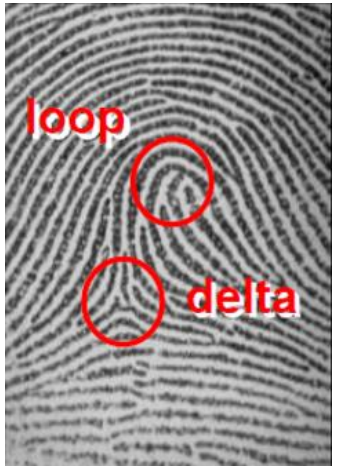
Feature Extraction

Fingerprint Anatomy (Level 1-2)

A fingerprint is composed of a set of lines (ridge lines), which mainly flow parallel, making a pattern (ridge pattern).

Sometimes the ridge lines produce local macro-singularities, called whorl (O), loop (U), and delta (Δ).



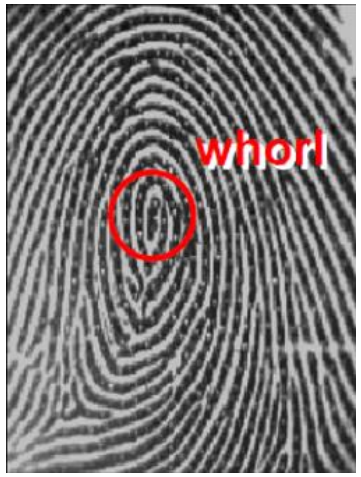


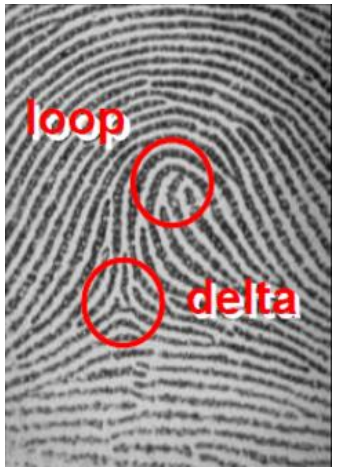
Fingerprint Anatomy (Level 1-2)

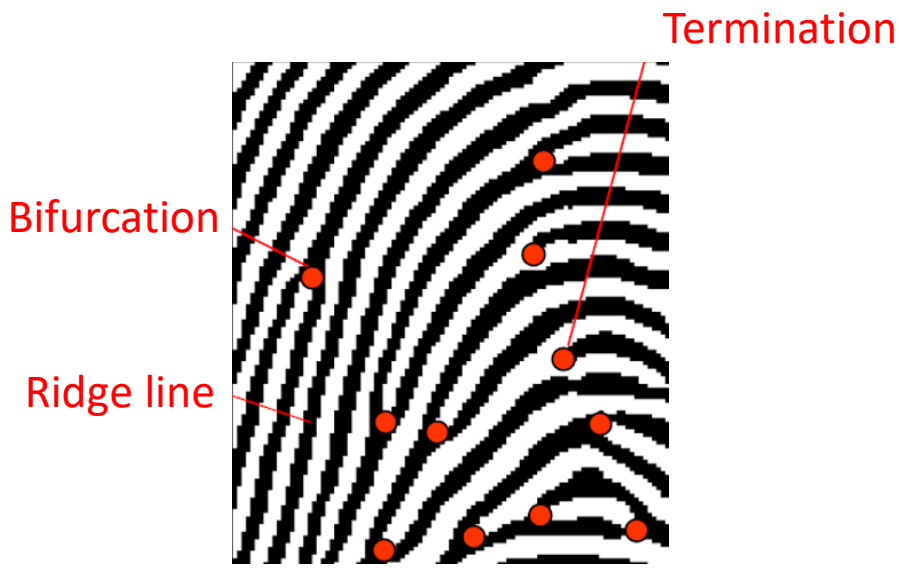
A fingerprint is composed of a set of lines (ridge lines), which mainly flow parallel, making a pattern (ridge pattern).

Sometimes the ridge lines produce local macro-singularities, called whorl (O), loop (U), and delta (Δ).

The minutiae, or Galton's characteristics, are determined by the termination or the bifurcation of the ridge lines

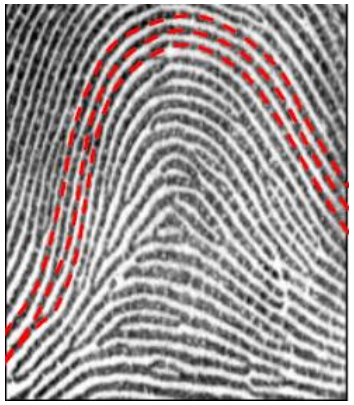






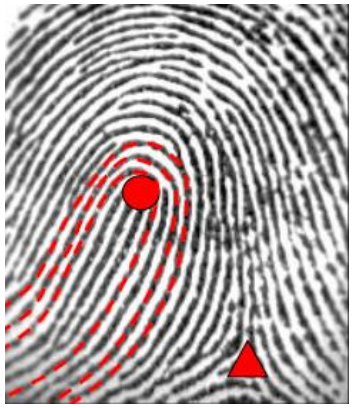
Fingerprint Anatomy (Level 1-2)

The five main fingerprint classes:



Arch

Tented Arch



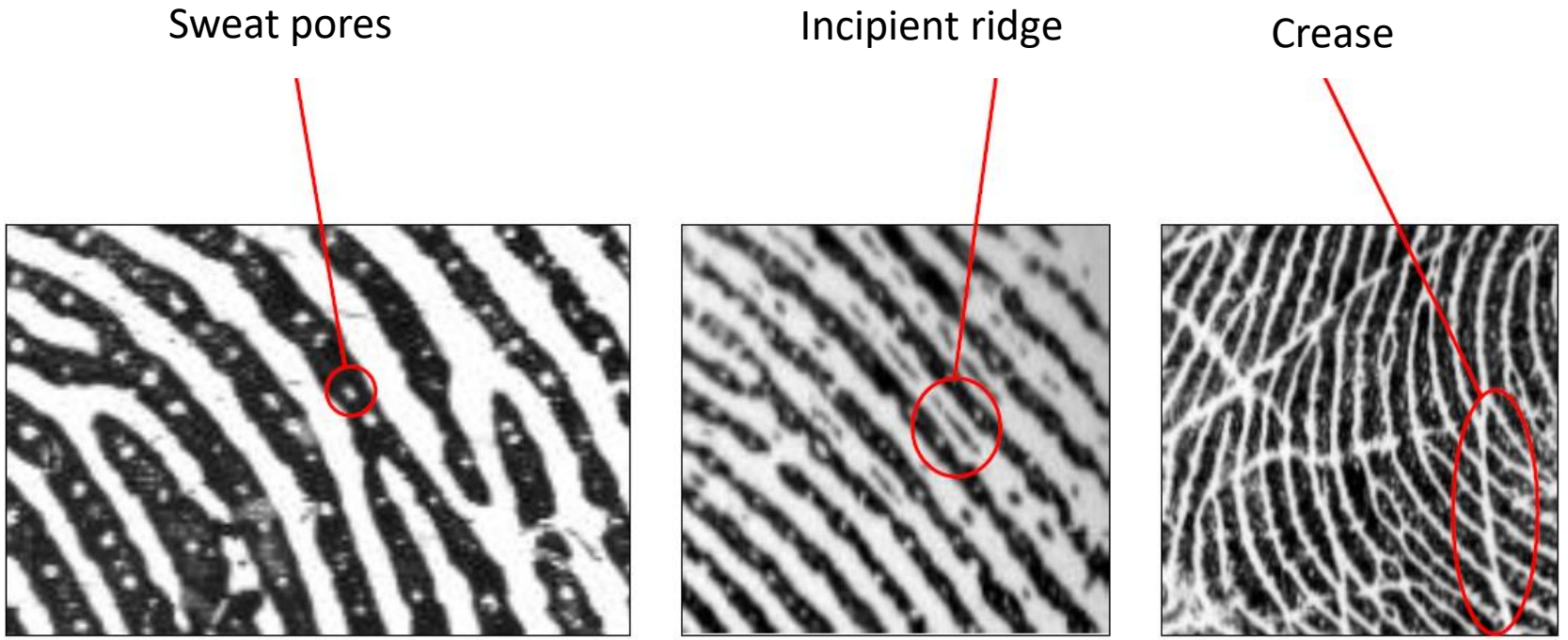
Left Loop

Right Loop

Whorl

Fingerprint Anatomy (Level 3)

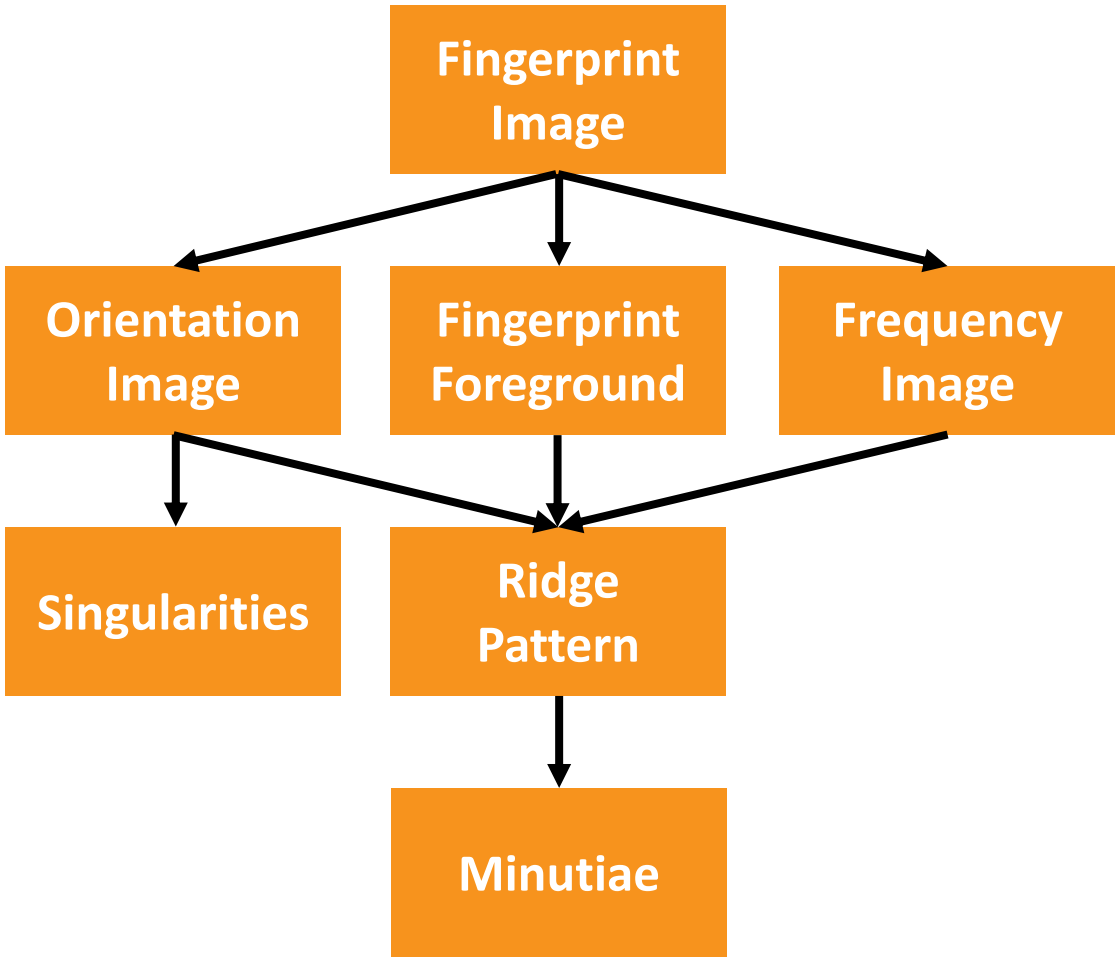
At the very local level (e.g., acquisition at 1000 dpi), it is possible to identify sweat pores (from 60 to 250µm), incipient ridges, creases, etc.



Feature Extraction

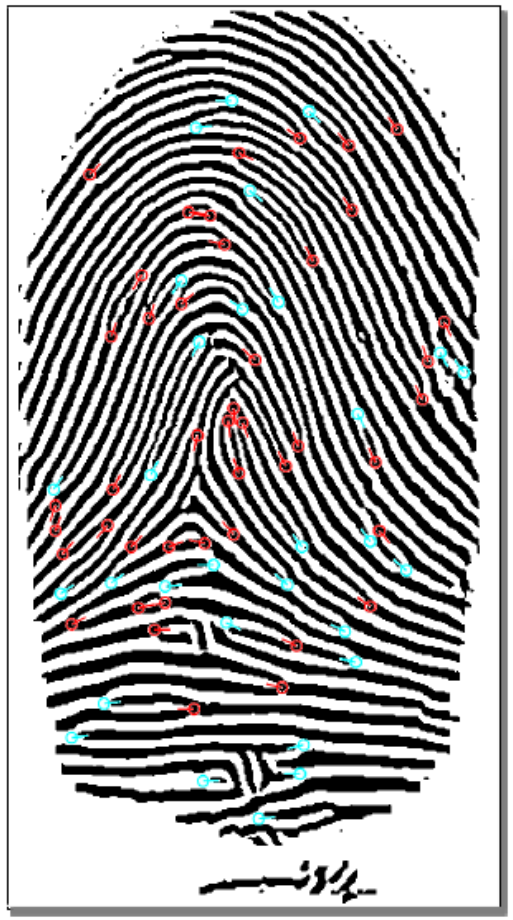
Fingerprint Image

Minutiae

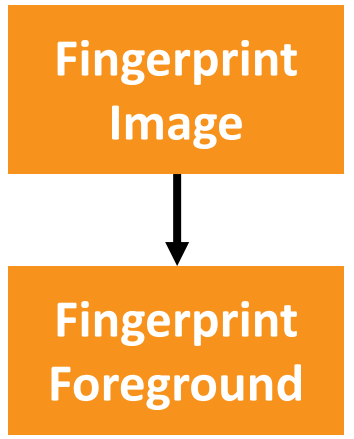


Feature Extraction

Fingerprint Image



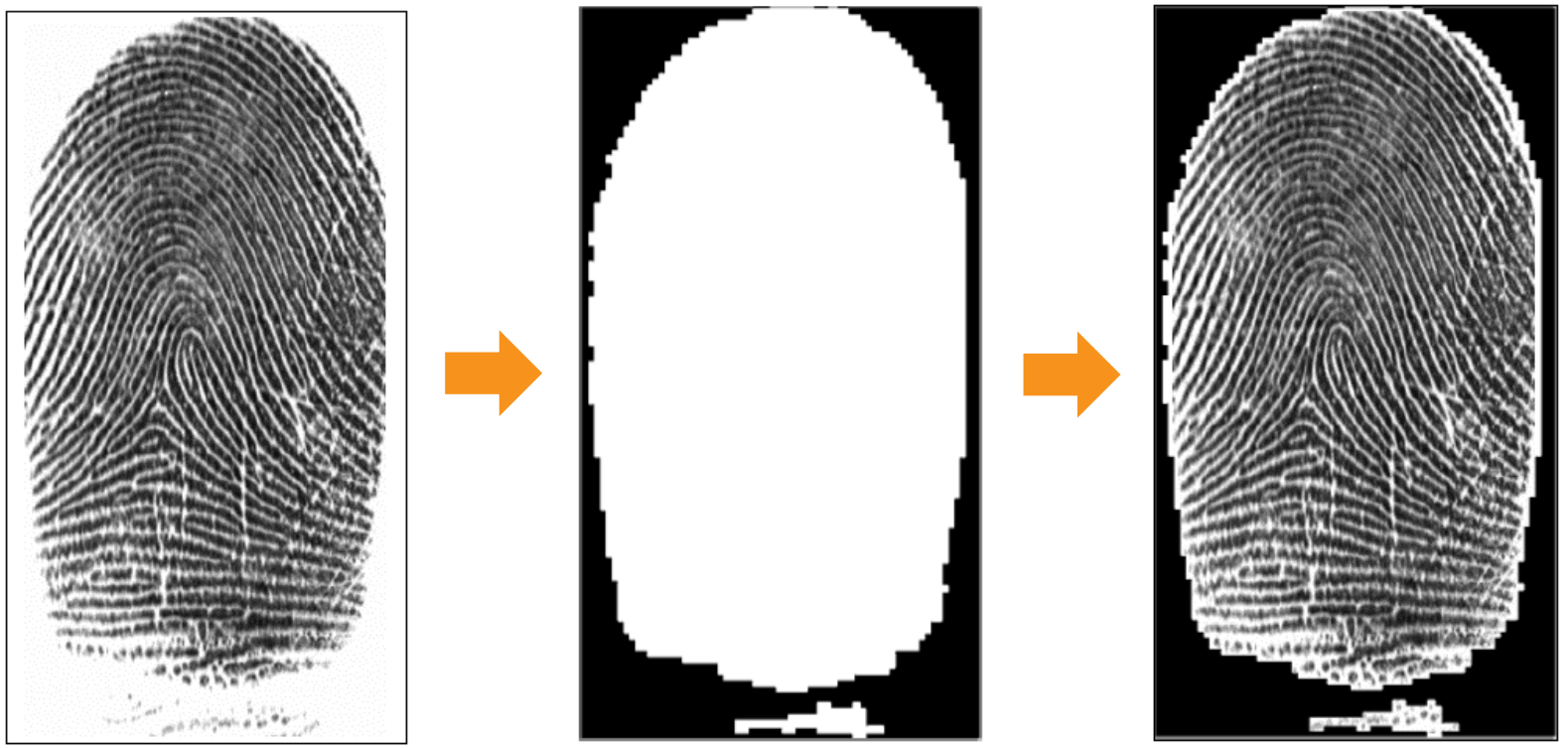
Minutiae



Fingerprint Foreground

The segmentation stage is aimed to separate the fingerprint area (foreground) from the image background.

Foreground is characterized by the presence of a striped and oriented pattern. Background presents a uniform pattern.

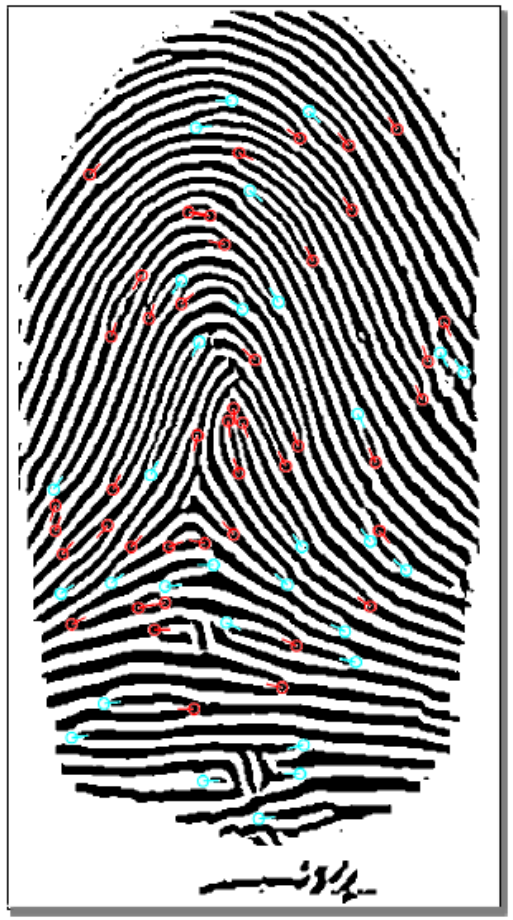


Fingerprint Image

Fingerprint Foreground

Feature Extraction

Fingerprint Image



Minutiae

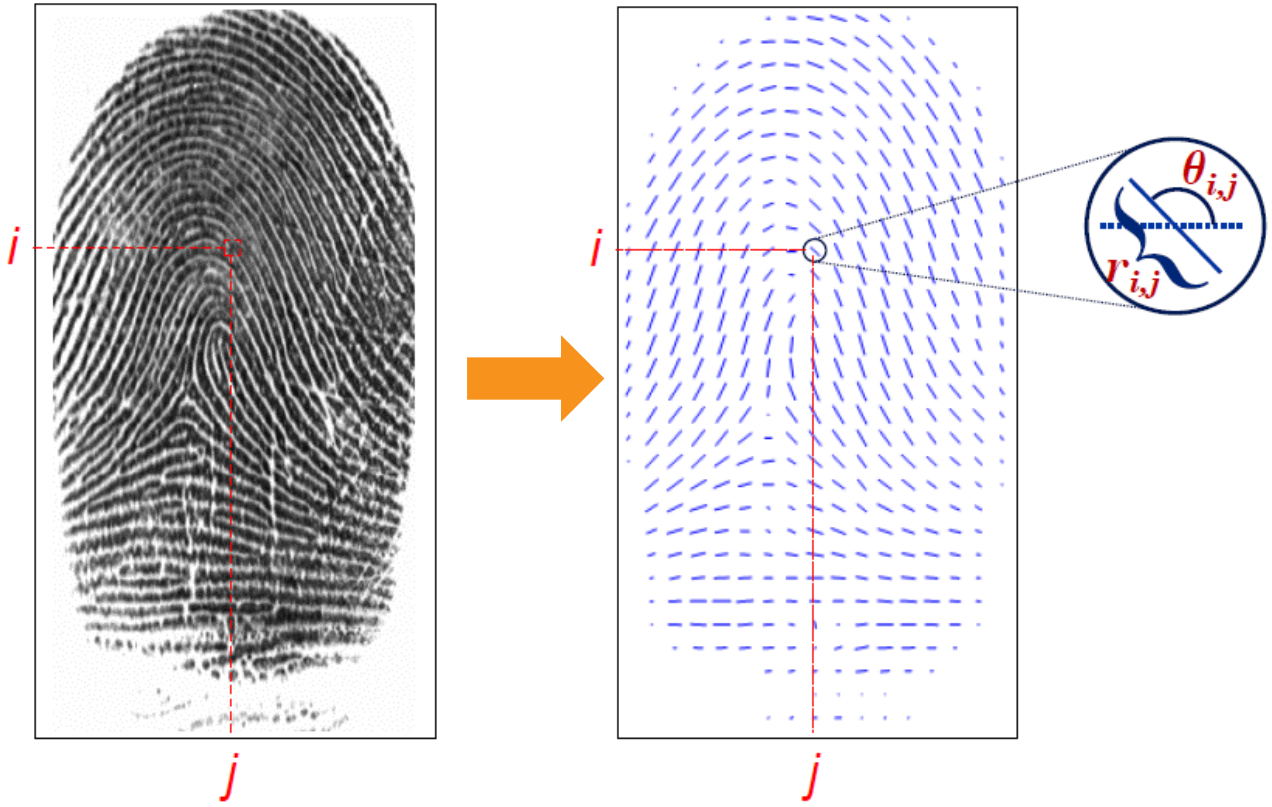
Fingerprint Image

Orientation Image

Orientation Image

The local ridge orientation at $[i,j]$ is the angle $\theta ij \in [0,180°]$ that the fingerprint ridges form with the horizontal axis in an arbitrary small neighborhood centered at $[i,j]$.

The simplest approach to extract local ridge orientations is based on computation of gradient phase angles.

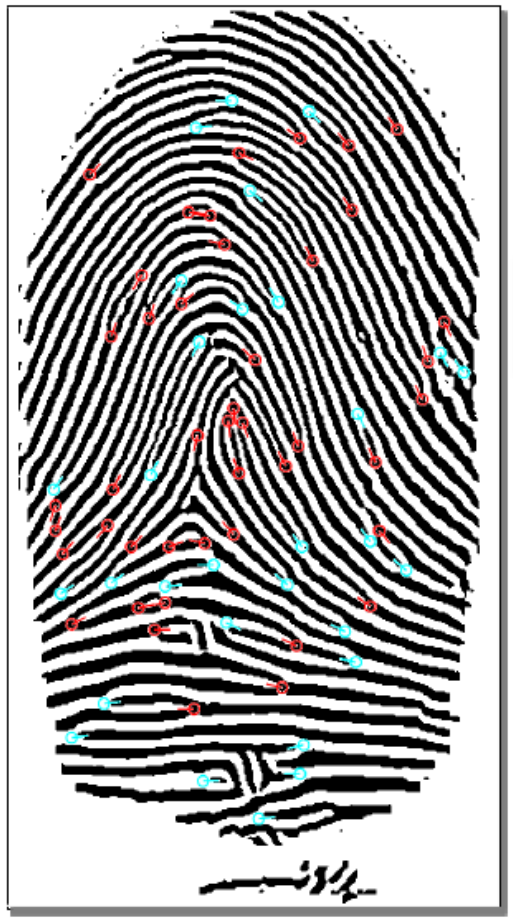


Fingerprint Image

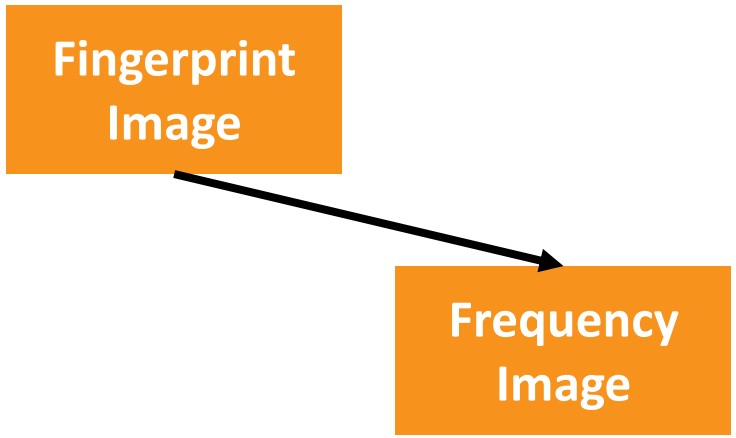
Orientation Image

Feature Extraction

Fingerprint Image



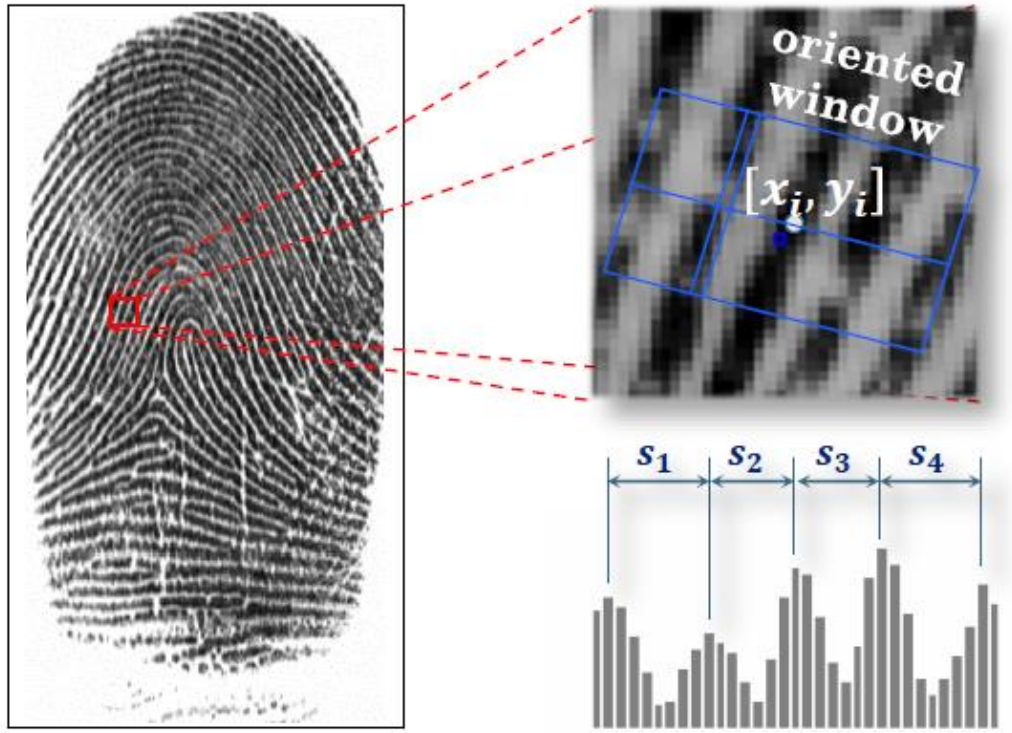
Minutiae



Frequency Image

The local ridge frequency fxy at $[x, y]$ is the number of ridges per unit length along a hypothetical segment centered at $[x, y]$ and orthogonal to the local ridge orientation θxy.

A possible approach is to count the average number of pixels between two consecutive peaks of gray-levels along the direction normal to the local ridge orientation.

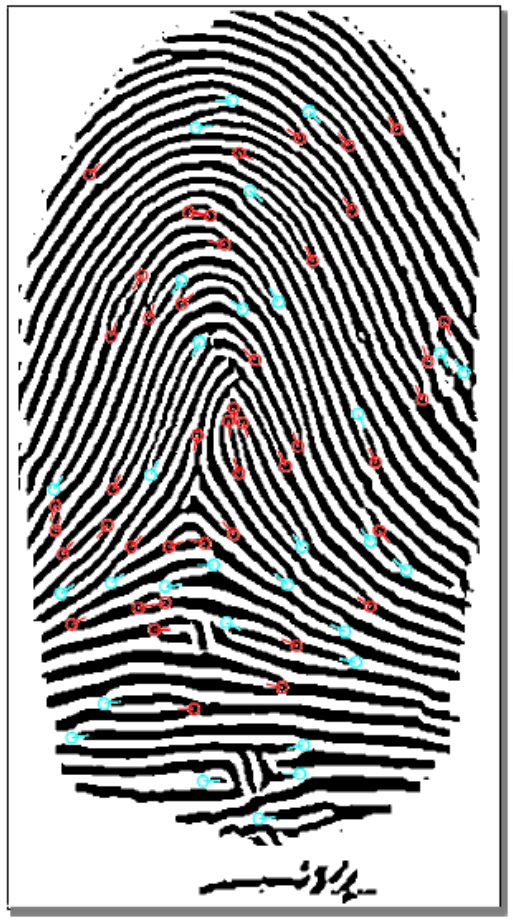


Fingerprint Image

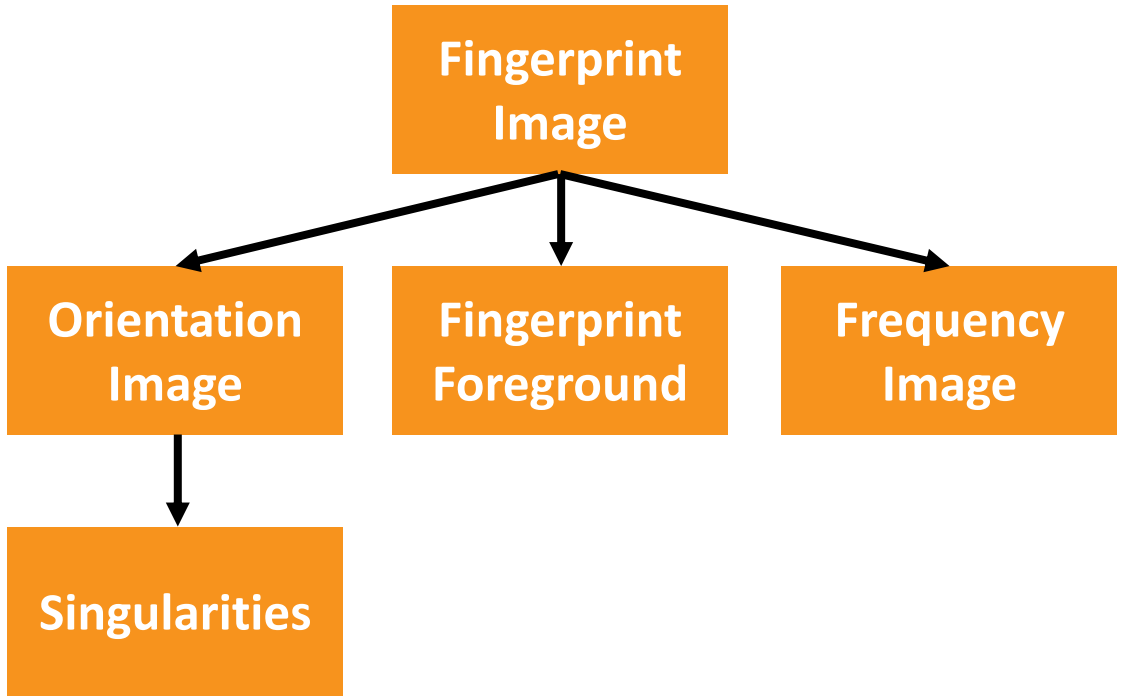
Frequency Image

Feature Extraction

Fingerprint Image

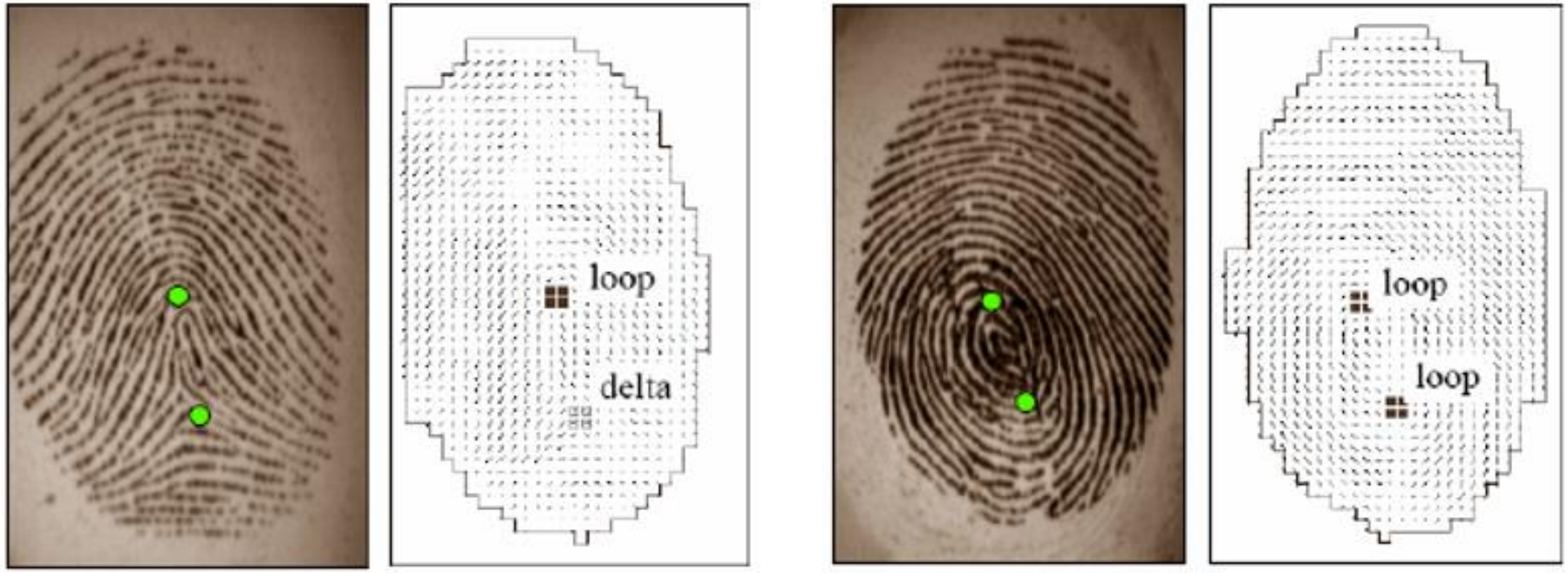


Minutiae



Singularities

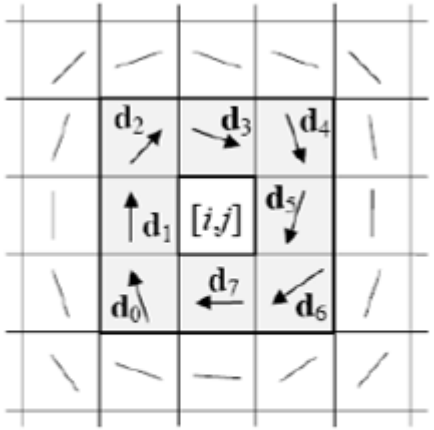
Detection of macro-singularities such as whorl (O), loop (U), and delta (Δ) using the orientation image.



Singularities

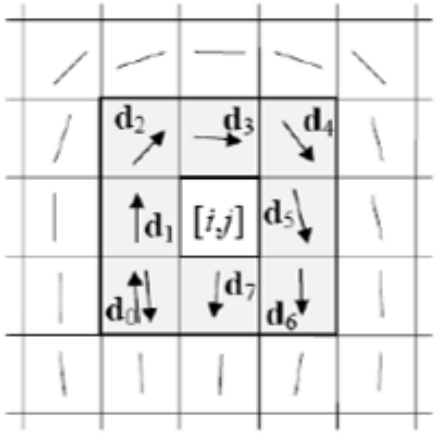
Popular Method: The Poincaré index $P_{G,C}(i,j)$ at $[i,j]$ is computed as:

- The closed curve C, is an ordered sequence of orientations, such that $[i,j]$, is an internal point.
- $P_{G,C}(i,j)$ is computed by algebraically summing the orientation differences between adjacent elements of C. Summing orientation differences requires a direction (among two possible) to be associated at each orientation.
- The orientation image is divided into 32 x 32 subregions.



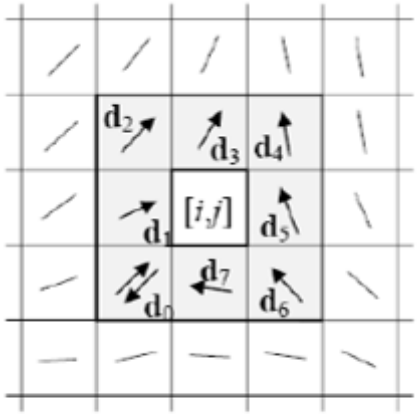
$P_{G,C}(i,j) = 360°$

whorl



$P_{G,C}(i,j) = 180°$

loop



$P_{G,C}(i,j) = -180°$

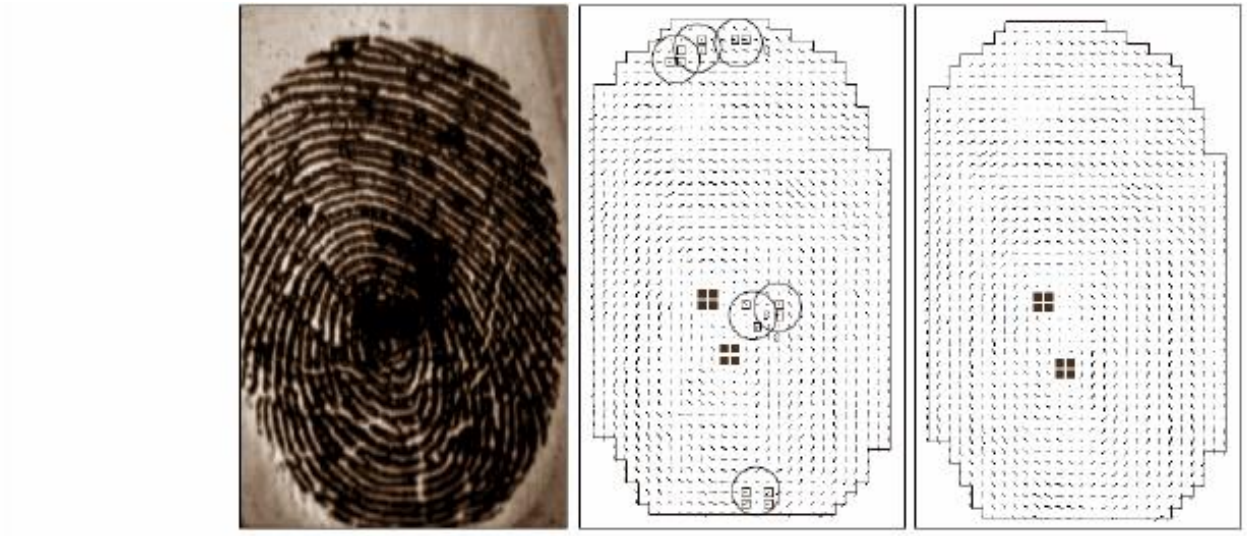
delta

- M. Kawagoe and A. Tojo, “Fingerprint pattern classification,” Pattern recognition, 17(3), 295-303, 1984.

Singularities

Popular Method: The Poincaré index $P_{G,C}(i,j)$ at $[i,j]$ is computed as:

- The closed curve C, is an ordered sequence of orientations, such that $[i,j]$, is an internal point.
- $P_{G,C}(i,j)$ is computed by algebraically summing the orientation differences between adjacent elements of C. Summing orientation differences requires a direction (among two possible) to be associated at each orientation.
- The orientation image is divided into 32 x 32 subregions.



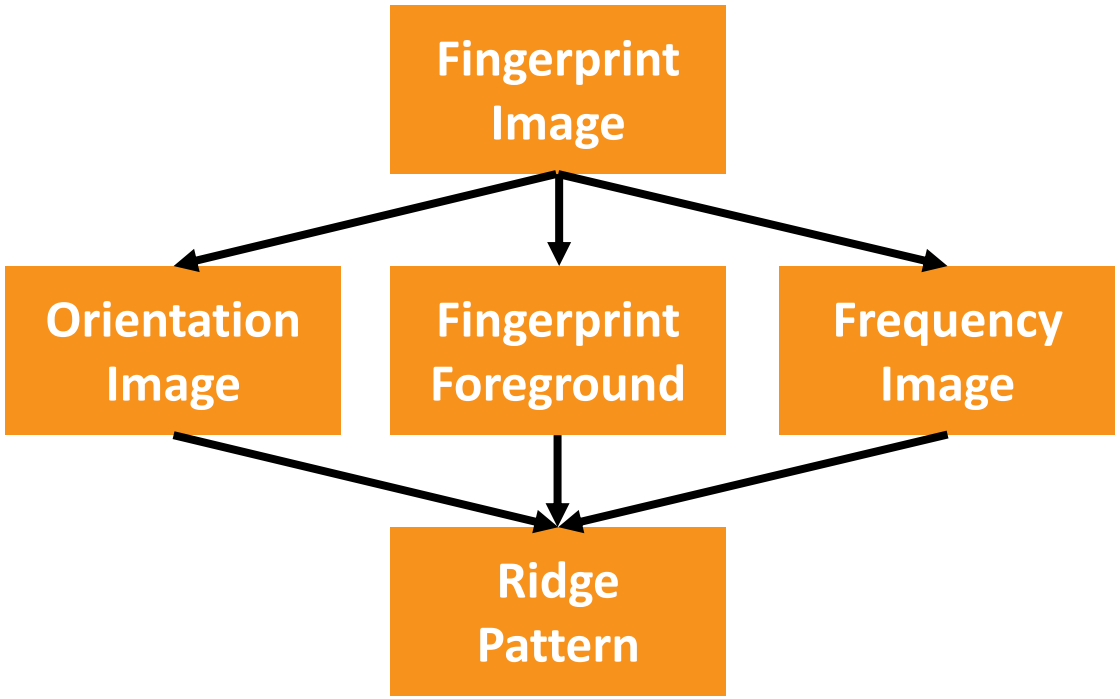
Smoothing is necessary to avoid singularity errors

- M. Kawagoe and A. Tojo, “Fingerprint pattern classification,” Pattern recognition, 17(3), 295-303, 1984.

Feature Extraction

Fingerprint Image

Minutiae



Ridge Pattern

Traditional approach:

- Enhancement/binarization: conversion into a binary image.
- Thinning: the binary image is submitted to a thinning stage aimed to reduce the ridge thickness to one pixel.

Fingerprint Image

Enhancement/Binarization

Thinning

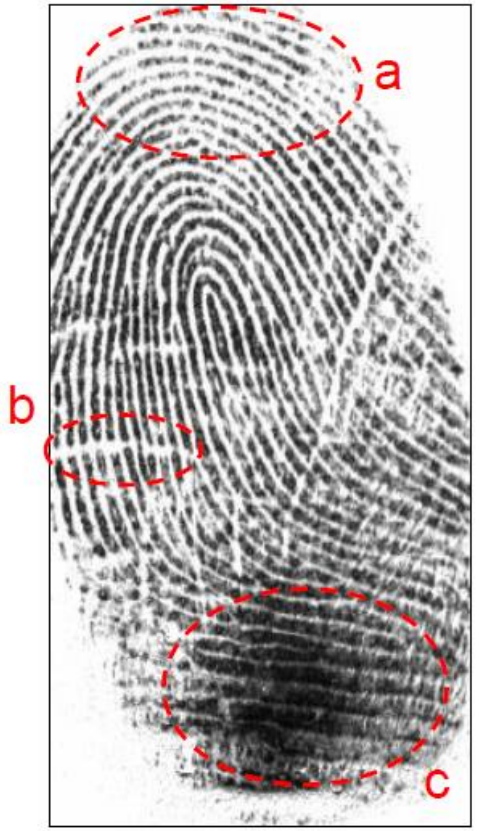
Enhancement

The performance of the feature extraction and comparison algorithms are strictly related to the image quality.

The objective of the enhancement techniques is to improve the fingerprint image quality.

Typical degradations:

a) Ridge lines are not continuous.
b) Cuts, creases, and bruises on the finger.
c) Parallel ridges are not well separated.



The most widely used technique for fingerprint enhancement is based on contextual filters.

In contextual filtering, the characteristics of the filter used change according to the local context.

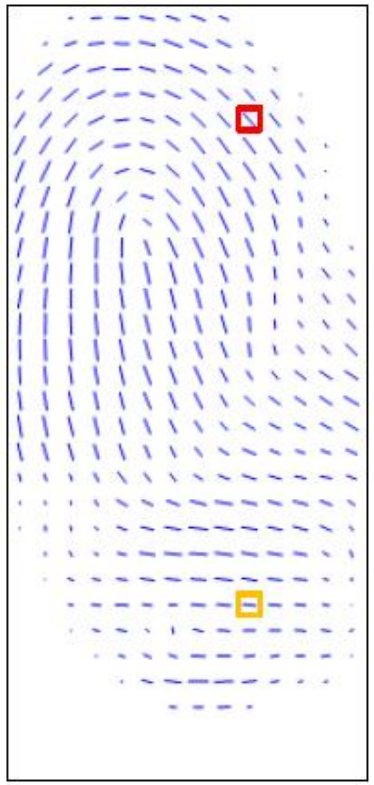
Enhancement

The local context of a fingerprint is represented by the ridge orientation and frequency.

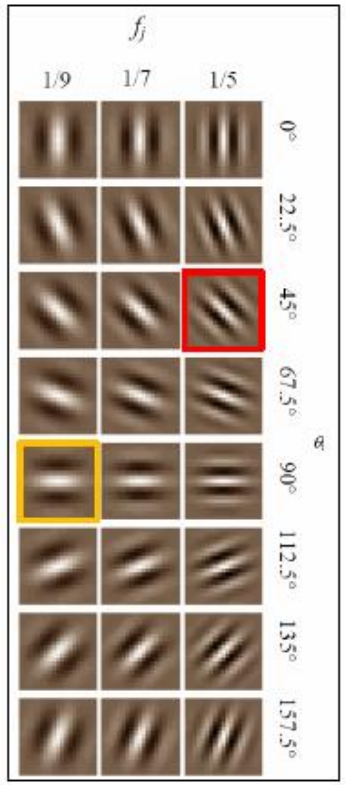
Gabor Filter: sinusoidal plane wave tapered by a Gaussian.

Fingerprint Image

Frequency Image



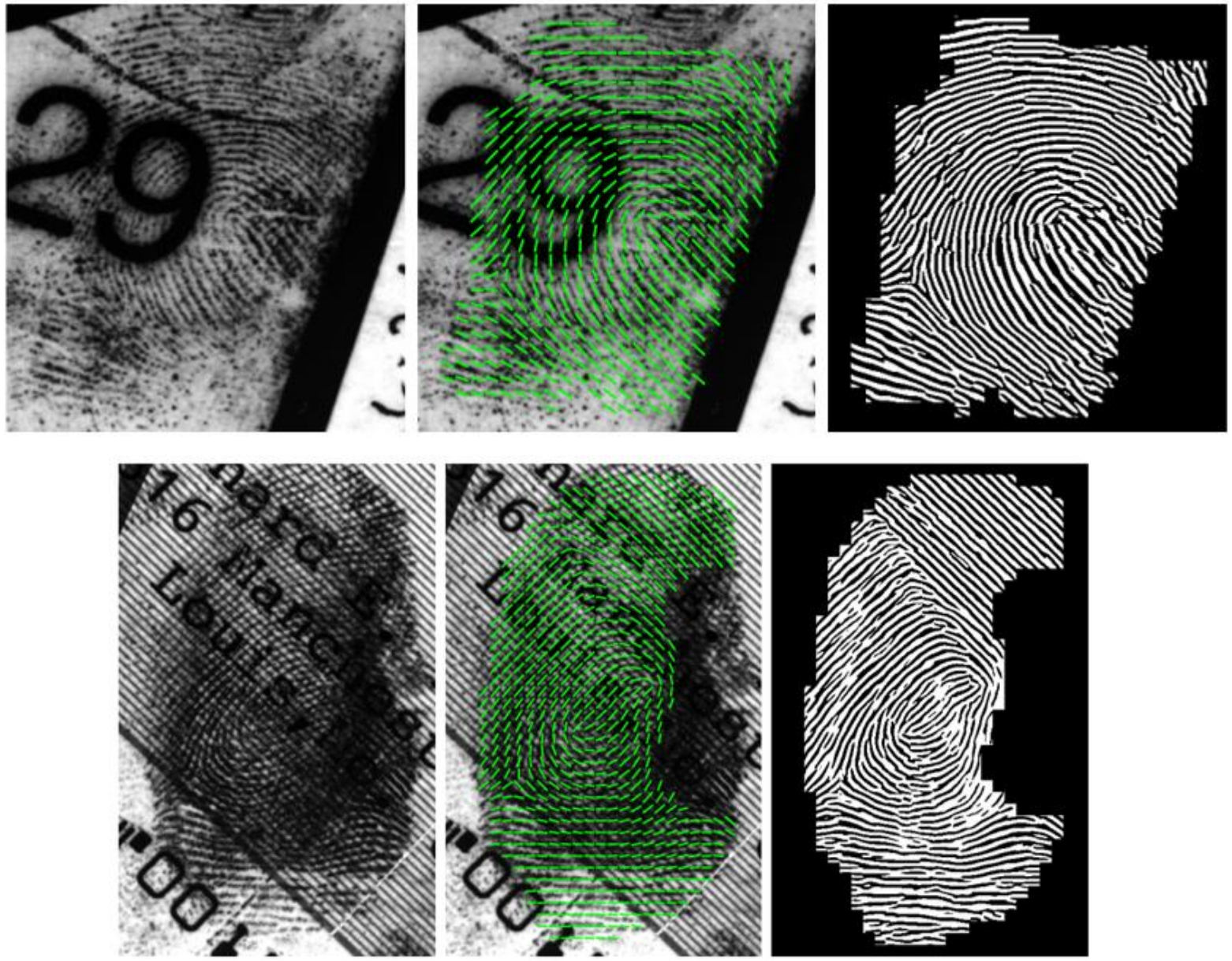
Orientation Image



Gabor Filters

Enhancement

Enhancement (examples)

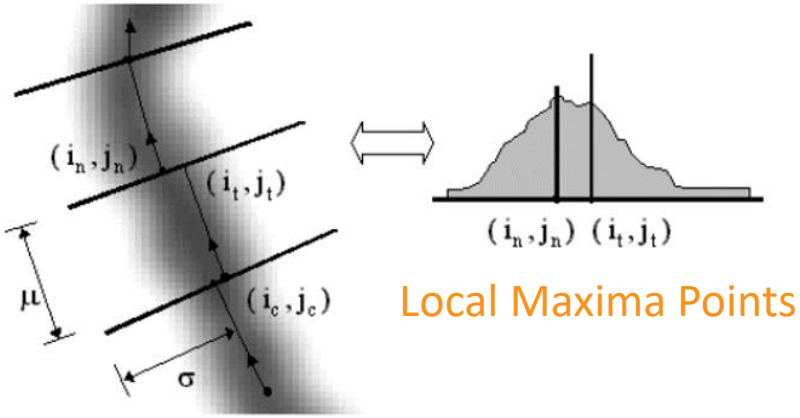


Thinning

A ridge-line is made of a set of points that are the local maxima with respect to the direction orthogonal to the ridge-line itself.

Enhancement/Binarization

Thinning

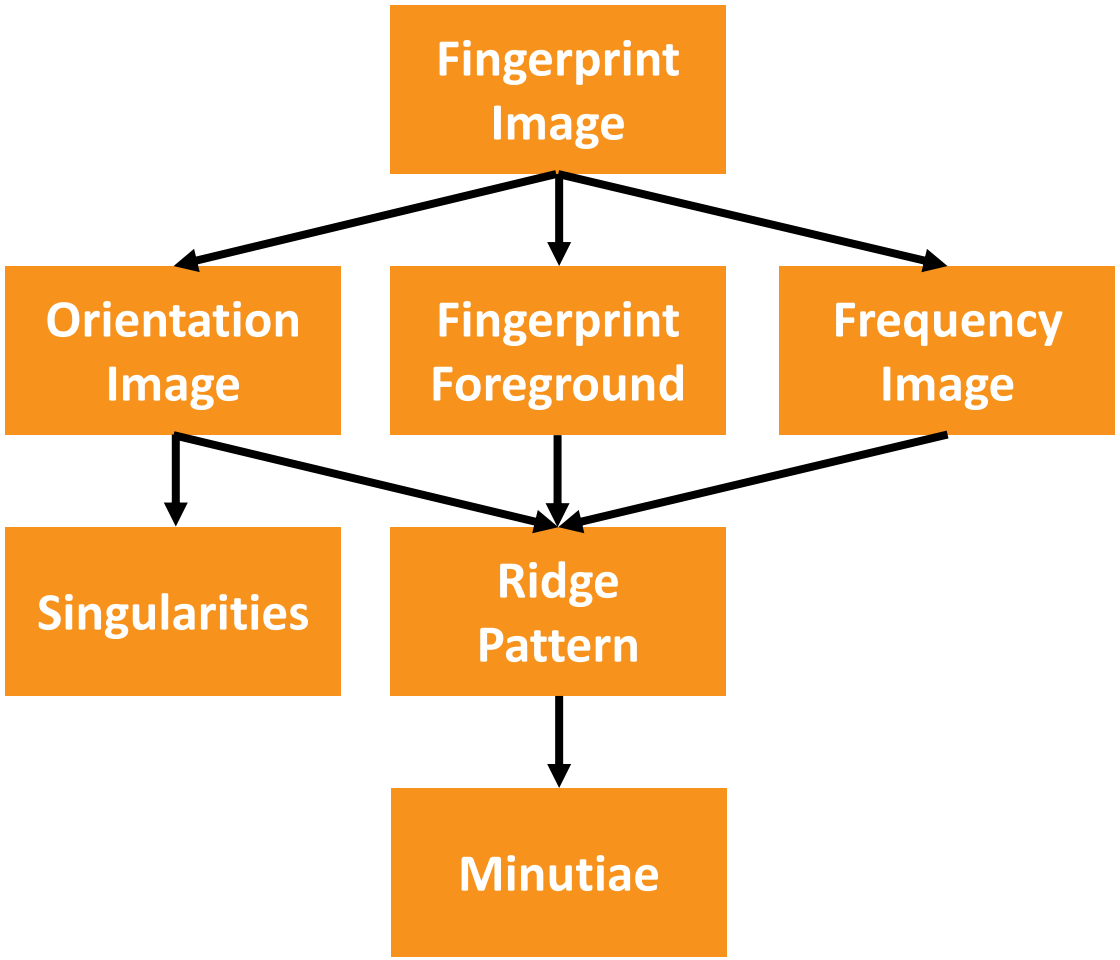


Local Maxima Points

Feature Extraction

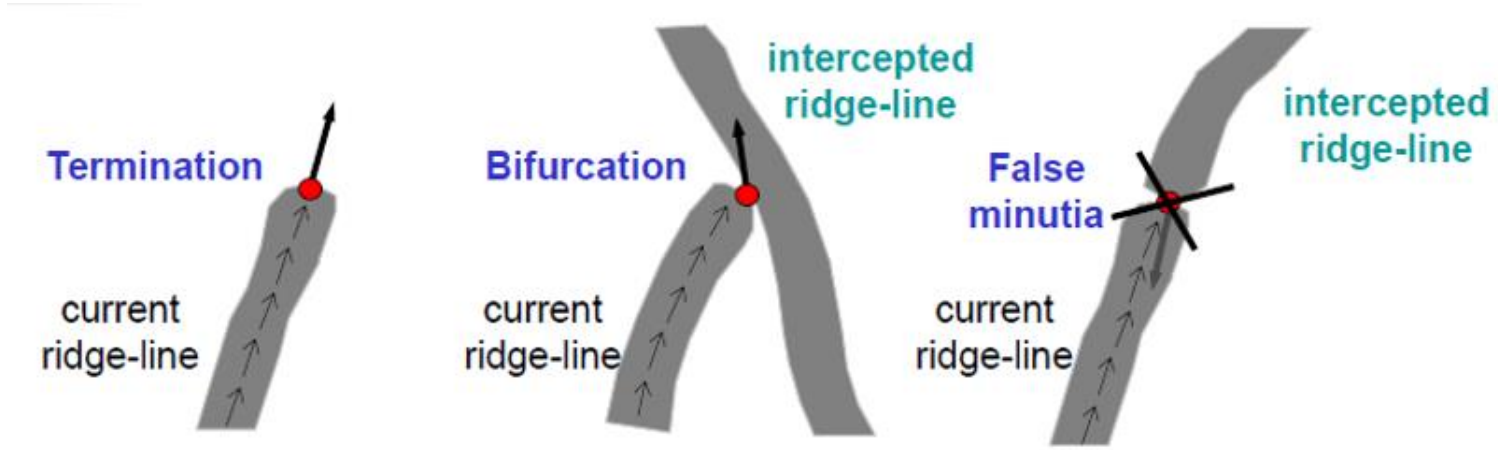
Fingerprint Image

Minutiae



Minutiae

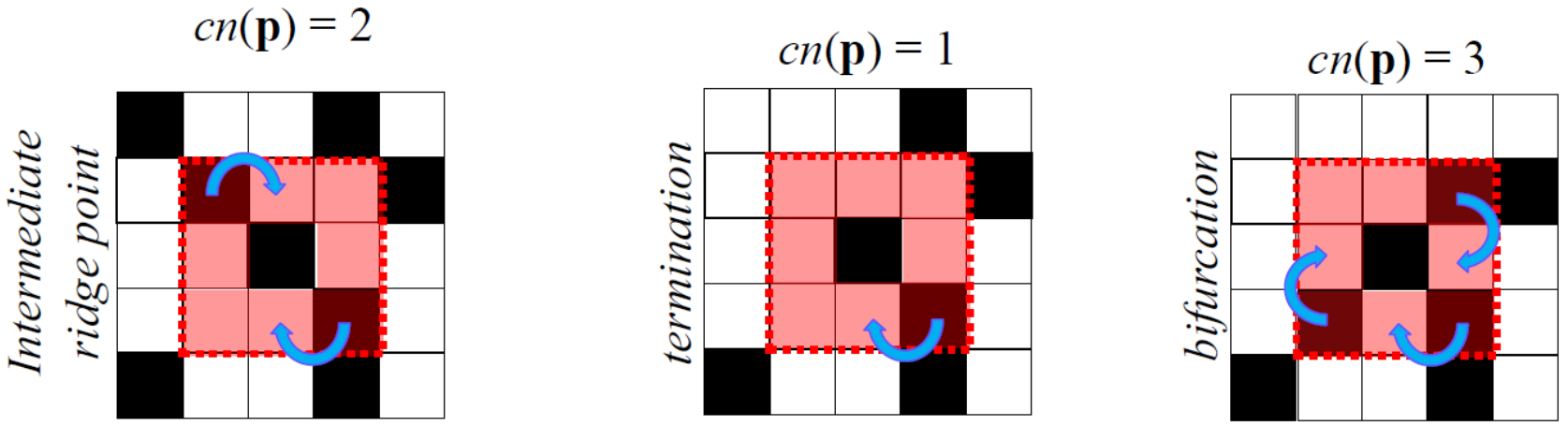
A set of starting points is determined (according to a square-mesh grid superimposed to the image). For each point, the algorithm finds the nearest ridge-line and follows it until a bifurcation or a termination is reached.



Minutiae

A set of starting points is determined (according to a square-mesh grid superimposed to the image). For each point, the algorithm finds the nearest ridge-line and follows it until a bifurcation or a termination is reached.

Minutiae detection is based on the computation of the crossing number (cn):

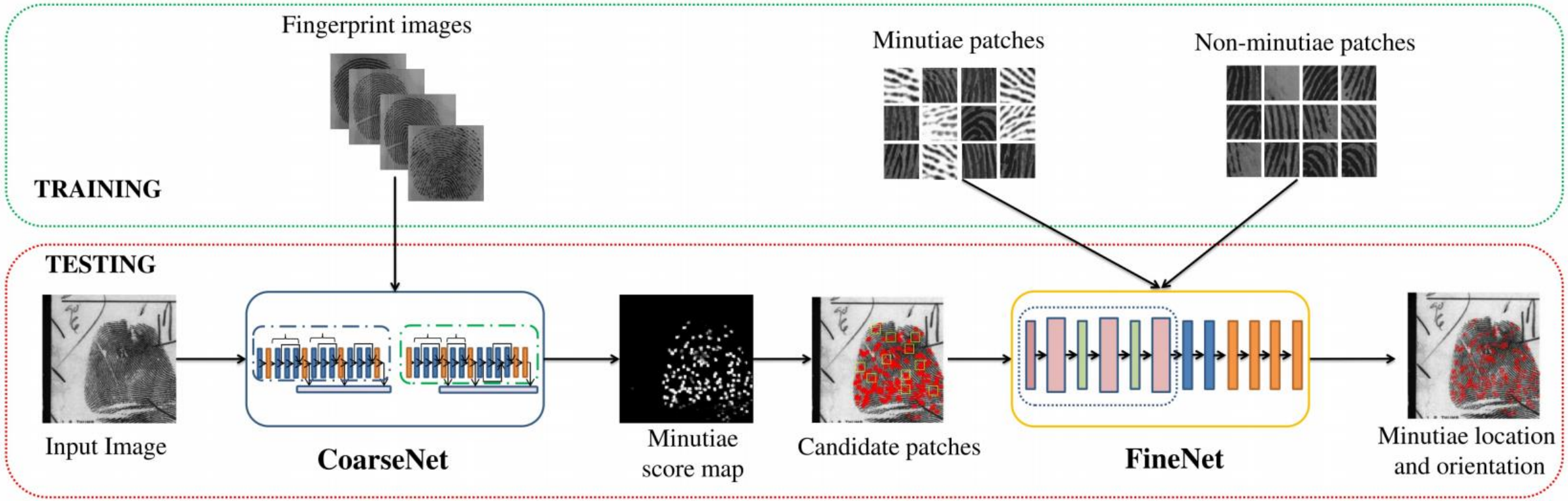


It is simple to note that a pixel black p:

- Is an intermediate ridge point if cn(p)=2.
- Is a termination if cn(p)=1.
- Is a bifurcation if cn(p)=3.

Minutiae

MinutiaeNet: Extracting minutiae features using DCNN.

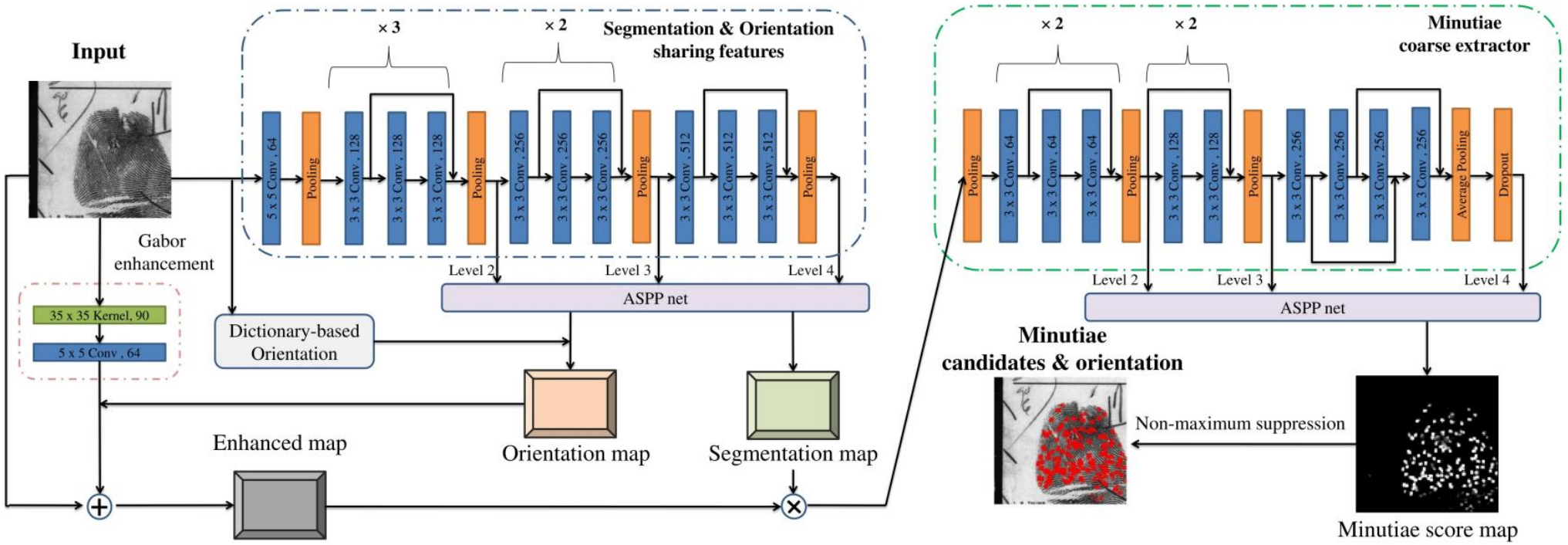


- D. L. Nguyen, K. Cao and A. K. Jain, “Robust minutiae extractor: Integrating deep networks and fingerprint domain knowledge,” in Proc. IEEE International Conference on Biometrics, 2018
- Code: https://github.com/luannd/MinutiaeNet

Minutiae

MinutiaeNet: Extracting minutiae features using DCNN.

- CoarseNet: estimates the minutiae score map and minutiae orientation based on residual CNN and fingerprint domain knowledge (enhanced image, orientation field, and segmentation map).

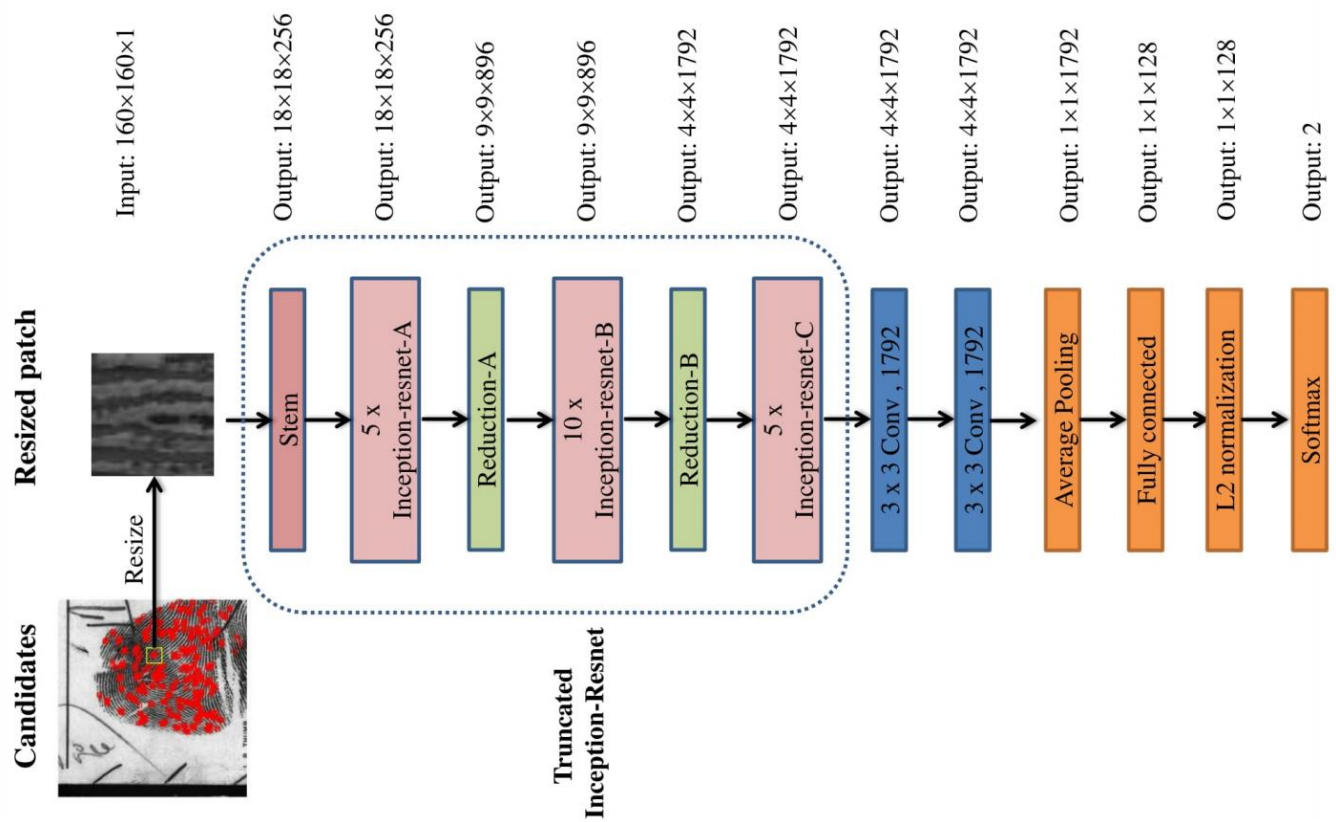


- D. L. Nguyen, K. Cao and A. K. Jain, “Robust minutiae extractor: Integrating deep networks and fingerprint domain knowledge,” in Proc. IEEE International Conference on Biometrics, 2018
- Code: https://github.com/luannd/MinutiaeNet

Minutiae

MinutiaeNet: Extracting minutiae features using DCNN.

- FineNet: refines the candidate minutiae locations based on score map. It takes candidate patches from the output of CoarseNet as input to decide whether the region 10x10 has a valid minutiae or not.



- D. L. Nguyen, K. Cao and A. K. Jain, “Robust minutiae extractor: Integrating deep networks and fingerprint domain knowledge,” in Proc. IEEE International Conference on Biometrics, 2018
- Code: https://github.com/luannd/MinutiaeNet

Minutiae

MinutiaeNet: Results on latent fingerprint databases (NIST SD27 y FVC 2004).

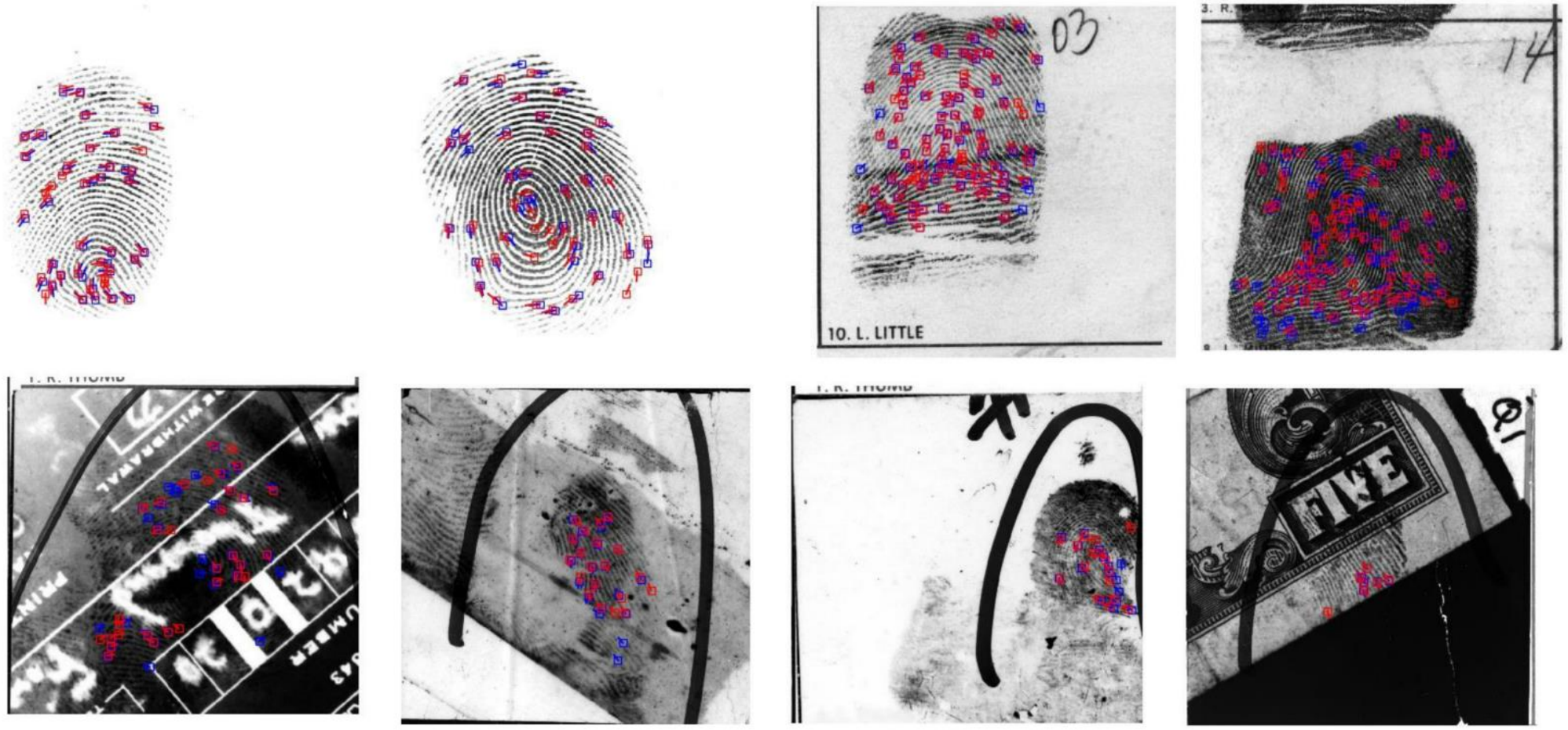
Dataset	Methods	Setting 1 ($\mathcal{D} = 8, \mathcal{O} = 10$)			Setting 2 ($\mathcal{D} = 12, \mathcal{O} = 20$)			Setting 3 ($\mathcal{D} = 16, \mathcal{O} = 30$)		
		Precision	**Recall**	**F1 score**	**Precision**	**Recall**	**F1 score**	**Precision**	**Recall**	**F1 score**
NIST SD27	MINDTCT [24]	8.3%	14.7%	0.106	10.0%	16.4%	0.124	11.2%	18.9%	0.141
	VeriFinger [23]	3.6%	40.1%	0.066	5.3%	47.9%	0.095	7.6%	58.3%	0.134
	Gao *et al.* [5]	-	-	-	-	-	-	23.5%	8.7%	0.127
	Sankaran *et al.* [18]	-	-	-	-	-	-	26.4%	63.1%	0.372
	Tang *et al.* [21]	-	-	-	-	-	-	53.0%	53.4%	0.532
	FingerNet [22]	53.2%	49.5%	0.513	58.0%	58.1%	0.58	63.0%	63.2%	0.631
	Proposed method	**69.2%**	**67.7%**	**0.684**	**70.5%**	**72.3%**	**0.714**	**71.2%**	**75.7%**	**0.734**
FVC 2004	MINDTCT [24]	30.8%	64.3%	0.416	37.7%	72.1%	0.495	42.1%	79.8%	0.551
	VeriFinger [23]	39.8%	69.2%	0.505	45.6%	77.5%	0.574	51.8%	81.9%	0.635
	Gao *et al.* [5]	-	-	-	-	-	-	48.8%	82.7%	0.614
	FingerNet [22]	68.7%	62.1%	0.643	72.9%	70.4%	0.716	76.0%	80.0%	0.779
	Proposed method	**79.0%**	**80.1%**	**0.795**	**83.6%**	**83.9%**	**0.837**	**85.9%**	**84.8%**	**0.853**

MINDTCT: NIST Biometric Image Software; VeriFinger: Commercial SDK Software; Others: Deep Learning

- D. L. Nguyen, K. Cao and A. K. Jain, “Robust minutiae extractor: Integrating deep networks and fingerprint domain knowledge,” in Proc. IEEE International Conference on Biometrics, 2018
- Code: https://github.com/luannd/MinutiaeNet

Minutiae

MinutiaeNet: Examples from NIST SD27 y FVC 2004 (Blue: Ground truth; Red: MinutiaNet).



- D. L. Nguyen, K. Cao and A. K. Jain, “Robust minutiae extractor: Integrating deep networks and fingerprint domain knowledge,” in Proc. IEEE International Conference on Biometrics, 2018
- Code: https://github.com/luannd/MinutiaeNet

Automatic Fingerprint Recognition: Architecture

Input Fingerprint

Presentation Attack Detection

Real or Fake?

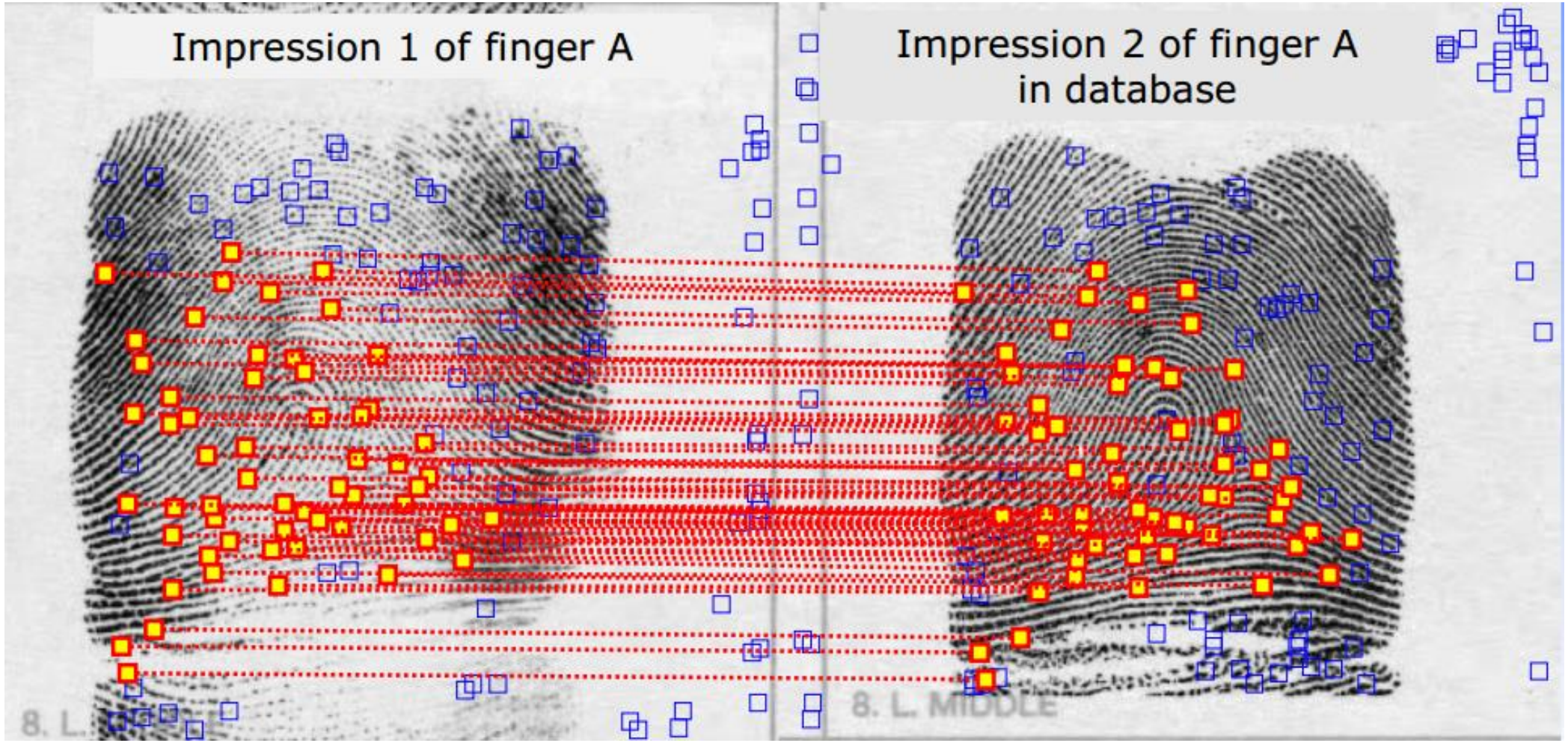
Feature Extraction

Matching

Identity
Match/Non-match

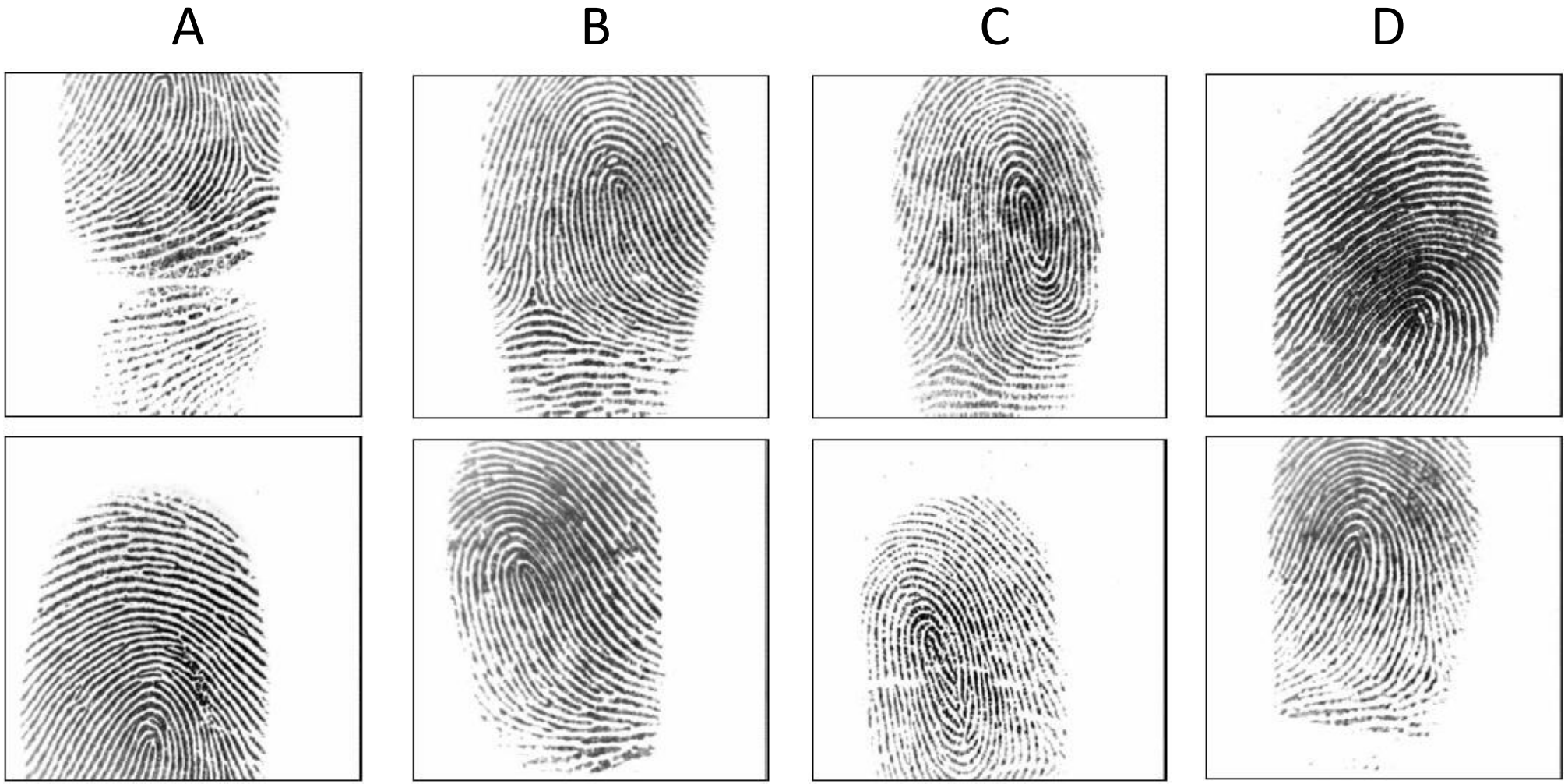
Database

Matching


Impression 1 of finger A
Impression 2 of finger A
in database
8. L.
8. L. MIDDLE

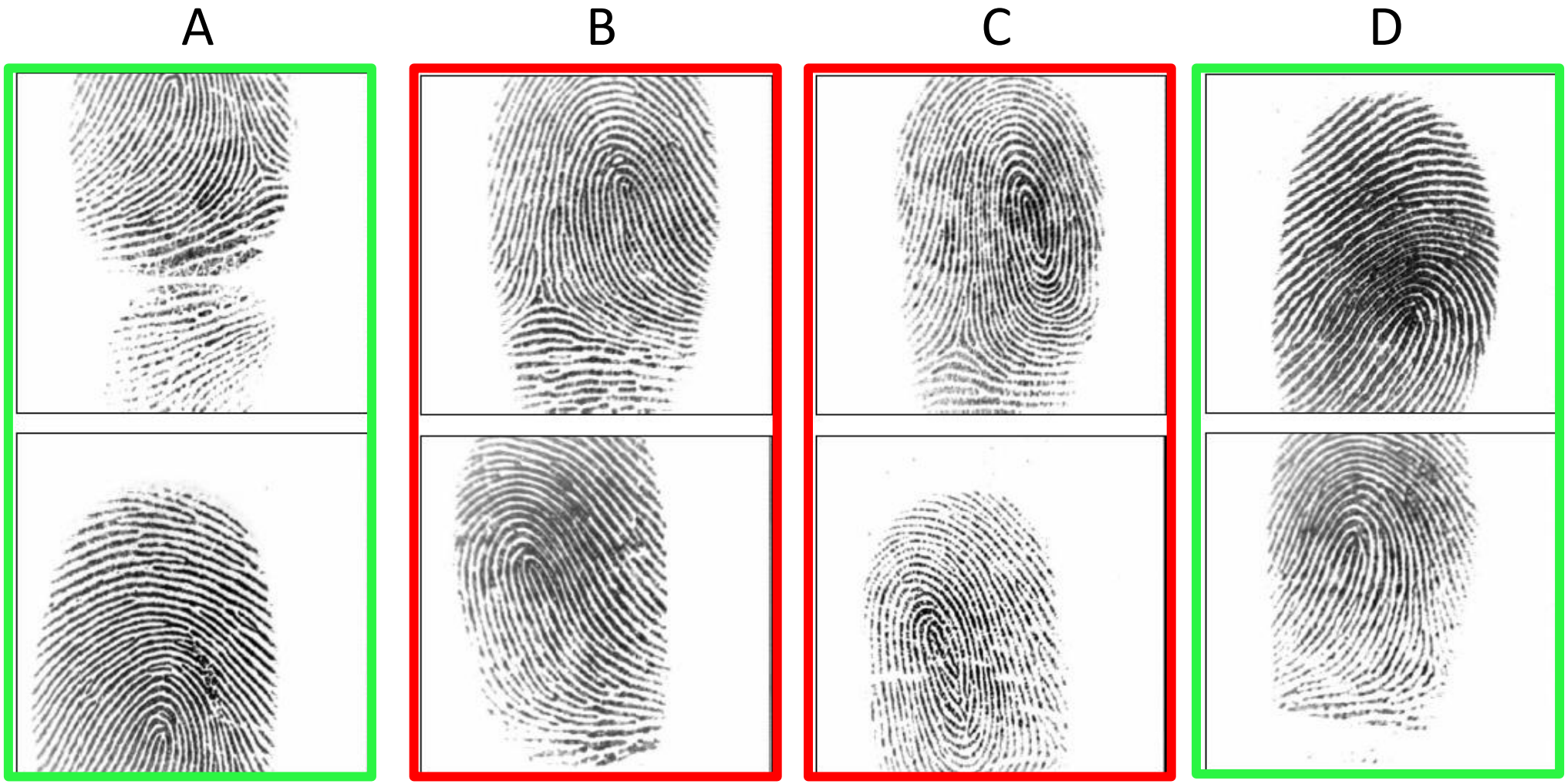
Matching

During fingerprint matching, the degree of similarity between two fingerprints is evaluated.



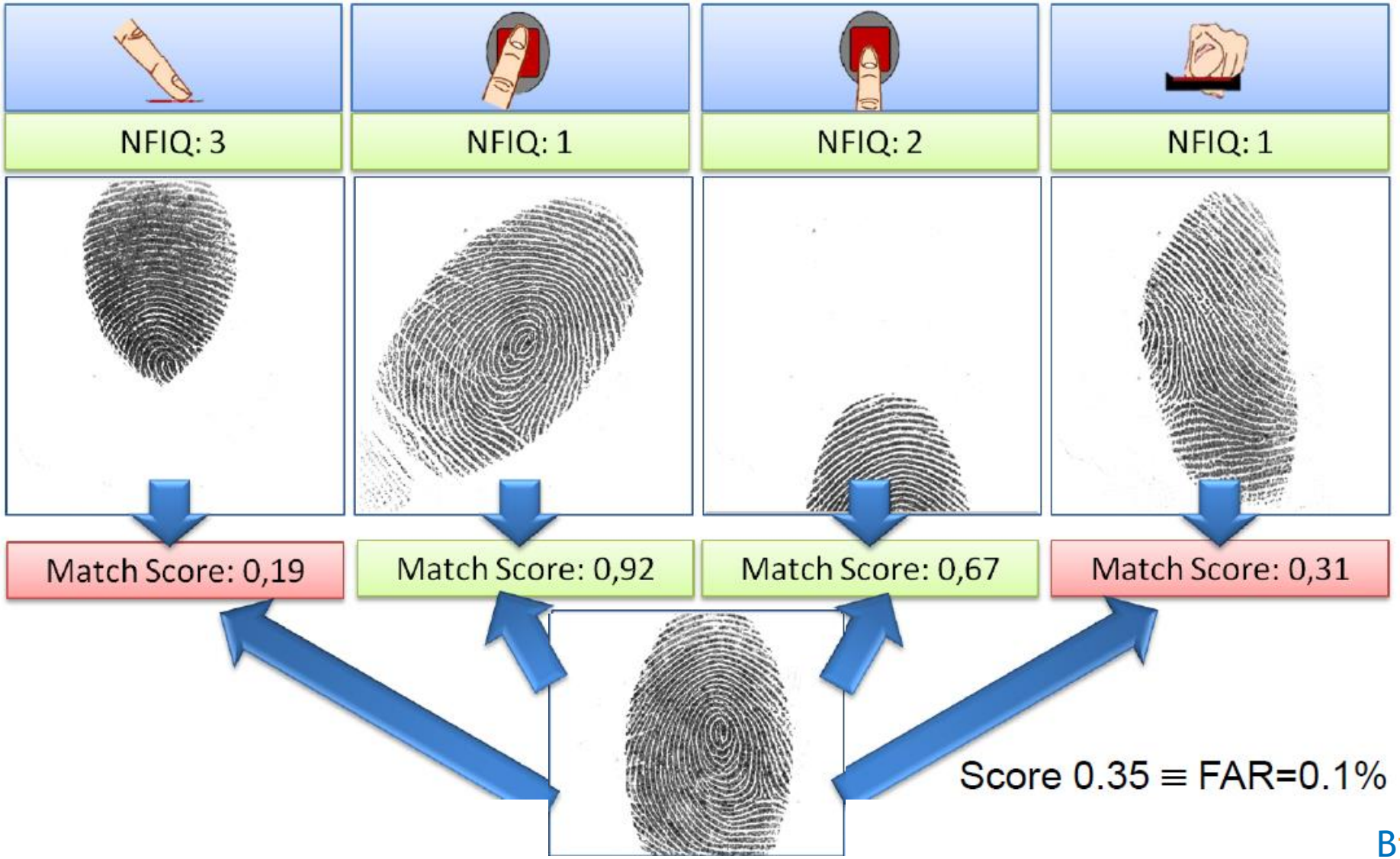
Matching

During fingerprint matching, the degree of similarity between two fingerprints is evaluated.



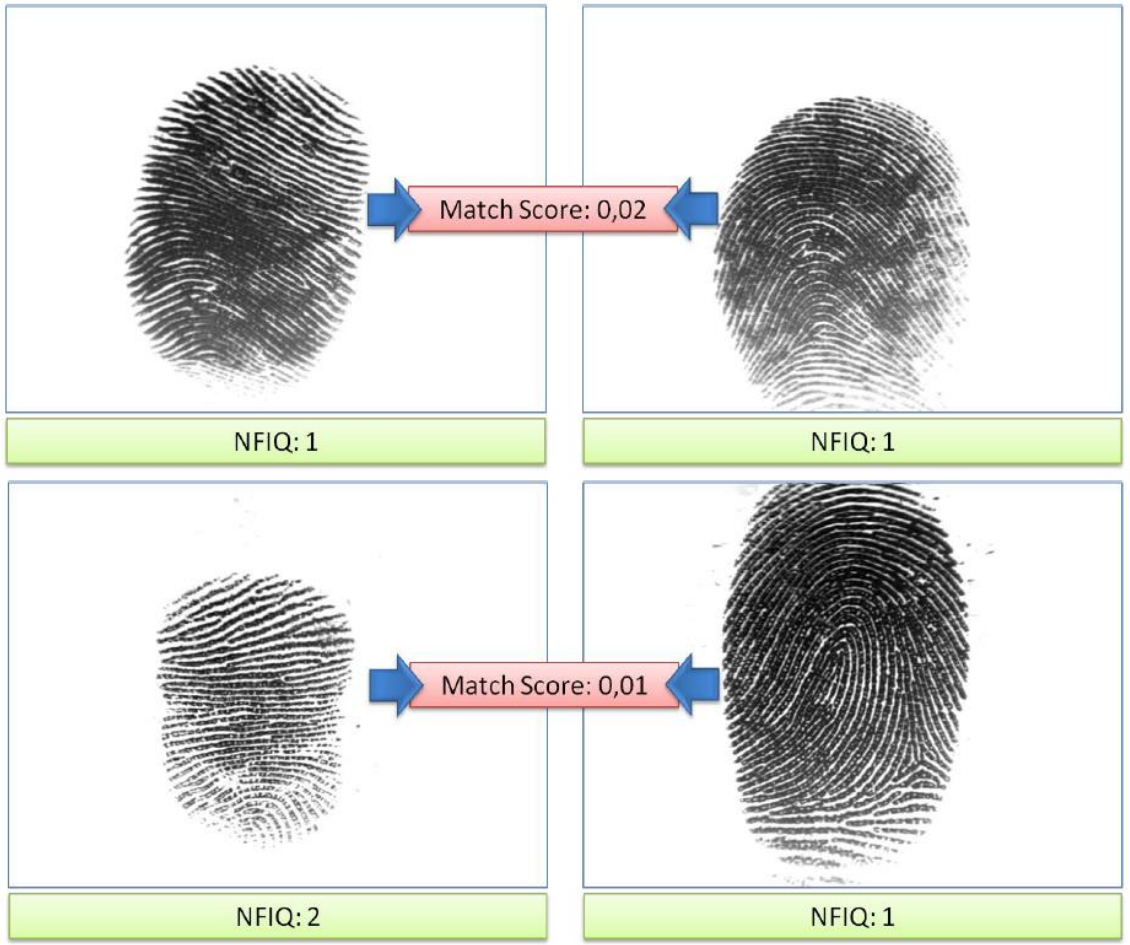
Matching: Main Challenges

Bad positioning:



Matching: Main Challenges

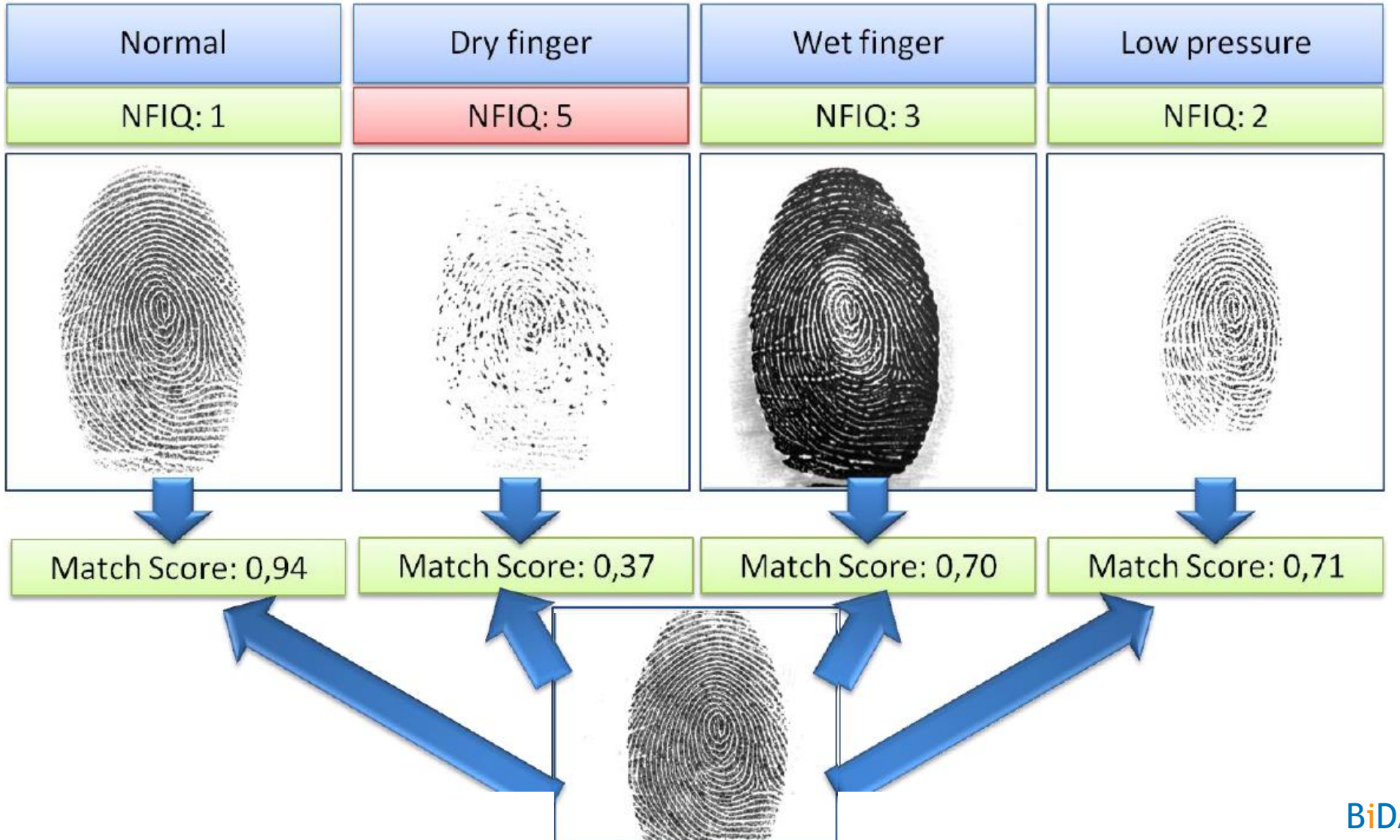
Non-linear distortions: the act of sensing maps the 3D shape of a finger onto the 2D surface of the sensor (due to skin plasticity).



Score = 0.35
FAR=0.1%

Matching: Main Challenges

Bad skin conditions and wrong pressure:



Matching: Main Challenges

Interoperability among sensors and acquisition methods:

- Each country, agency or government have their own records (millions of fingerprints) acquired according specific protocols and sensors.
- Can we match fingerprints from different records? E.g., EU Interpol record and USA FBI record?
- Do we have to enroll all the users every time we update the sensor?

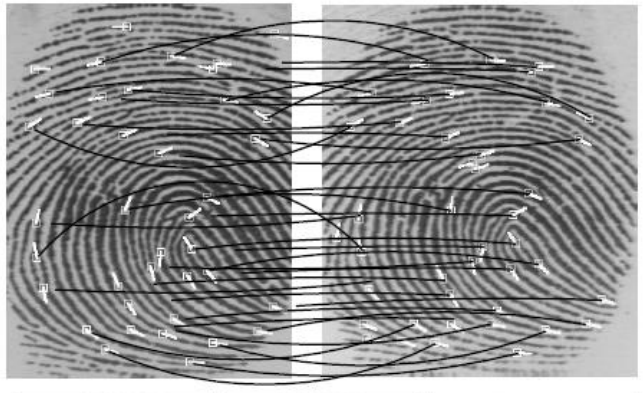
Standards are necessary to stablish common protocols

(ISO/IEC 19794-2 and ANSI/INCITS 378)

Matching: Approaches

Minutiae-Based matching:

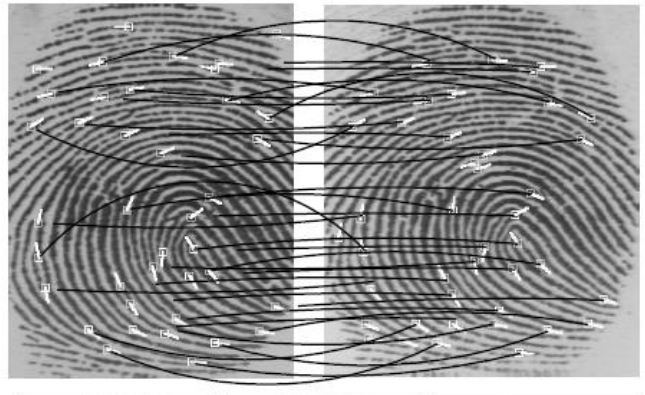
- The most popular and widely used technique. Minutiae-based matching consists in finding the alignment that results in the maximum number of minutiae pairings.



Matching: Approaches

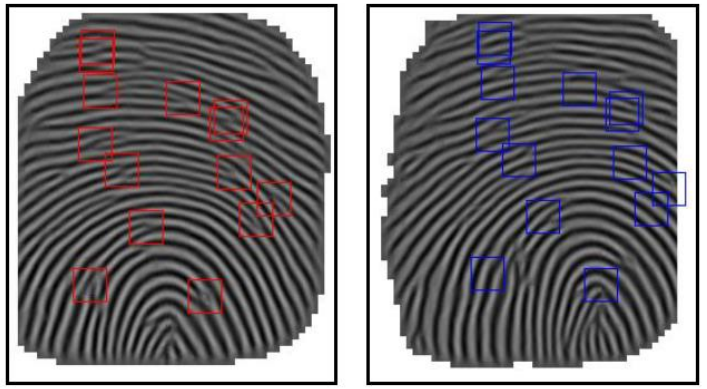
Minutiae-Based matching:

- The most popular and widely used technique. Minutiae-based matching consists in finding the alignment that results in the maximum number of minutiae pairings.



Correlation-Based matching:

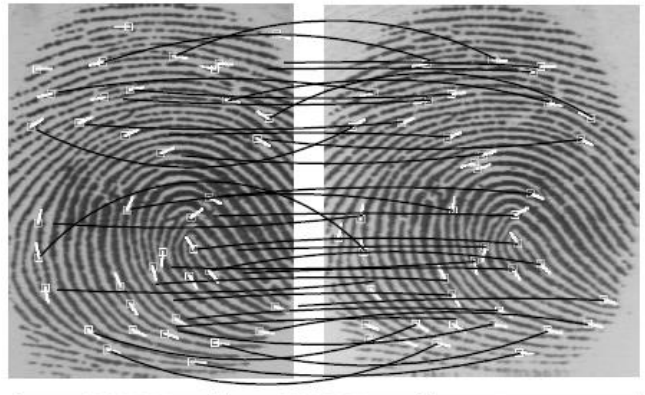
- Two fingerprints are superimposed and the correlation between corresponding pixels is computed for different alignments.



Matching: Approaches

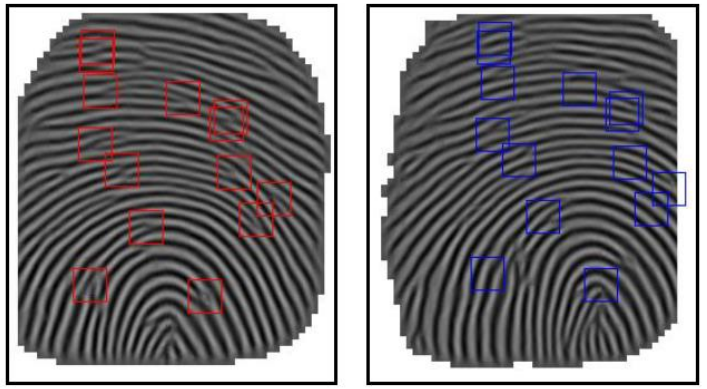
Minutiae-Based matching:

- The most popular and widely used technique. Minutiae-based matching consists in finding the alignment that results in the maximum number of minutiae pairings.



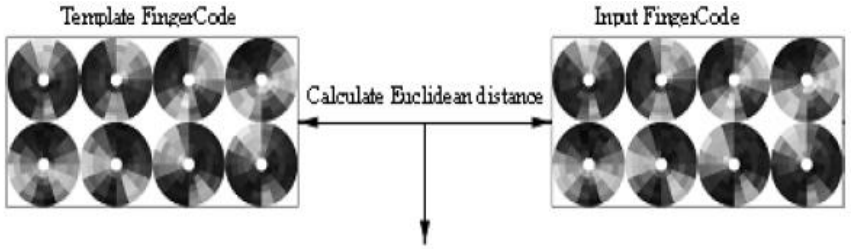
Correlation-Based matching:

- Two fingerprints are superimposed and the correlation between corresponding pixels is computed for different alignments.

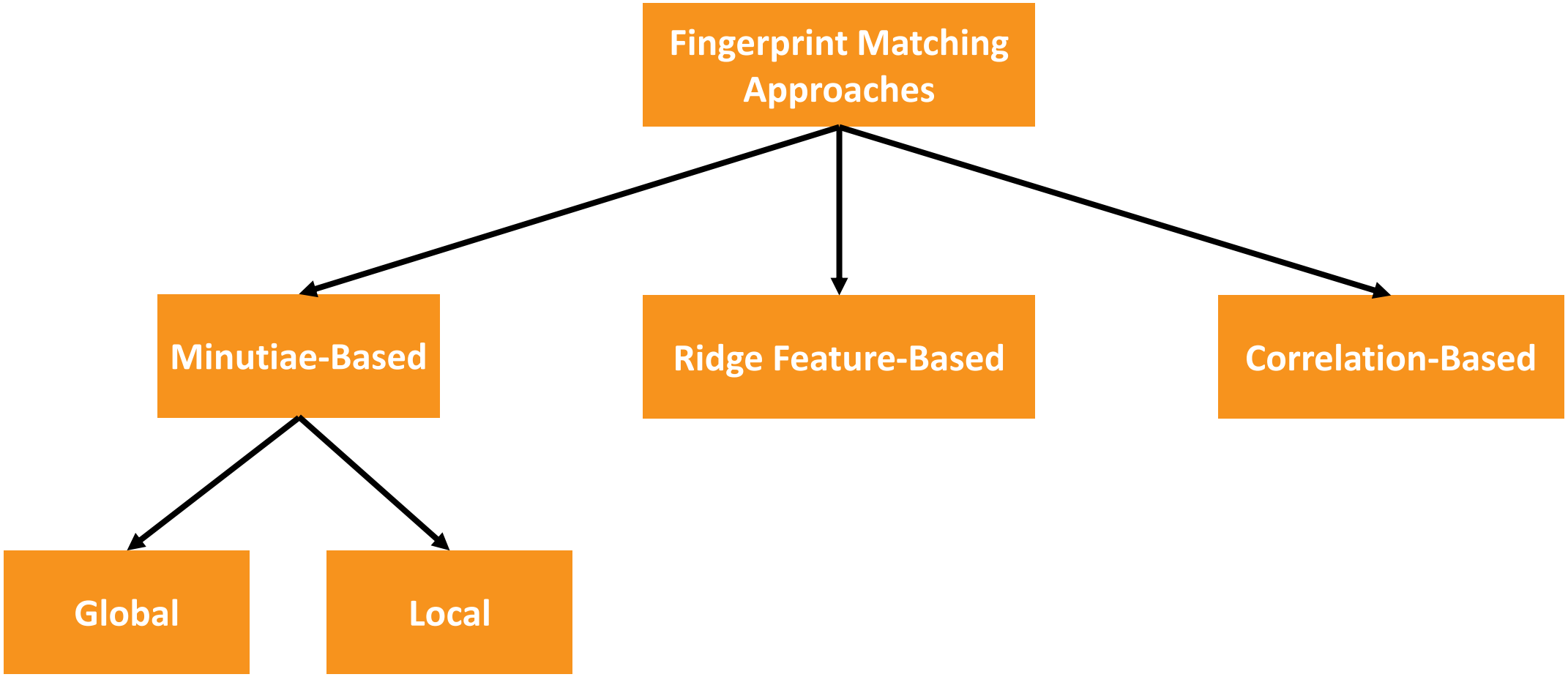


Ridge feature-Based matching:

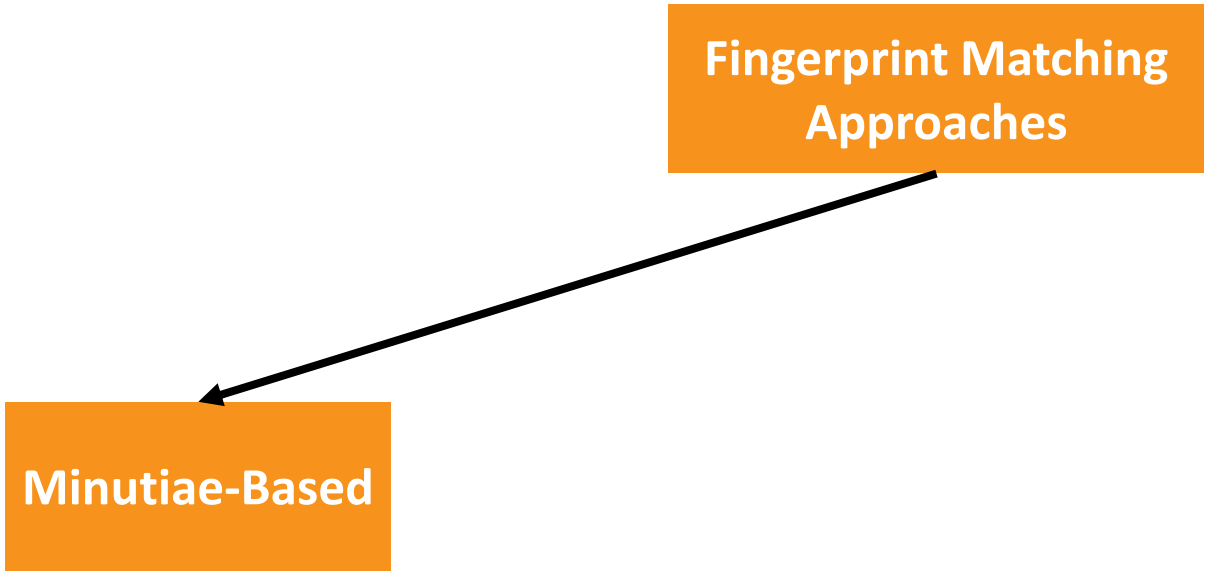
- Other features of the fingerprint ridge pattern (e.g., local orientation and frequency, ridge shape, texture information) may be extracted more reliably than minutiae in low-quality images.



Matching: Approaches



Matching: Approaches



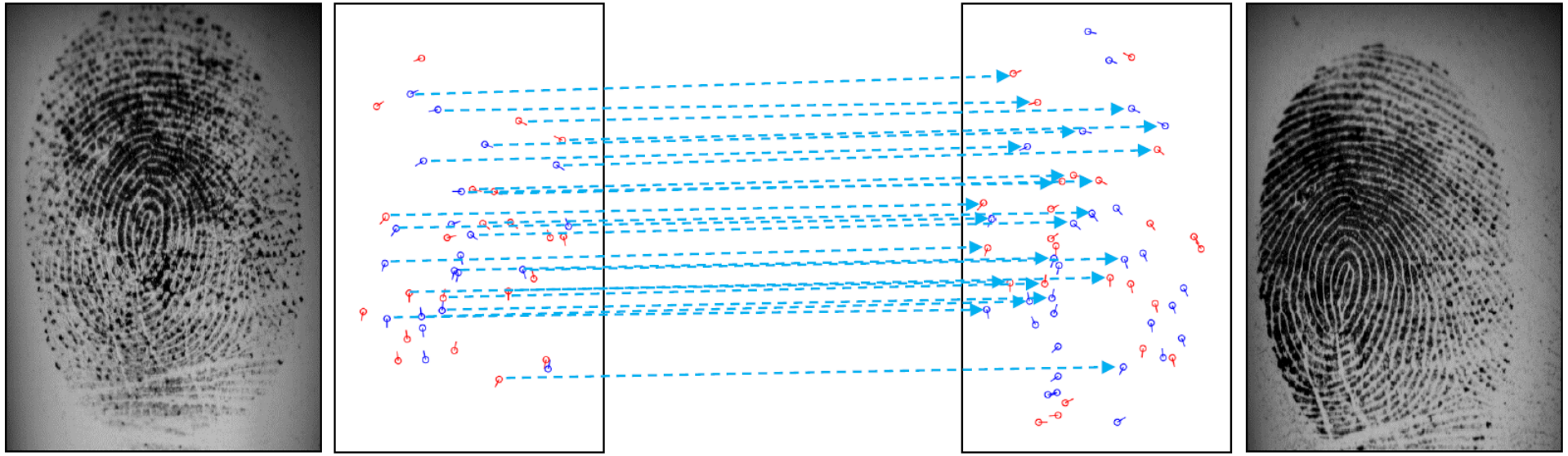
Minutiae-Based

In minutiae-based comparison, the fingerprint is represented by a feature vector of variable length whose elements are the fingerprint minutiae.

A minutiae is represented by the tuple $\mathrm{m} = \{\mathrm{x}, \mathrm{y}, \theta, \mathrm{t}\}$ containing the minutiae coordinates, its orientation and type.

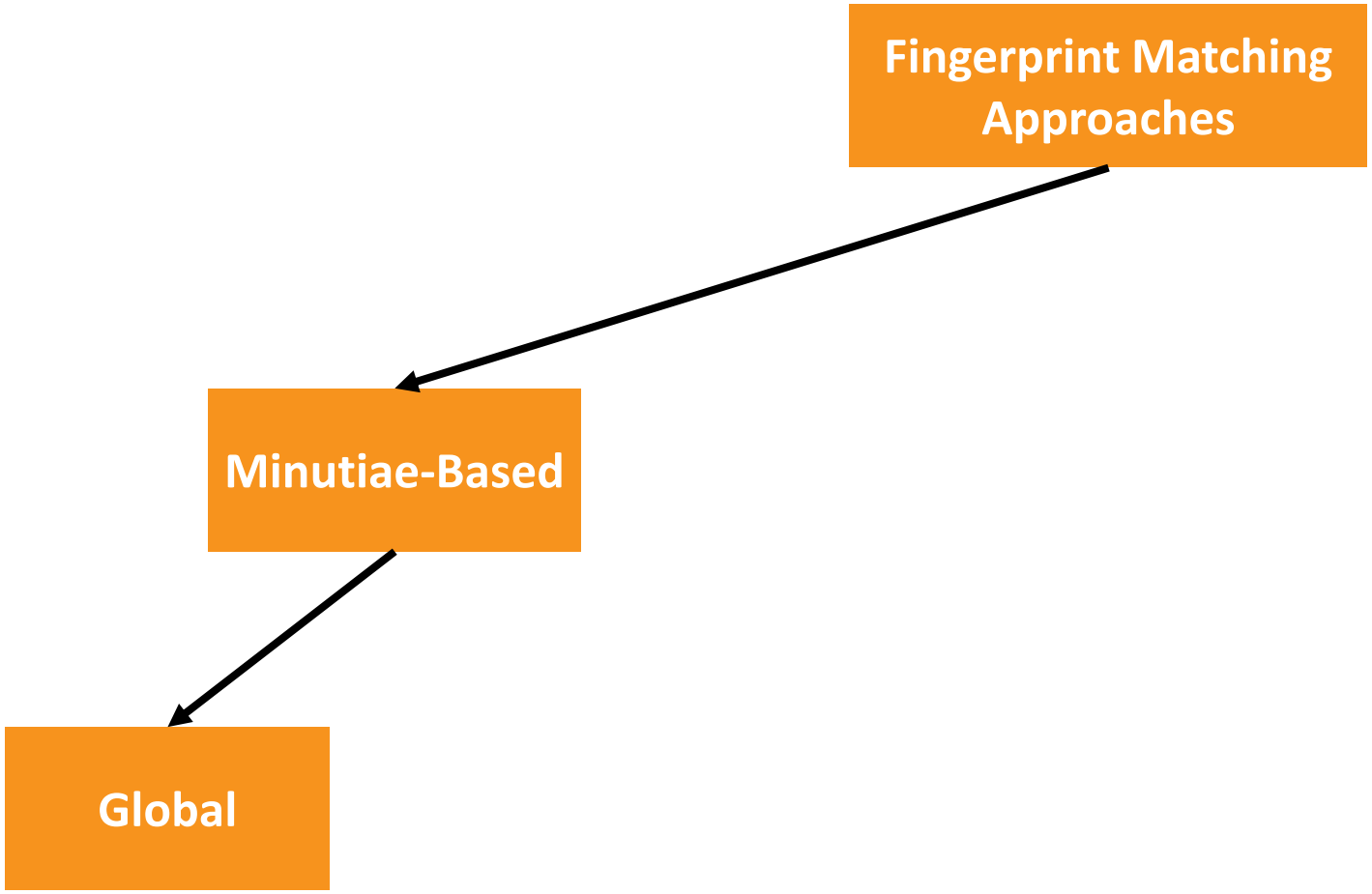
$$T_1 = \{m_1, m_2, \ldots, m_u\}$$

$$T_2 = \{m'_1, m'_2, \ldots, m'_v\}$$



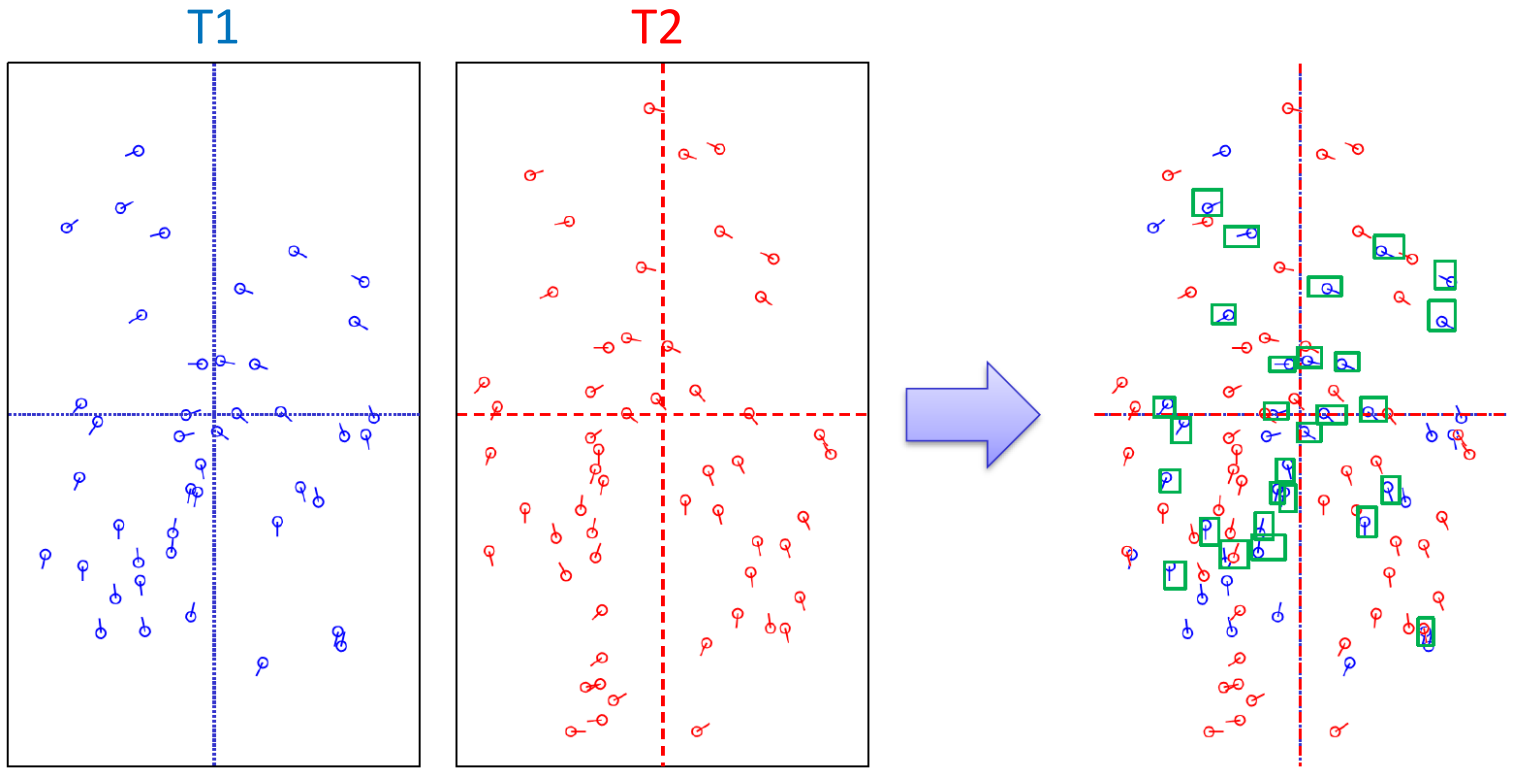
$$score = \frac{\#pairs}{(u+v)/2}$$

Matching: Approaches



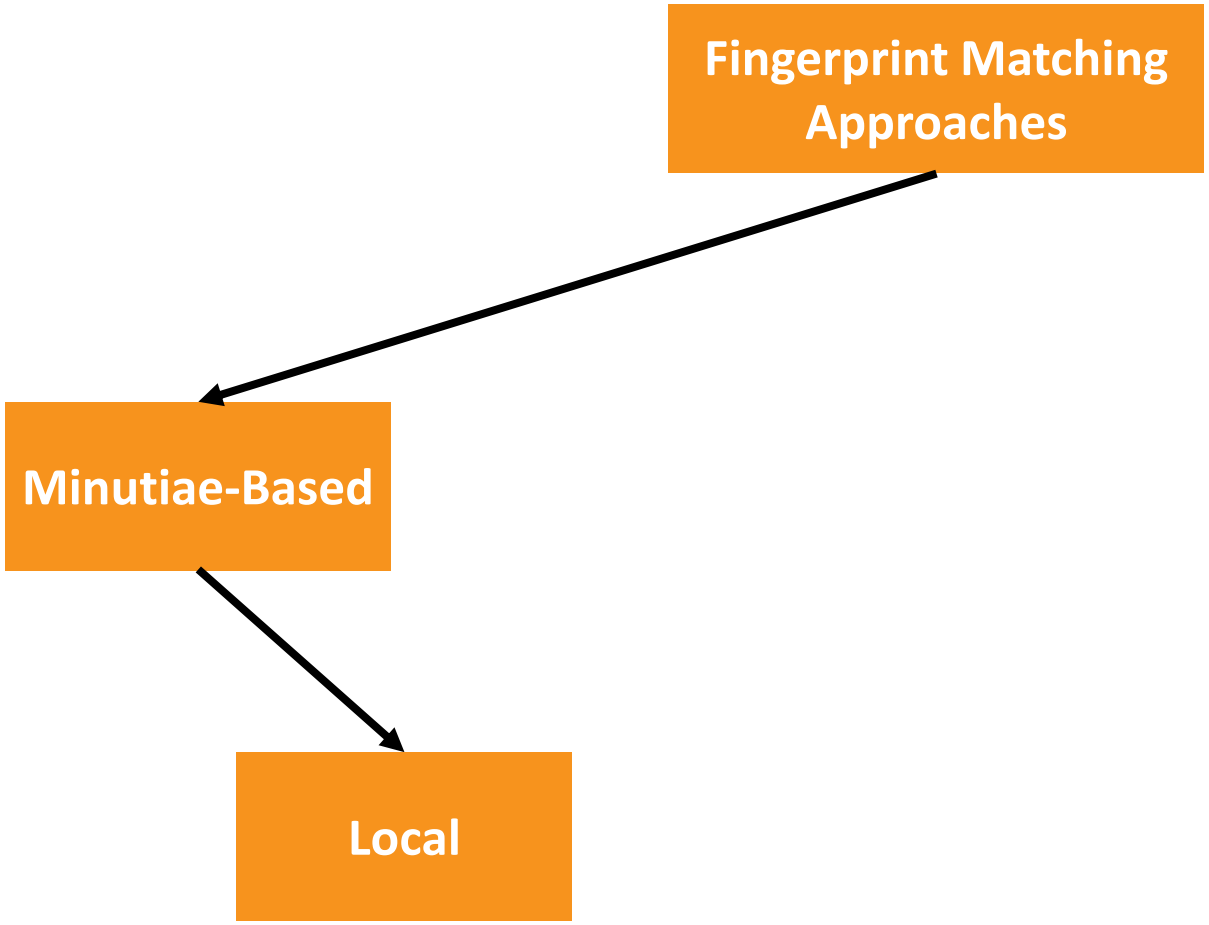
Global Minutiae-Based

The objective of global minutiae-based approaches is to apply a global transformation that allows to maximize the number of resulting paired minutiae.



Some works in the literature propose to use the Hough transform (or Ransac implementations) to find the best rigid transformation to align two minutiae template.

Matching: Approaches

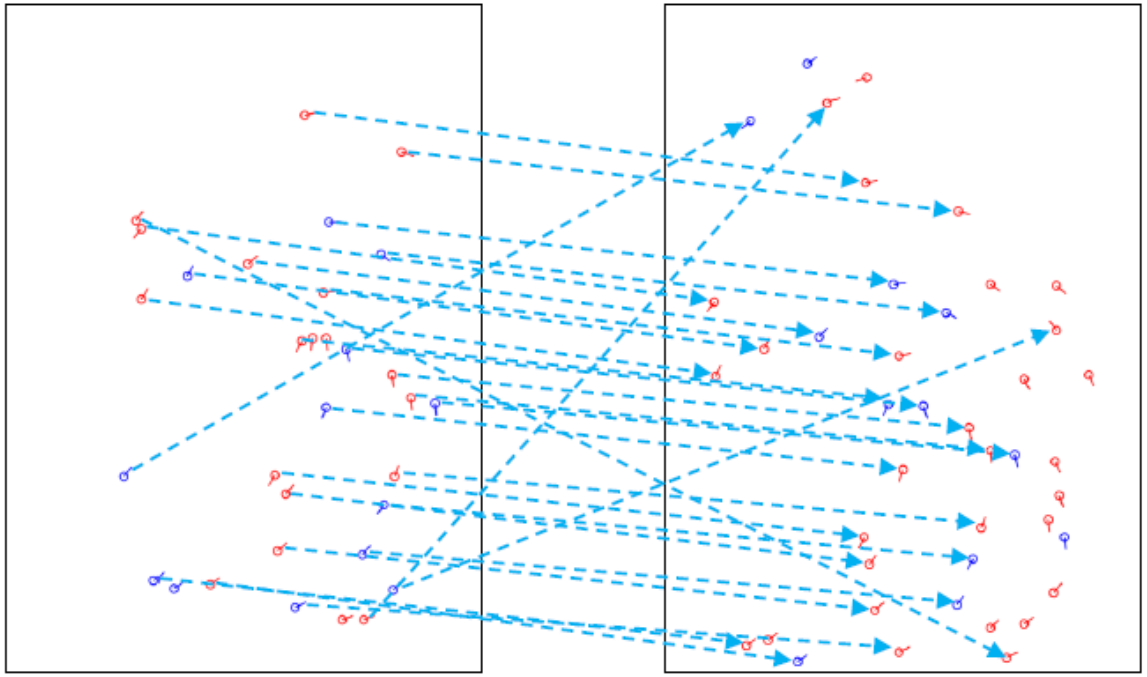


Local Minutiae-Based

The objective of local minutiae-based approaches is to pair minutiae using local minutiae features invariant to global transformation without a pre-alignment step.

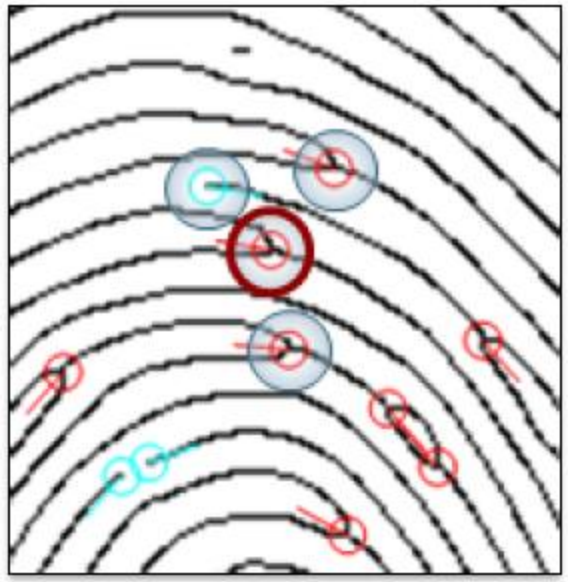
Usually they are based on the following steps:

1. For each minutiae, local features are computed from local minutiae neighborhoods.
2. The minutiae are paired according to local features (fast, robust to distortion but less distinctive).
3. A consolidation step is performed to verify if local matches hold at global level.



Local Minutiae-Based

Nearest neighbor-based local structures: the neighbors of the central minutiae are formed by its *K* closest minutiae.

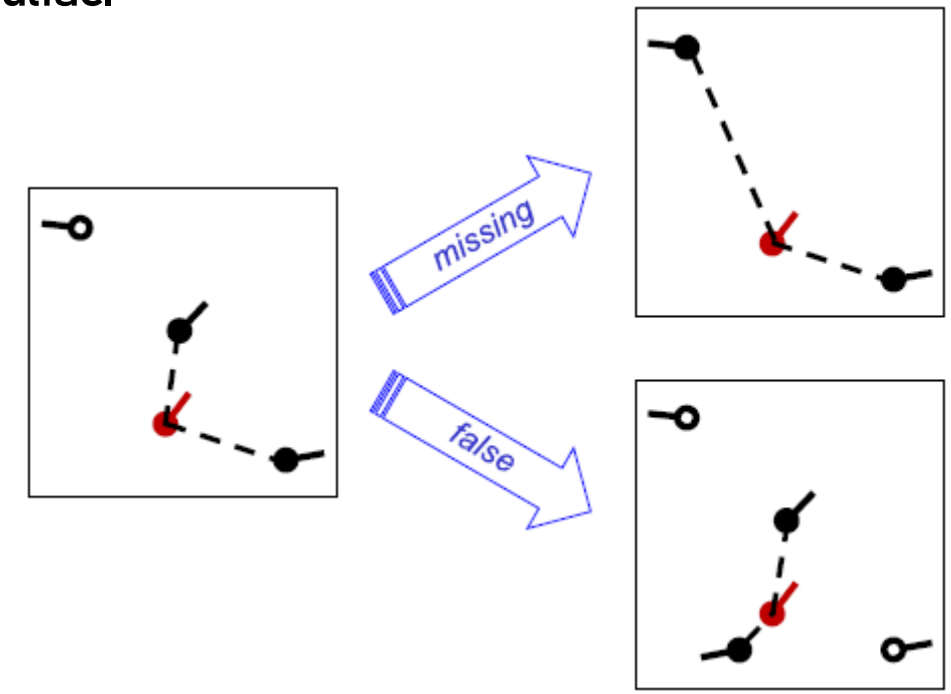


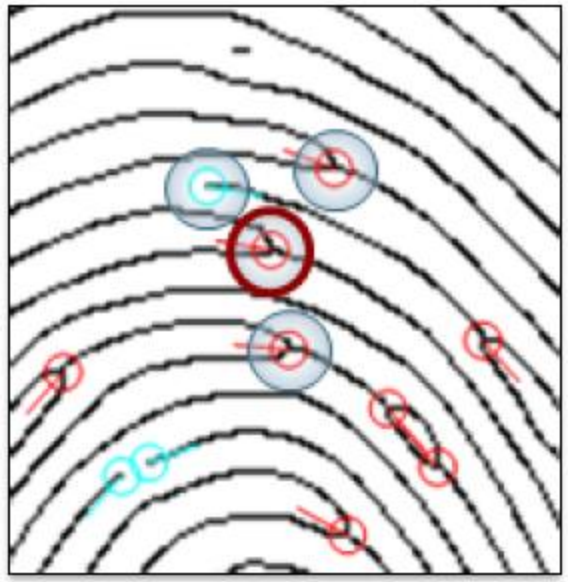
Local Minutiae-Based

Nearest neighbor-based local structures: the neighbors of the central minutiae are formed by its *K* closest minutiae.

Advantages: fixed-length descriptors that can be compared very efficiently.

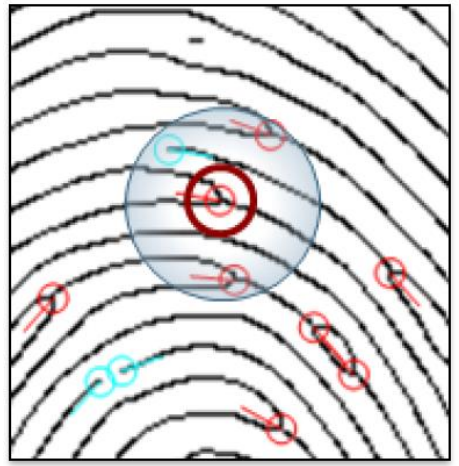
Drawbacks: possibility of exchanging nearest neighbor minutiae due to missing or false minutiae.





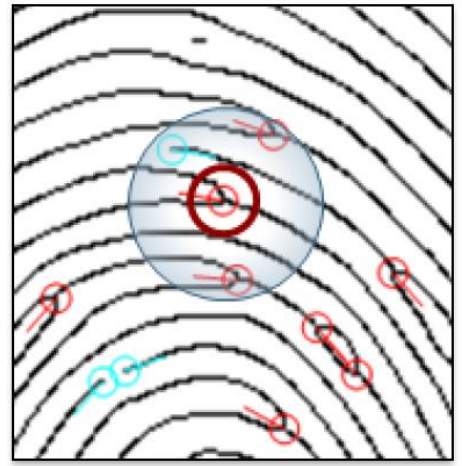
Local Minutiae-Based

Fixed radius-based local structures: the neighbors are defined as all the minutiae that are closer than a given radius R from the central minutiae.



Local Minutiae-based

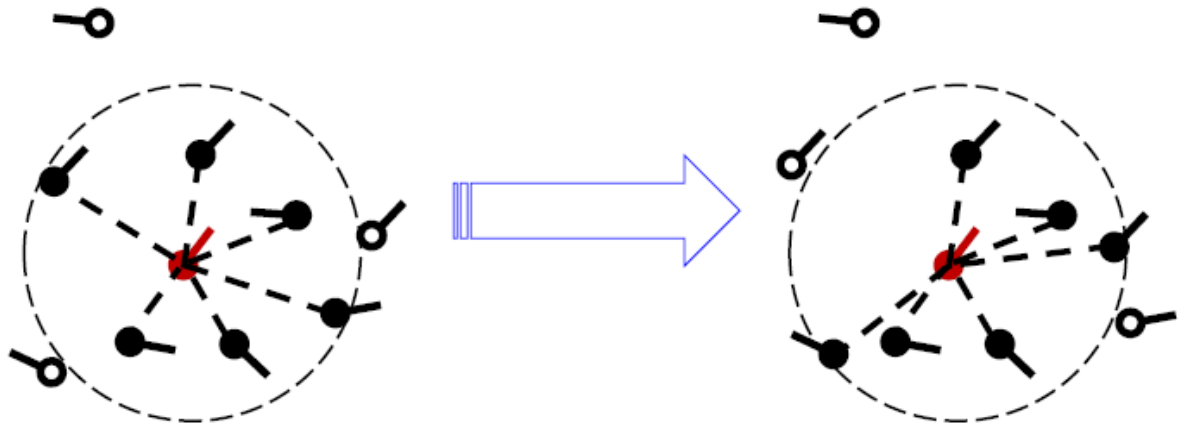
Fixed radius-based local structures: the neighbors are defined as all the minutiae that are closer than a given radius R from the central minutiae.



Advantages: missing and false minutiae are better tolerated.

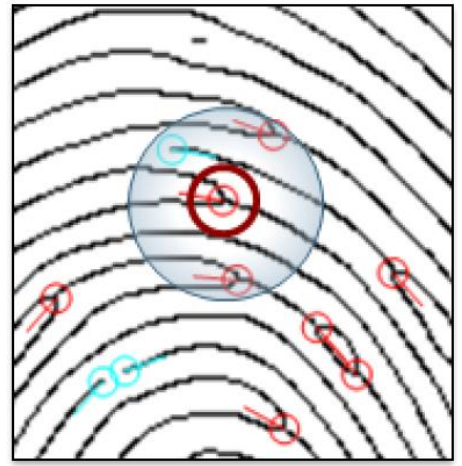
Drawbacks:

- The description length is variable leading to a more complex comparison.
- Minutiae close to the border can be mismatched because of different local distortion or location inaccuracy.



Local Minutiae-Based

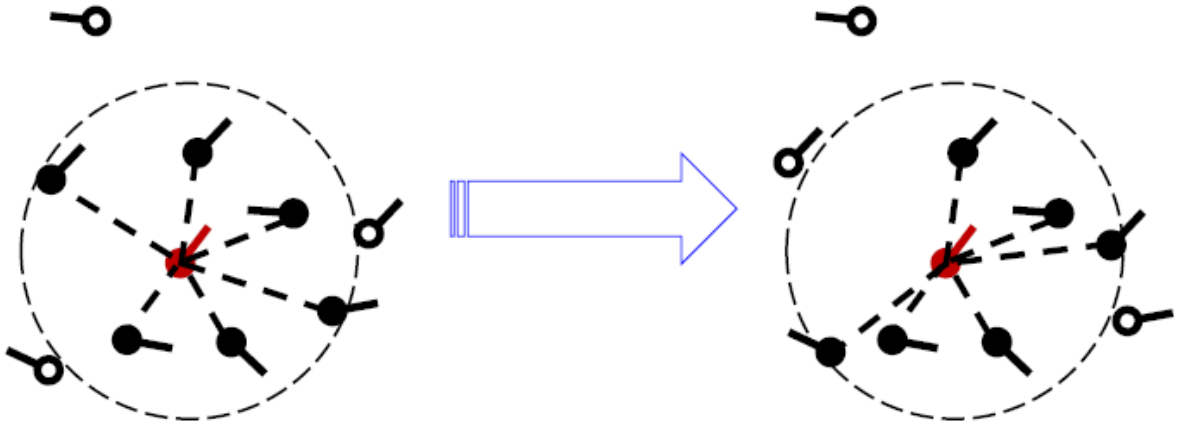
Fixed radius-based local structures: the neighbors are defined as all the minutiae that are closer than a given radius R from the central minutiae.



Advantages: missing and false minutiae are better tolerated.

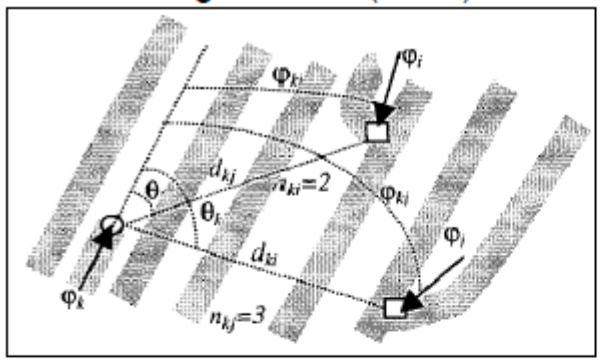
Drawbacks:

- The description length is variable leading to a more complex comparison.
- Minutiae close to the border can be mismatched because of different local distortion or location inaccuracy.

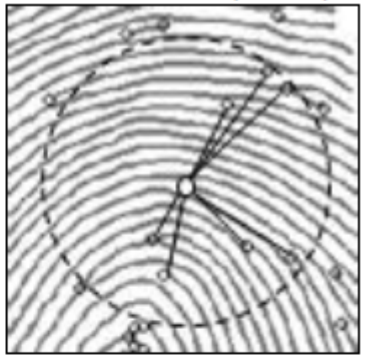


Local Minutiae-Based: Local Structures Examples

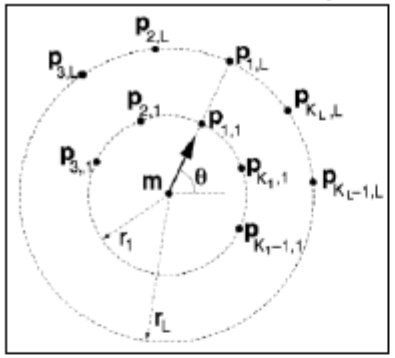
Jiang and Yau (2000)



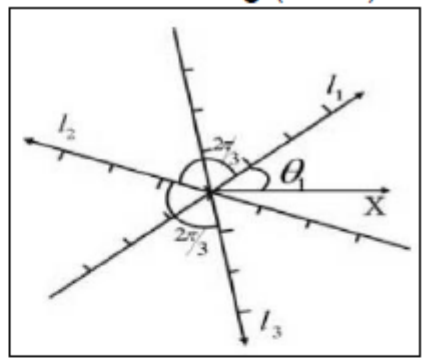
Ratha et al. (2000)



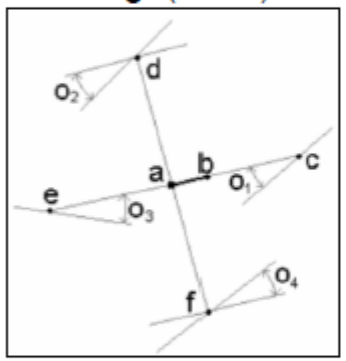
Tico and Kuosmanen (2003)



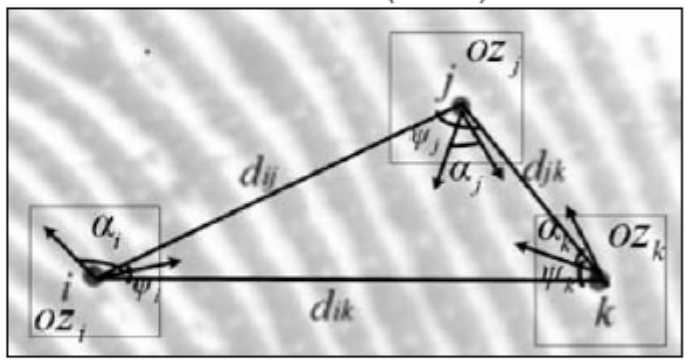
Qi and Wang (2004)



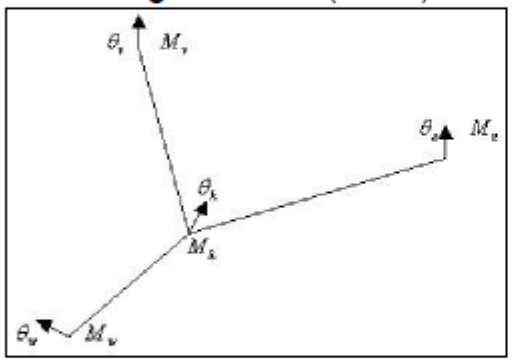
Ng (2004)



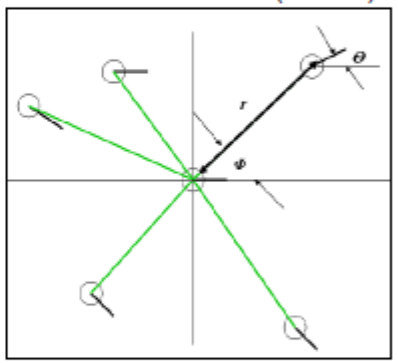
Chen et al. (2005)



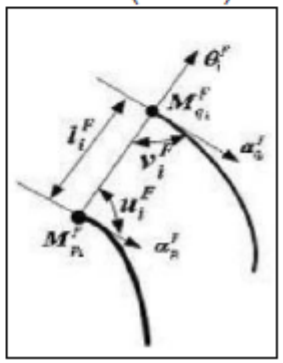
Deng and Huo (2005)



Chikkerur et al. (2006)



He (2006)



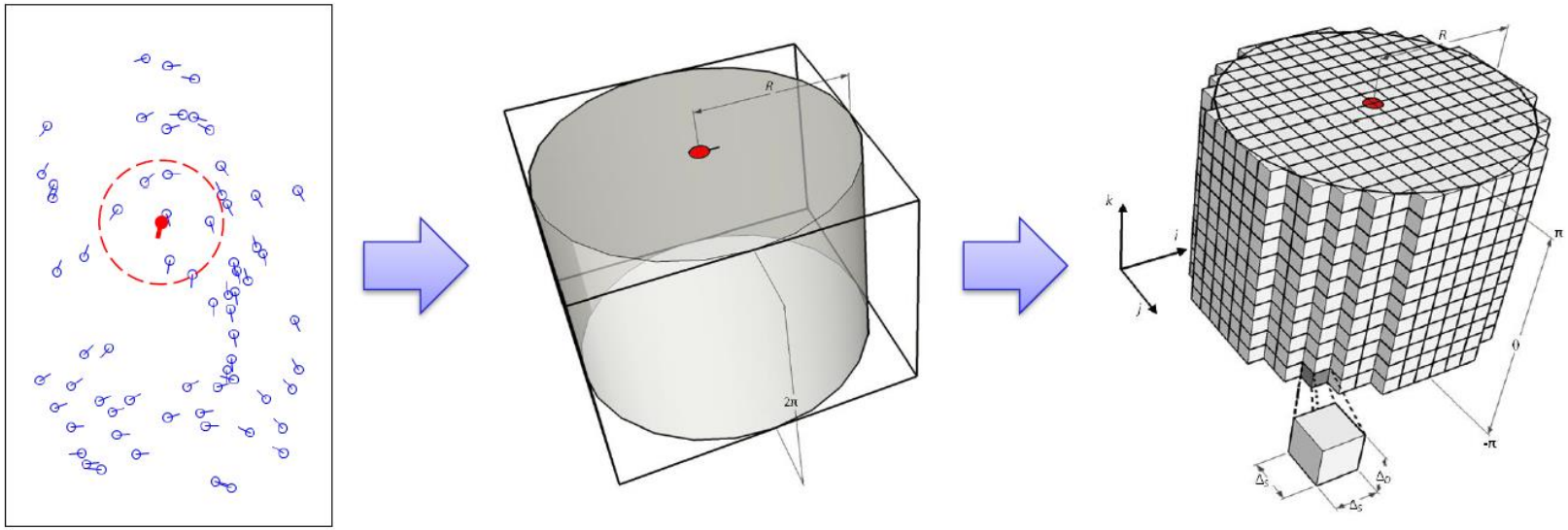
Feng (2008)

Local Minutiae-Based

Minutia Cylinder Code (MCC): representation based on 3D data structures (cylinders) built from minutiae distances and angles.

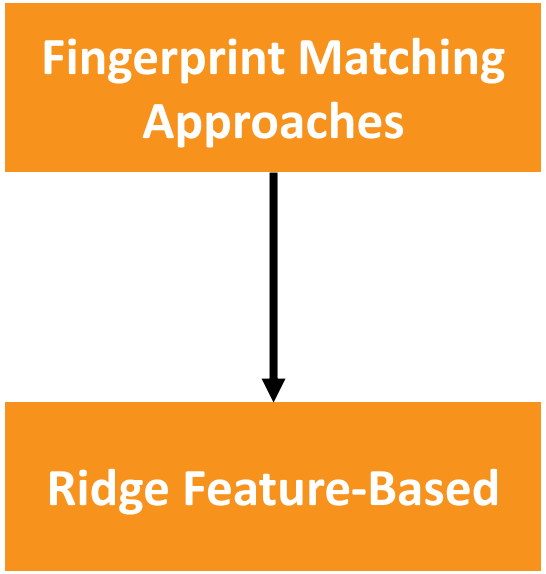
Advantages:

- Fixed-radius structure.
- Fixed-length structure.
- Toleration of local distortion and small feature extraction errors.
- Bit-oriented coding.
- Fast and simple local structure comparison phase.



- R. Cappelli, M. Ferrara, and D. Maltoni, “Fingerprint indexing based on minutia cylinder-code,” IEEE Transactions on Pattern Analysis and Machine Intelligence, 33(5), 1051-1057, 2010.

Matching: Approaches



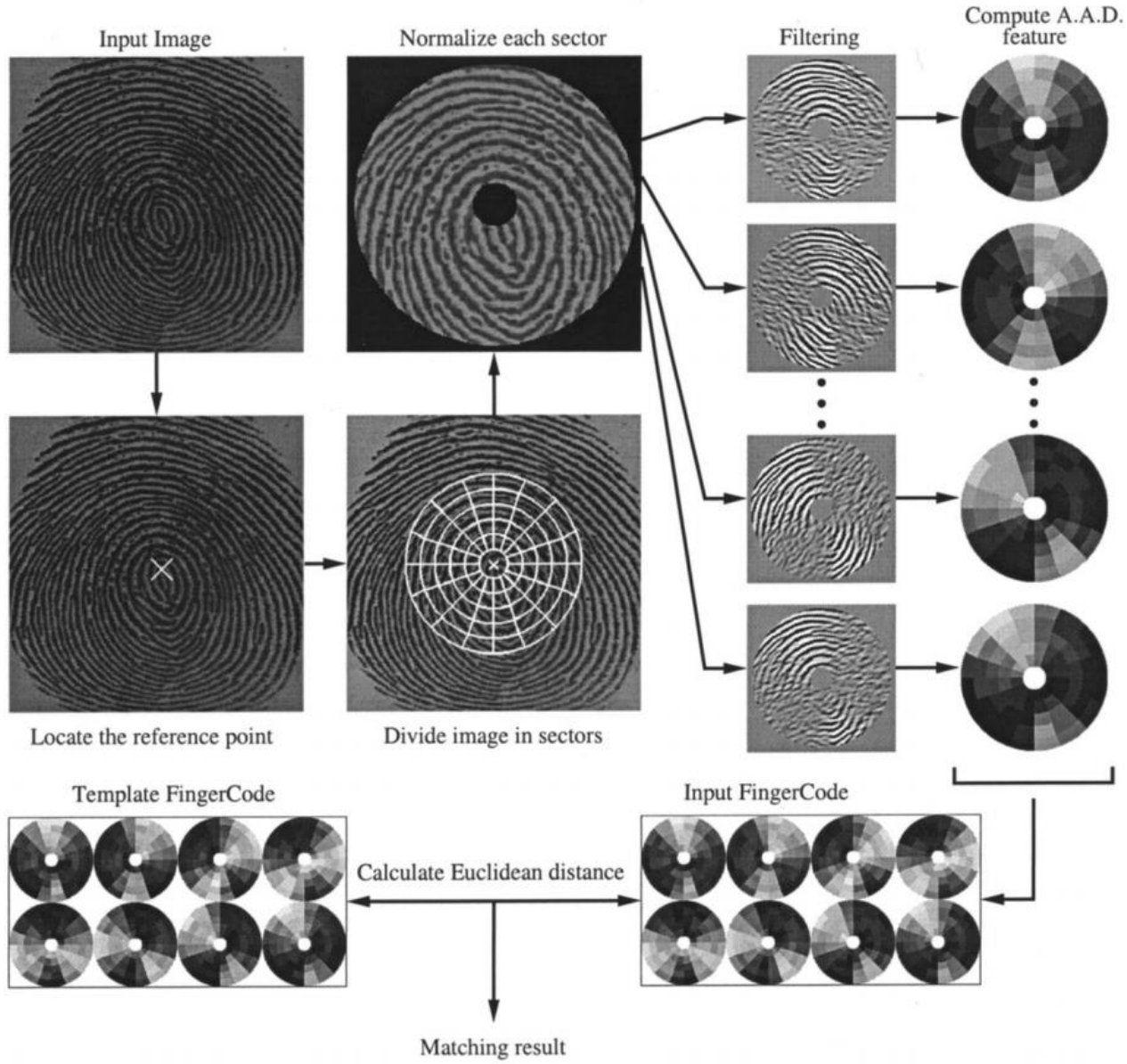
Ridge Feature-Based

FingerCode: Based on texture information.

- Using a bank of Gabor Filters.
- Matching: simple Euclidean distance.

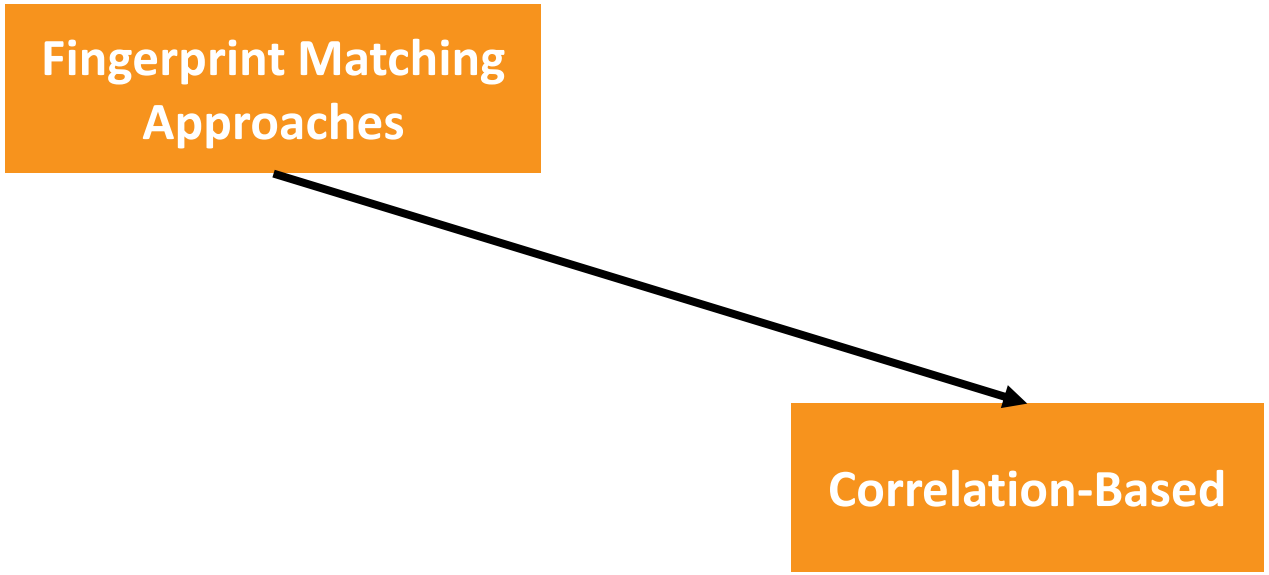
Advantage: Very fast.

A.A.D. = Average Absolute Deviation from the mean of gray values of individual sectors.



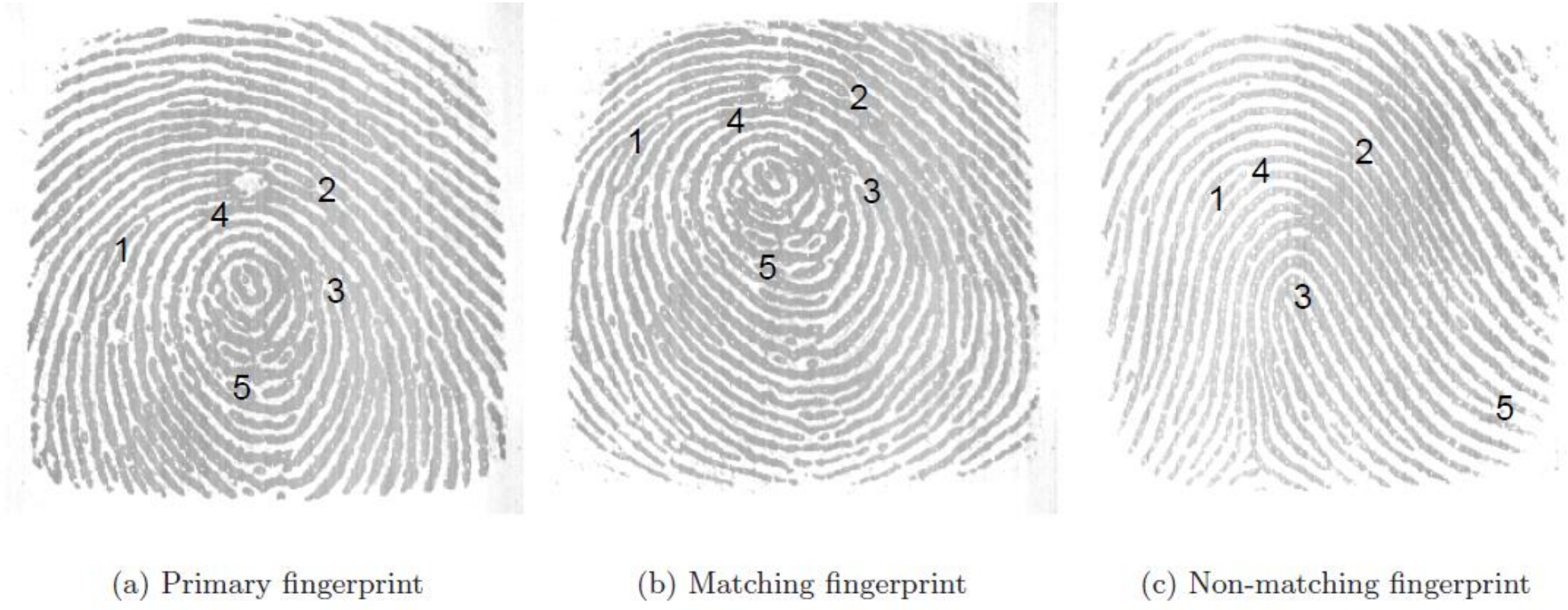
- A. K. Jain, S. Prabhakar, L. Hong and S. Pankanti, “Filterbank-Based Fingerprint Matching,” IEEE Transactions on Image Processing, vol. 9, n.5, pp. 846-859, 2000.

Matching: Approaches



Correlation Based

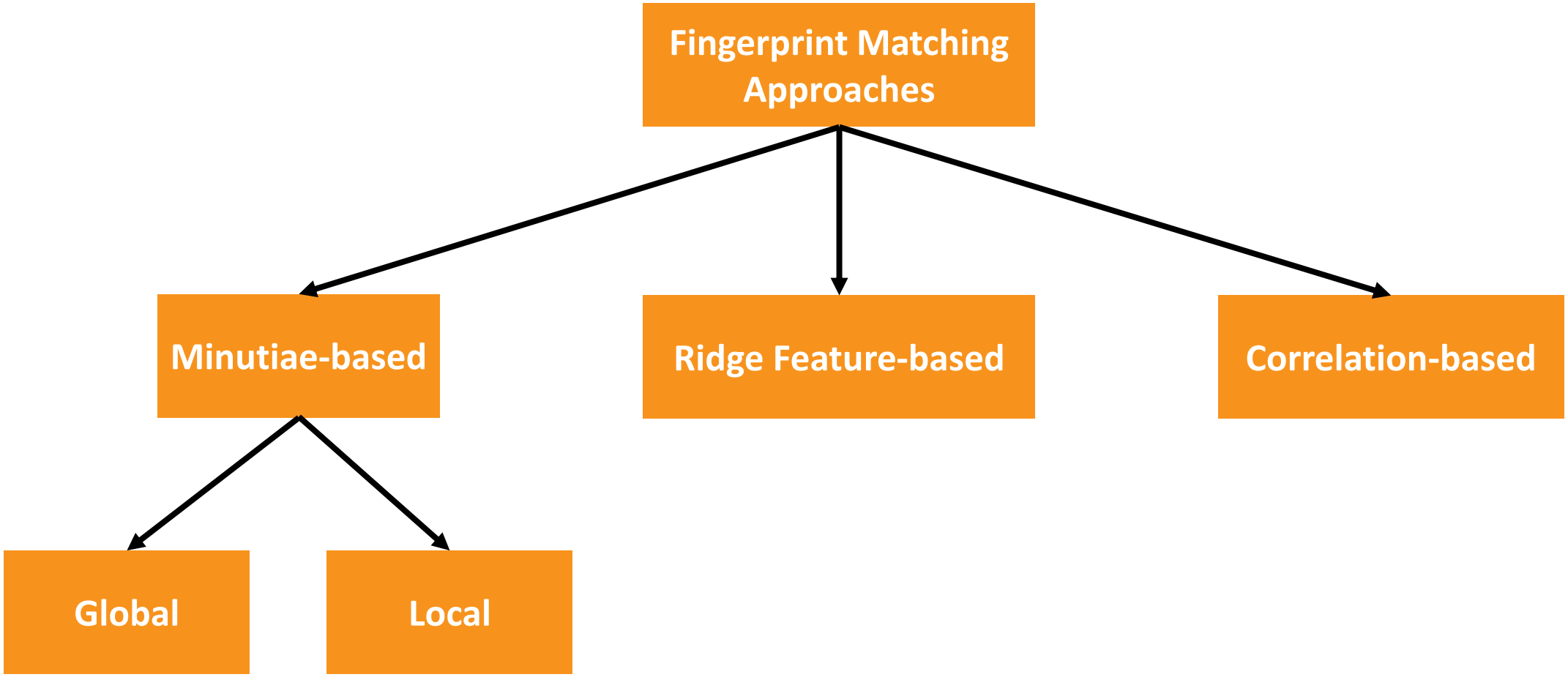
Two fingerprints are superimposed and the correlation between corresponding pixels is computed for different alignments.



(a) Primary fingerprint (b) Matching fingerprint (c) Non-matching fingerprint

- A. M. Bazen, G. T. Verwaaijen, S. H. Gerez, L. P. Veelenturf, and B. J. Van Der Zwaag, "A correlation-based fingerprint verification system," In Proc. Workshop on Circuits, Systems and Signal Processing, 2000.

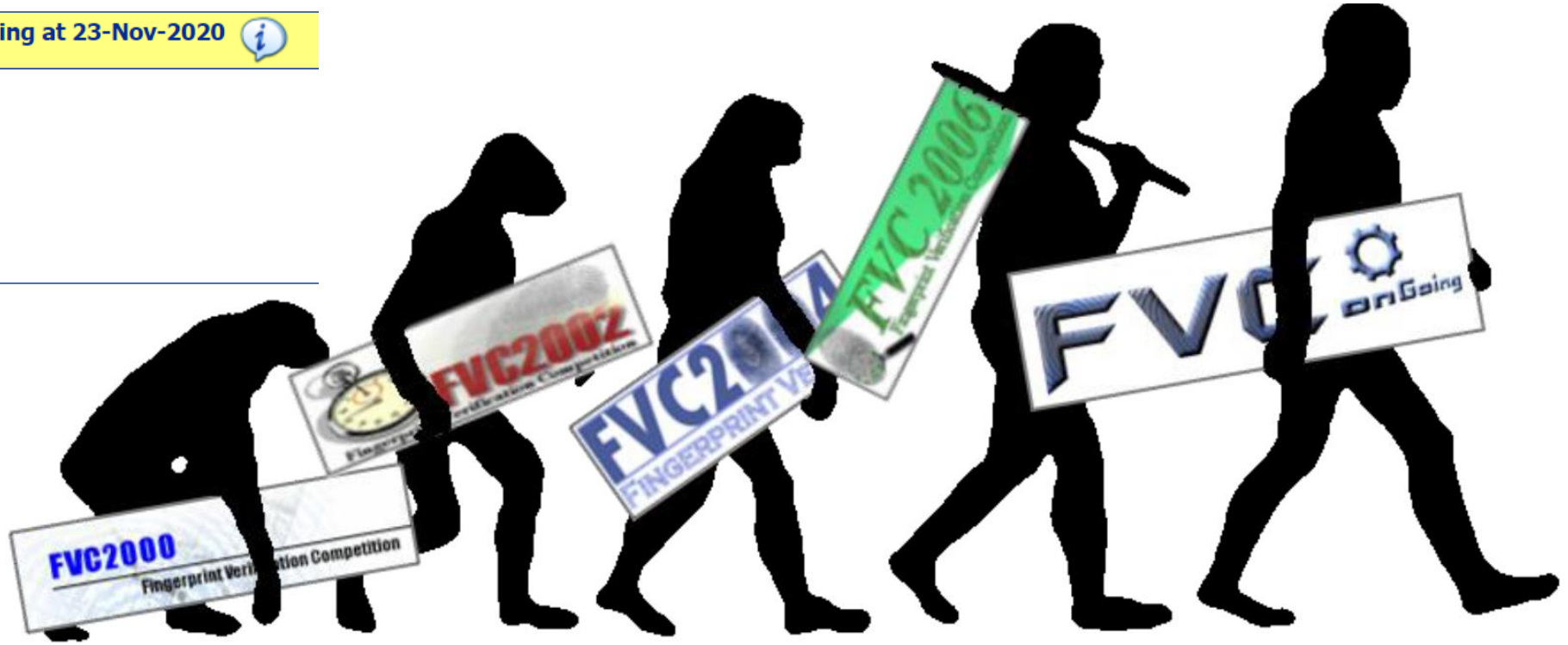
Matching: Approaches



Fingerprint Verification Competition (FVC)

FVC was born in 2000 as a strongly supervised evaluation for fingerprint verification algorithms to:

- Track the state of the art.
- To provide benchmarks and testing protocols for a fair evaluation.



- A. M. Bazen, G. T. Verwaaijen, S. H. Gerez, L. P. Veelenturf, and B. J. Van Der Zwaag, “A correlation-based fingerprint verification system,“ In Proc. Workshop on Circuits, Systems and Signal Processing, 2000.

Fingerprint Verification Competition (FVC)

FVC-Ongoing results on STD-1.0 database (operational conditions):

Fingerprint Verification

Published on	Benchmark	Participant	Type	Algorithm	Version	EER ▲	FMR_{1000}	FMR_{10000}	Show details
01/05/2020	FV-STD-1.0	Neurotechnology	Company	MM_FV	12.0	0.010 %	0.000 %	0.022 %	
27/07/2017	FV-STD-1.0	Beijing Hisign Bio-info Institute	Company	HXKJ	2.4	0.022 %	0.007 %	0.036 %	
29/08/2011	FV-STD-1.0	Tiger IT Bangladesh	Company	TigerAFIS	1.2ec	0.108 %	0.115 %	0.242 %	
14/09/2010	FV-STD-1.0	Green Bit S.p.A	Company	GBFRSW	1.3.2.0	0.118 %	0.155 %	0.519 %	
31/08/2011	FV-STD-1.0	AA Technology Ltd.	Company	EMB9300	1.1	0.142 %	0.159 %	0.220 %	
17/10/2016	FV-STD-1.0	Decatur Industries, Inc.	Company	Decatur	1.2	0.158 %	0.213 %	0.372 %	
15/05/2011	FV-STD-1.0	AA Technology Ltd.	Company	EMB9200	2.3	0.176 %	0.188 %	0.303 %	
15/01/2015	FV-STD-1.0	GenKey Netherlands BV	Company	BioFinger	1.0	0.249 %	0.267 %	0.375 %	
14/05/2011	FV-STD-1.0	Institute of Automation, Chinese Academy of Sciences	Academic Research Group	MntModel	1.0	0.293 %	0.512 %	1.209 %	
15/05/2011	FV-STD-1.0	UnionCommunity	Company	Triple_M	1.1	0.418 %	0.859 %	1.977 %	
20/05/2020	FV-STD-1.0	Beijing Bata Technolgy Co. Ltd.	Company	Bata-FP	2.0	0.432 %	0.595 %	0.869 %	
22/09/2020	FV-STD-1.0	Vsoft	Company	BioPass Finger	2.7	0.488 %	0.992 %	2.940 %	

- URL: https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx

Fingerprint Verification Competition (FVC)

FVC-Ongoing results on HARD 1.0 database (challenging conditions):

Fingerprint Verification

Published on	Benchmark	Participant	Type	Algorithm	Version	EER ▲	FMR_{1000}	FMR_{10000}	Show details
01/05/2020	FV-HARD-1.0	Neurotechnology	Company	MM_FV	12.0	0.214 %	0.342 %	0.626 %	
28/07/2017	FV-HARD-1.0	Beijing Hisign Bio-info Institute	Company	HXKJ	2.4	0.530 %	0.797 %	1.879 %	
29/08/2011	FV-HARD-1.0	Tiger IT Bangladesh	Company	TigerAFIS	1.2ec10	0.687 %	1.077 %	1.781 %	
17/10/2016	FV-HARD-1.0	Decatur Industries, Inc.	Company	Decatur	1.0.2	0.697 %	1.108 %	1.936 %	
02/07/2020	FV-HARD-1.0	Sonda Technologies Ltd.	Company	FPM	4.1.22	0.699 %	0.952 %	1.227 %	
15/05/2011	FV-HARD-1.0	AA Technology Ltd.	Company	EMB9200	2.3	0.700 %	1.247 %	1.817 %	
31/08/2011	FV-HARD-1.0	AA Technology Ltd.	Company	EMB9300	1.1	0.722 %	1.092 %	1.542 %	
14/09/2010	FV-HARD-1.0	Green Bit S.p.A	Company	GBFRSW	1.3.2.0	0.735 %	1.444 %	2.355 %	
14/05/2011	FV-HARD-1.0	Institute of Automation, Chinese Academy of Sciences	Academic Research Group	MntModel	1.0	1.257 %	2.795 %	4.436 %	
15/01/2015	FV-HARD-1.0	GenKey Netherlands BV	Company	BioFinger	1.0	1.489 %	2.127 %	2.914 %	

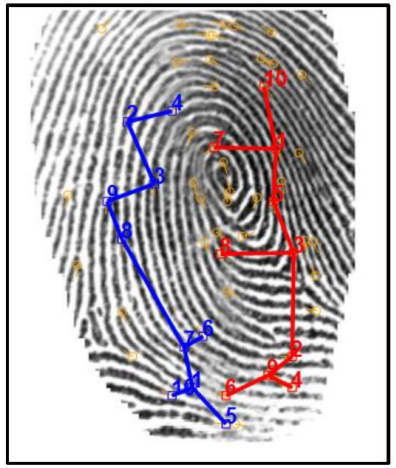
- URL: https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx

Fake Fingerprints (Presentation Attacks)

Altered Fingerprints

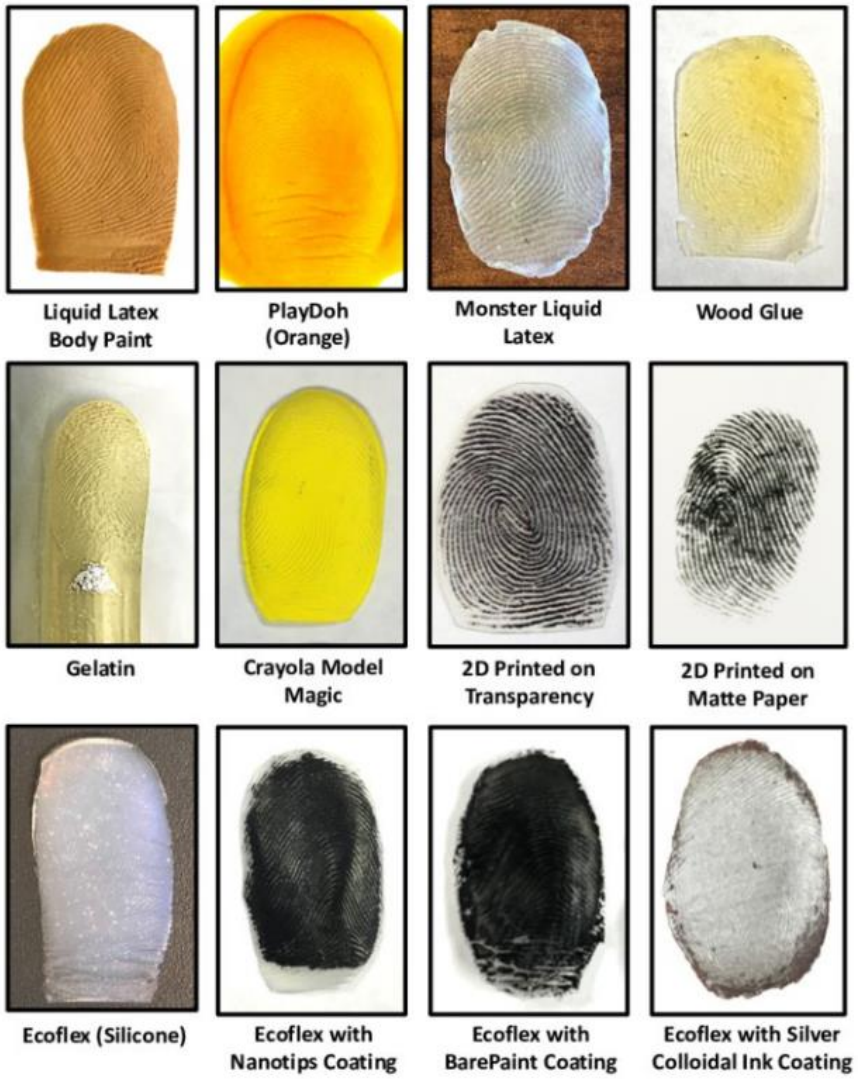
KEY RESEARCH LINES

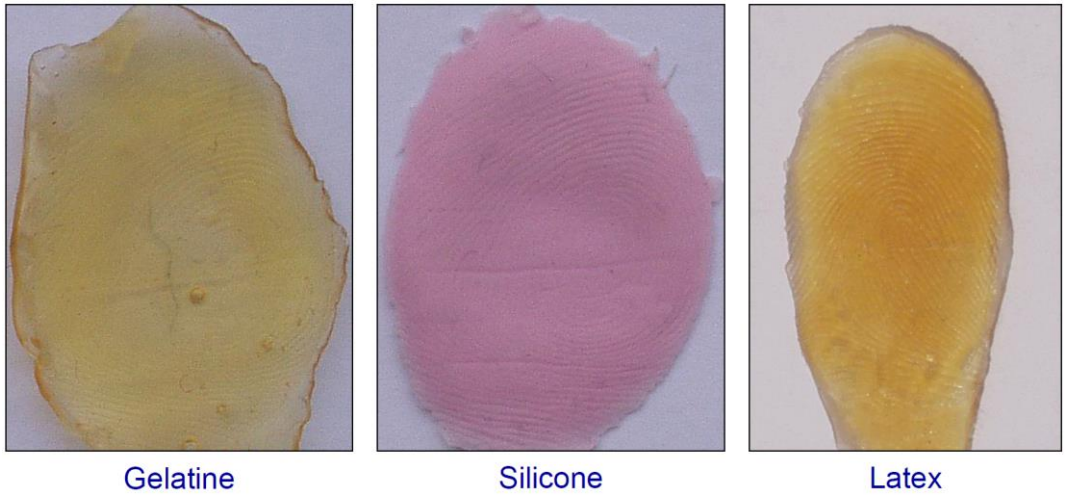
Double-Identity Fingerprints



Latent Fingerprints

Fake Fingerprints (Presentation Attacks)





- R. Tolosana, M. Gomez-Barrero, C. Busch and J. Ortega-Garcia, “Biometric presentation attack detection: Beyond the visible spectrum”, IEEE Transactions on Information Forensics and Security, vol 15, pp. 1261-1275, 2019.

Altered Fingerprints

Criminals who want to avoid identification will try almost any method to irreversibly alter their fingerprints

Transplanted

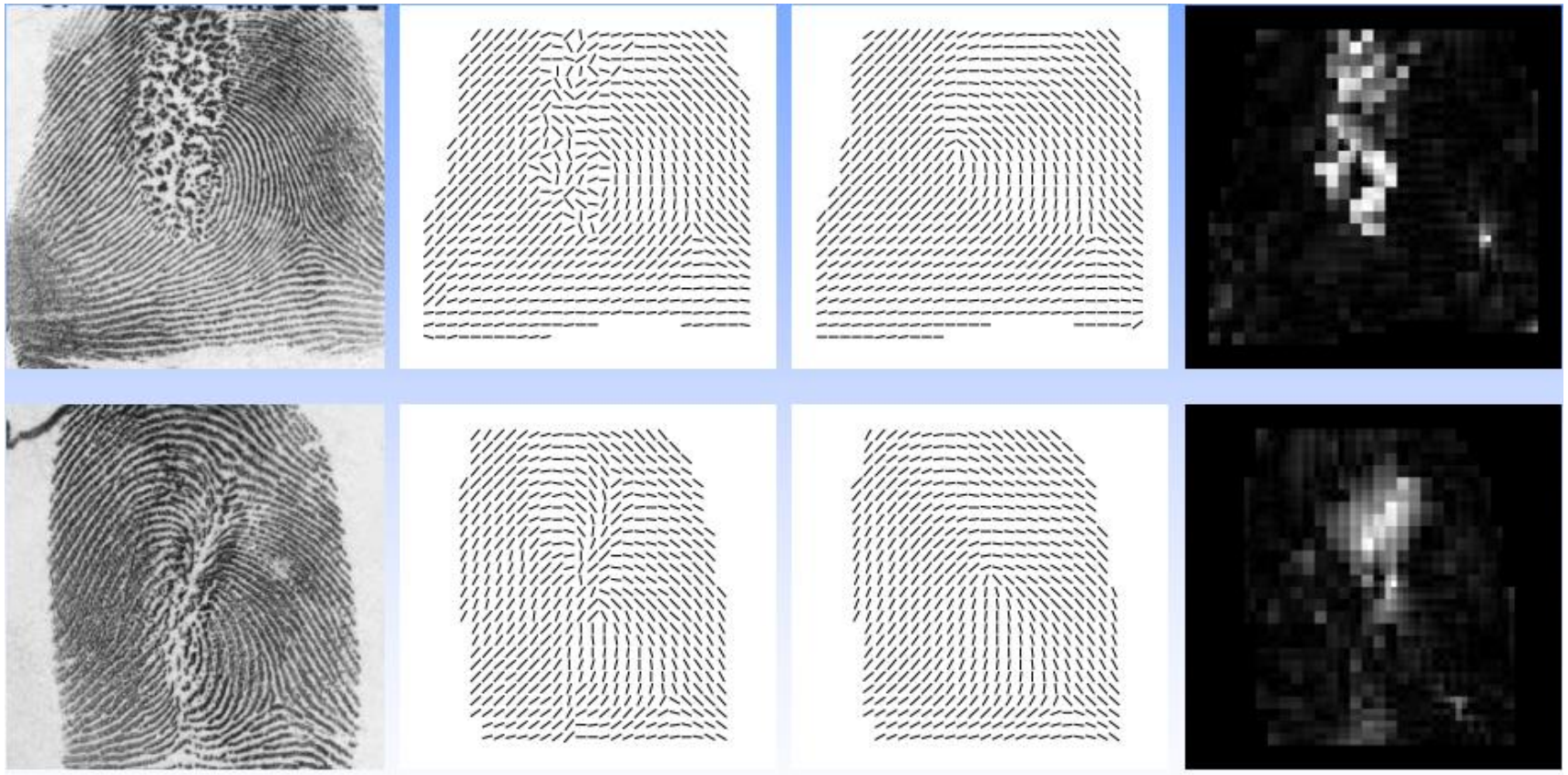
Bitten

Burnt with acid

Surgically altered

Altered Fingerprints

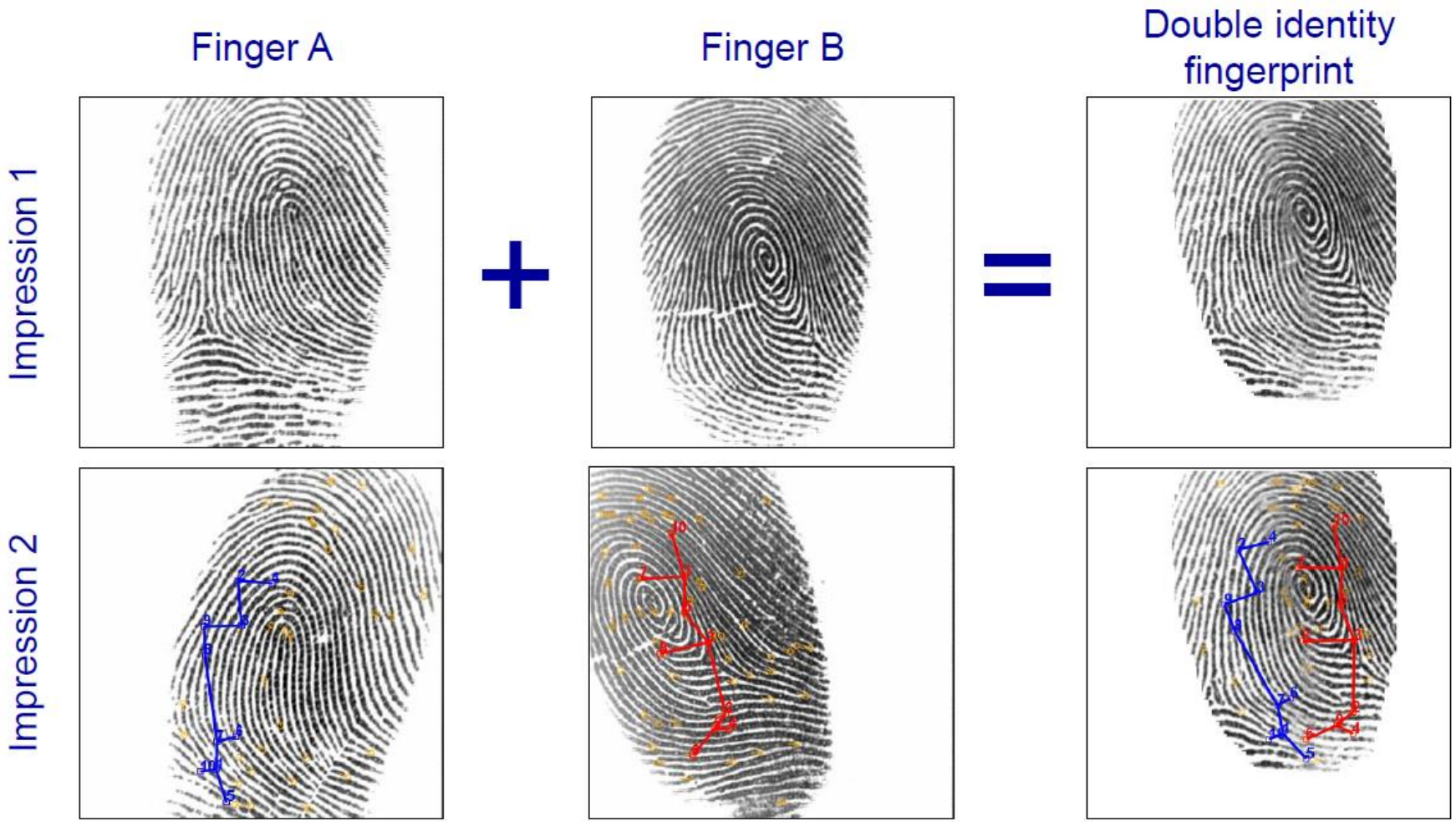
Criminals who want to avoid identification will try almost any method to irreversibly alter their fingerprints



Error is concentrated near the altered regions of the print

Double-Identity Fingerprints

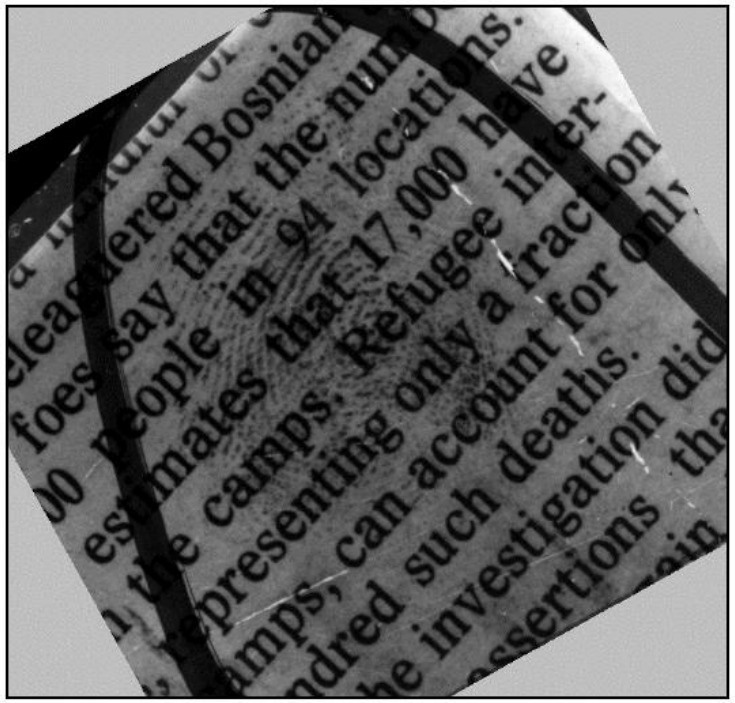
Double-identity fingerprint is a fake fingerprint created by combining features from two different fingers, so that it has a high chance to be falsely matched with fingerprints from both fingers.

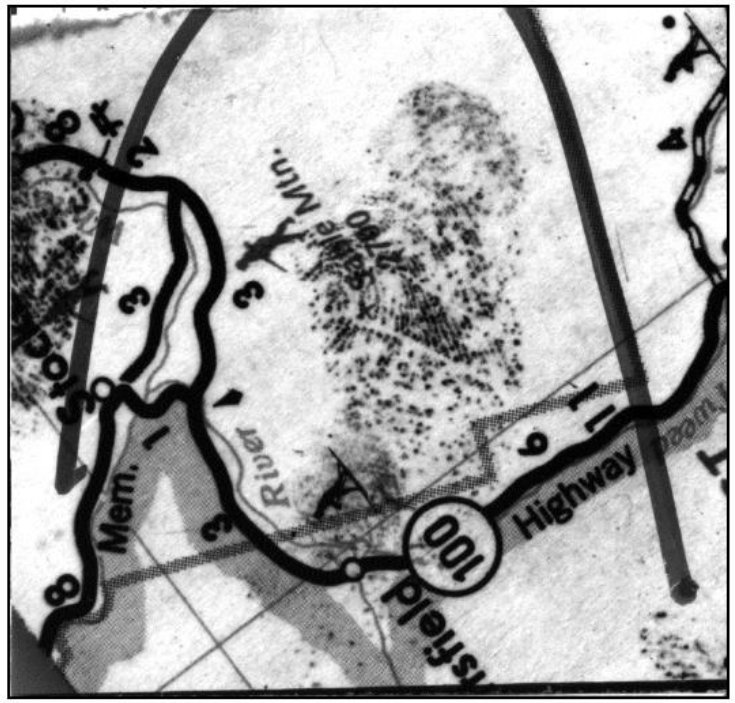


Latent Fingerprints

A latent fingerprint is an invisible fingerprint left on a surface by deposits of oils and/or perspiration from the finger. Usually it can be detected with the application of chemical or physical methods.

The key problem is reliably estimating the context (local orientations and frequencies).





Key References

- D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition. Springer Science & Business Media, 2009.
- S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun and D. Zhang, “Biometric recognition using deep learning: A survey.” arXiv:1912.00271, 2020.
- R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman and A. K. Jain, “Performance evaluation of fingerprint verification systems,” IEEE Transactions on Pattern Analysis and Machine Intelligence, 28(1), 3-18, 2005.
- R. Cappelli, M. Ferrara and D. Maltoni, “Large-scale fingerprint identification on GPU,” Information Sciences, 306, 1-20, 2015.
- R. Cappelli, M. Ferrara, A. Franco and D. Maltoni, “Fingerprint verification competition 2006,” Biometric Technology Today, 15(7-8), 7-9, 2007.
- R. Tolosana, M. Gomez-Barrero, C. Busch and J. Ortega-Garcia, “Biometric presentation attack detection: Beyond the visible spectrum”, IEEE Transactions on Information Forensics and Security, vol 15, pp. 1261-1275, 2019.
- C. Sousedik and C. Busch, “Presentation attack detection methods for fingerprint recognition systems: a survey", IET Biometrics, vol. 3, pp. 219–233, 2014.
- E. Marasco and A. Ross, “A survey on antispoofing schemes for fingerprint recognition systems", ACM Computing Surveys, 2015.
- K. Cao, and A. K. Jain, “Automated latent fingerprint recognition,” IEEE Transactions on Pattern Analysis and Machine Intelligence, 41(4), 788-800, 2018.
- D. Valdes-Ramirez, M.A. Medina-Pérez, R. Monroy, O. Loyola-González, J. Rodríguez-Ruiz, A. Morales and F. Herrera, “A Review of Fingerprint Feature Representations and Their Applications for Latent Fingerprint Identification: Trends and Evaluation,” IEEE Access, 7, 48484-48499, 2019.
- A. Sankaran, M. Vatsa and R. Singh, “Latent fingerprint matching: A survey,” IEEE Access, 2, 982-1004, 2014.
- A. K. Jain, K. Nandakumar, and A. Ross, “50 years of biometric research: Accomplishments, challenges, and opportunities.” Pattern Recognition Letters, 79, 80-105, 2016.

Fingerprint Recognition

Part of the content is based on the tutorial by Annalisa Franco (IAPR/IEEE Winter School on Biometrics 2020)

BiDA Lab
Biometrics & Data Pattern Analytics Lab

UAM
Universidad Autónoma de Madrid