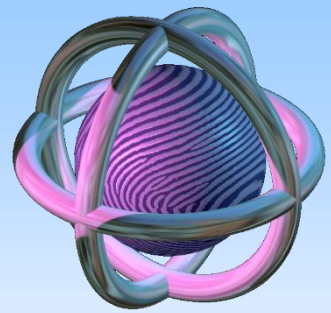
**Annalisa Franco**

**Biometric System Laboratory**
University of Bologna - ITALY

**http://biolab.csr.unibo.it**



# Fingerprint recognition

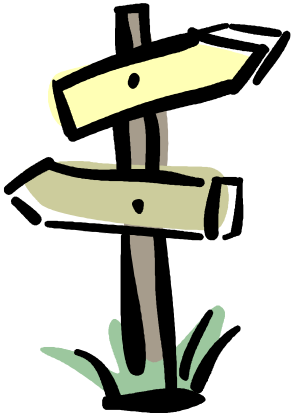
## State-of-the-art and new directions

**IAPR/IEEE WINTER SCHOOL ON BIOMETRICS 2018**
12 Jan – 16 Jan 2020 | Shenzhen, China

# Outline

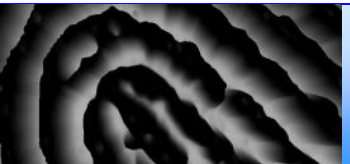
State-of-the-art

- Fingerprint anatomy
- Fingerprint acquisition
- Feature extraction
- Fingerprint comparison
- Performance evaluation



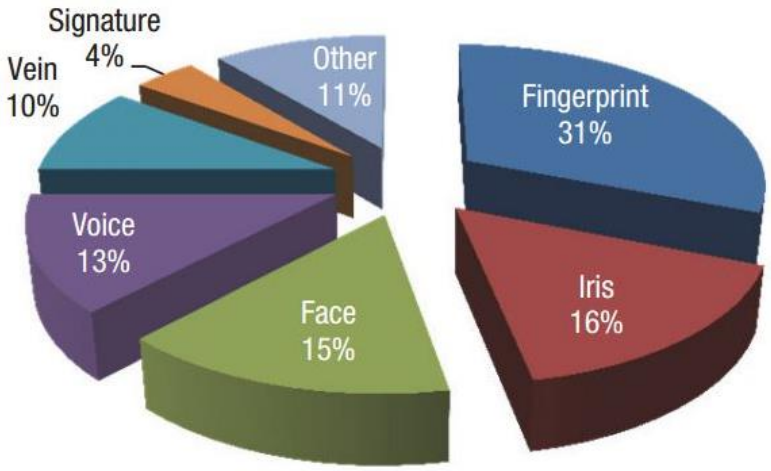
Main challenges

- Fake fingerprints
- Double-identity fingerprints
- Altered fingerprints
- Latent fingerprints



# Why fingerprints?

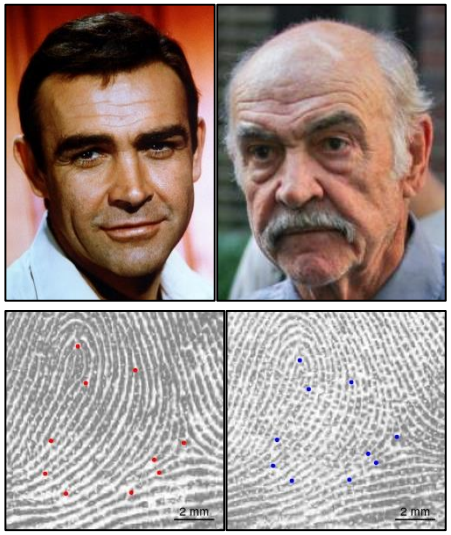
## Biometrics market share (2016)



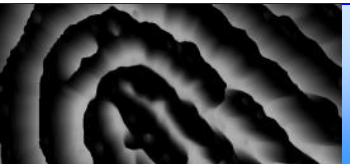

- Highly distinctive and unique
- Persistent
- Publicly accepted as reliable (evidence in a court of law)

## Identical twins have different fingerprints

## Do not change during the lifetime of a person

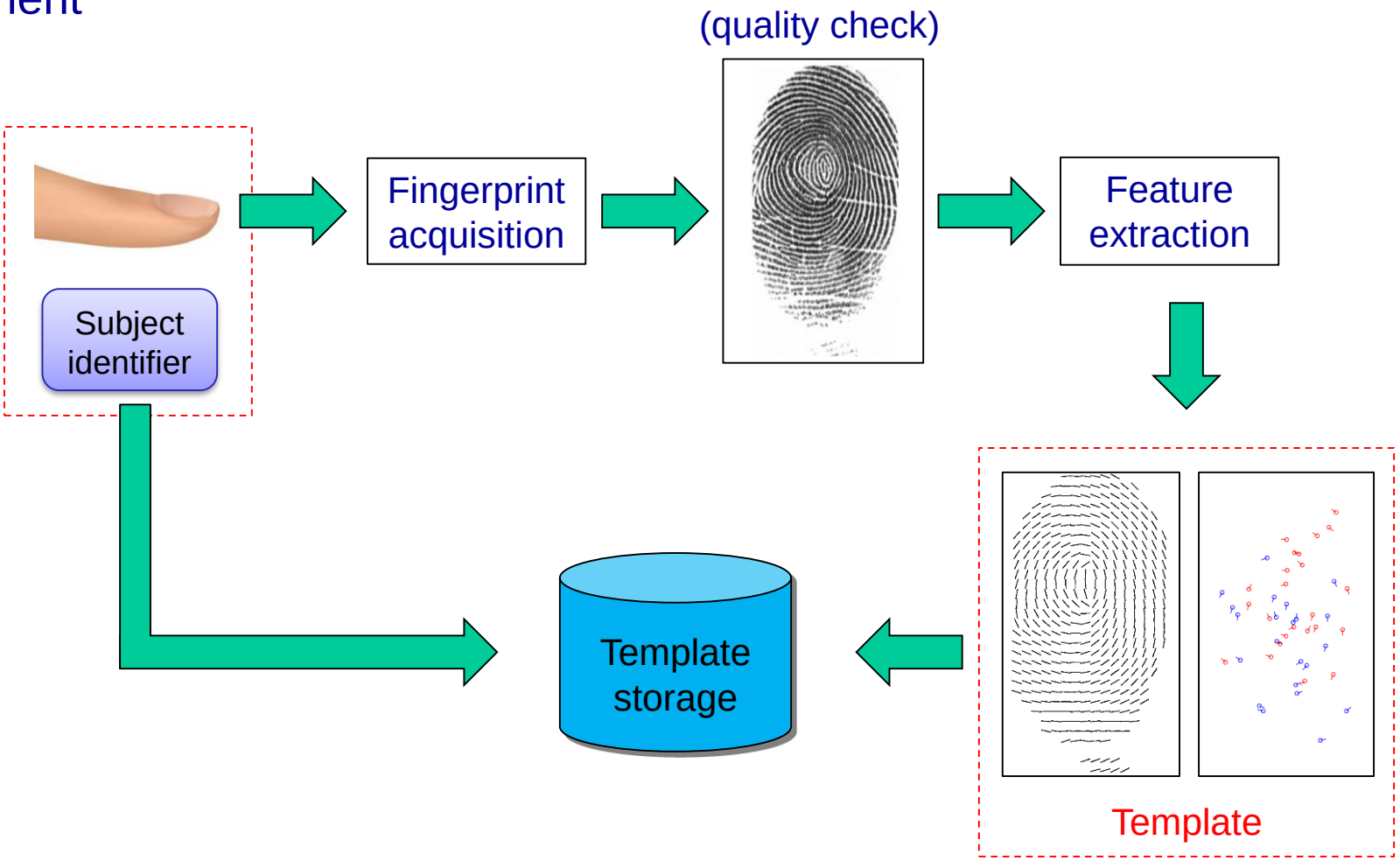



Their uniqueness is not proved but it has been accepted over time on the assumption that salient fingerprint features of different fingers are clearly different.



# How does a biometric system work? (1)

## Enrolment



# How does a biometric system work? (2)

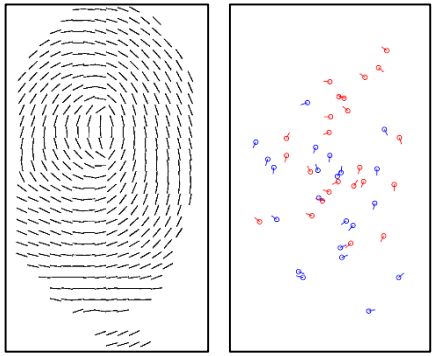
## Verification

Claimed identifier

Fingerprint acquisition

Feature extraction

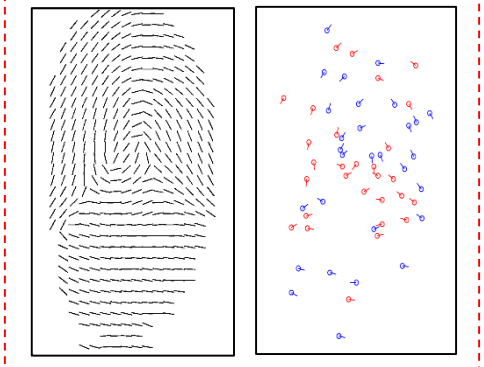
Template storage



Claimed Template

Comparison

Match/Non-match



Template

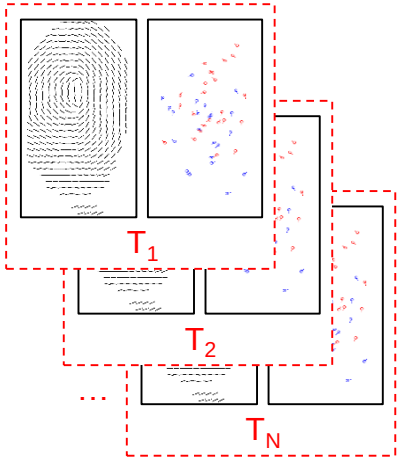
# How does a biometric system work? (3)

## Identification

Fingerprint acquisition

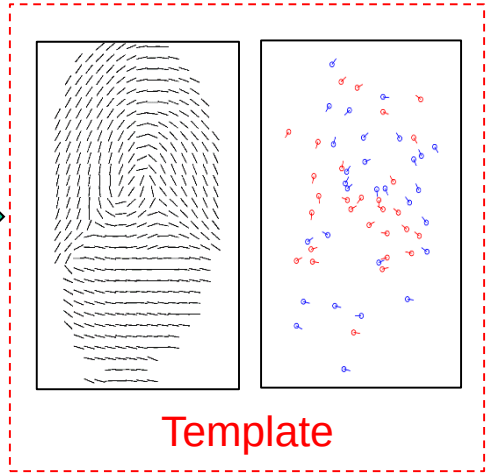
Feature extraction

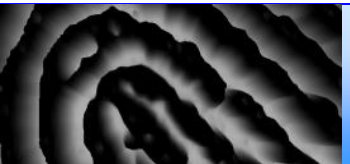
Template storage




Pre-selection and comparison

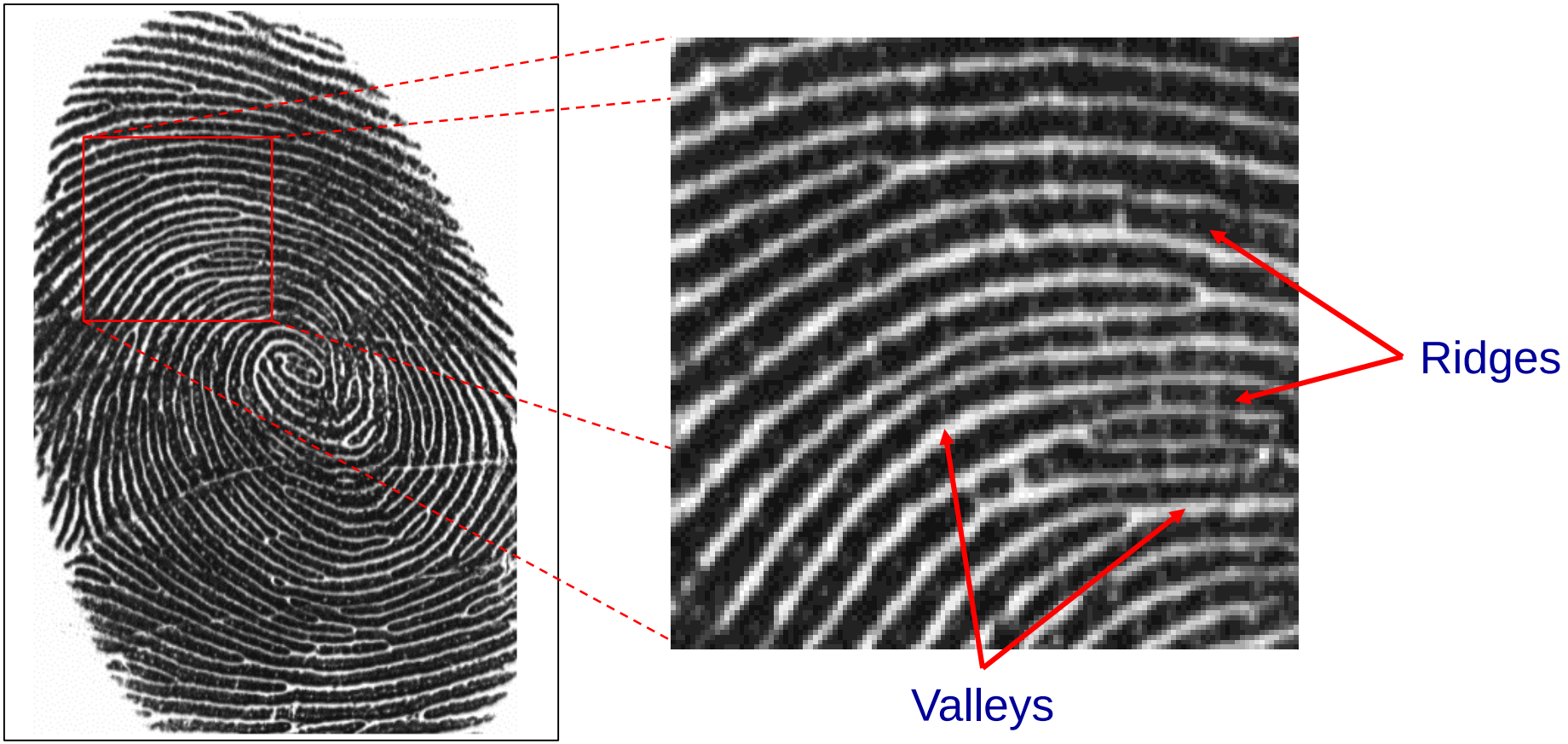
Candidate list or "not identified"

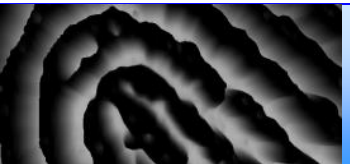


# Fingerprint anatomy

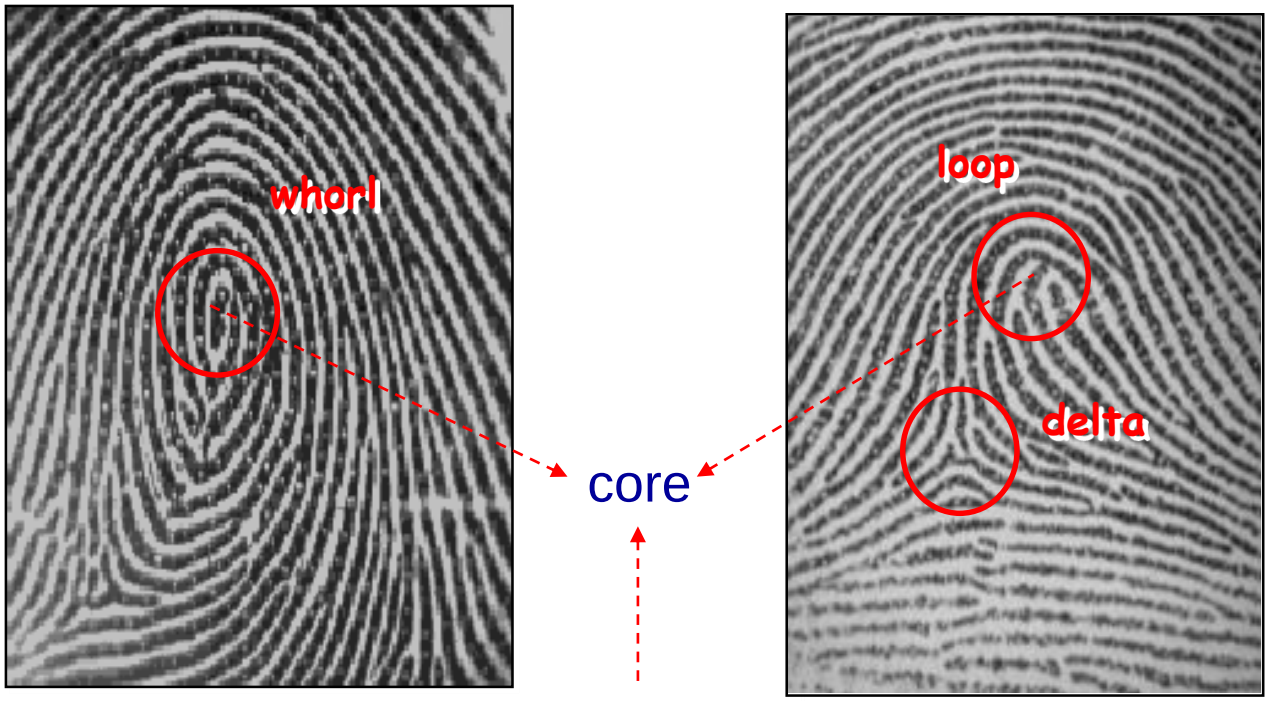
A fingerprint is composed of a set of lines (ridge lines), which mainly flow parallel, making a pattern (ridge pattern).



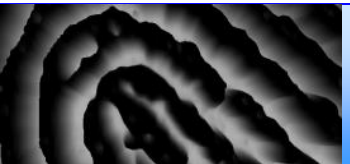



# Singularities

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

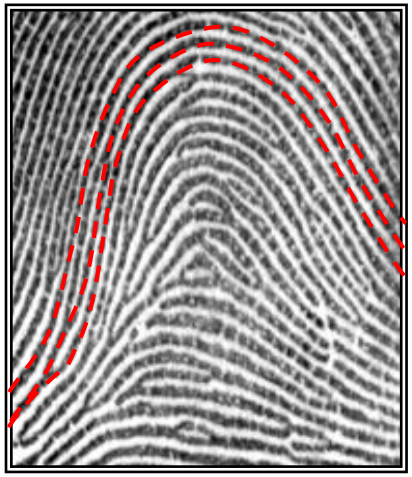



The center of the north most loop/whorl type singularity

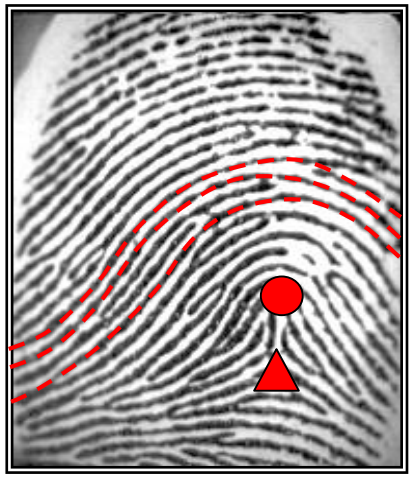


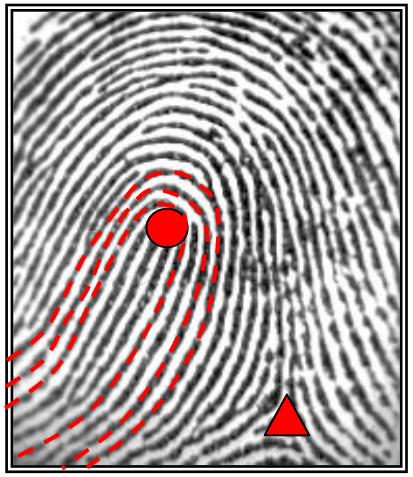
# Classes

arch (plain)

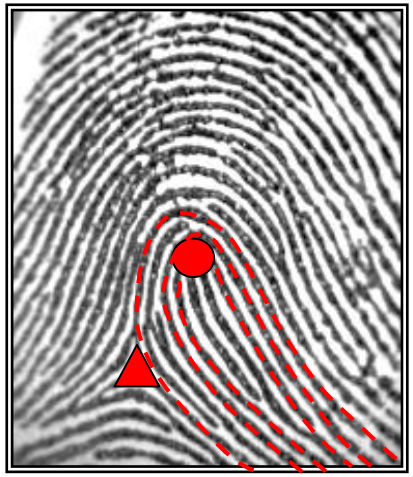


tented arch

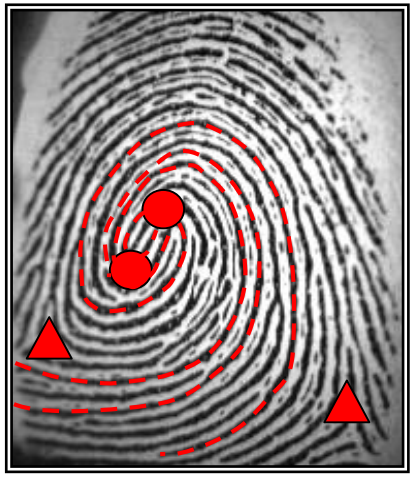




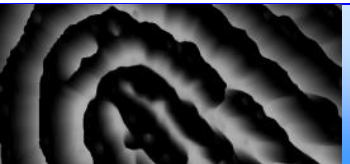
left loop



right loop

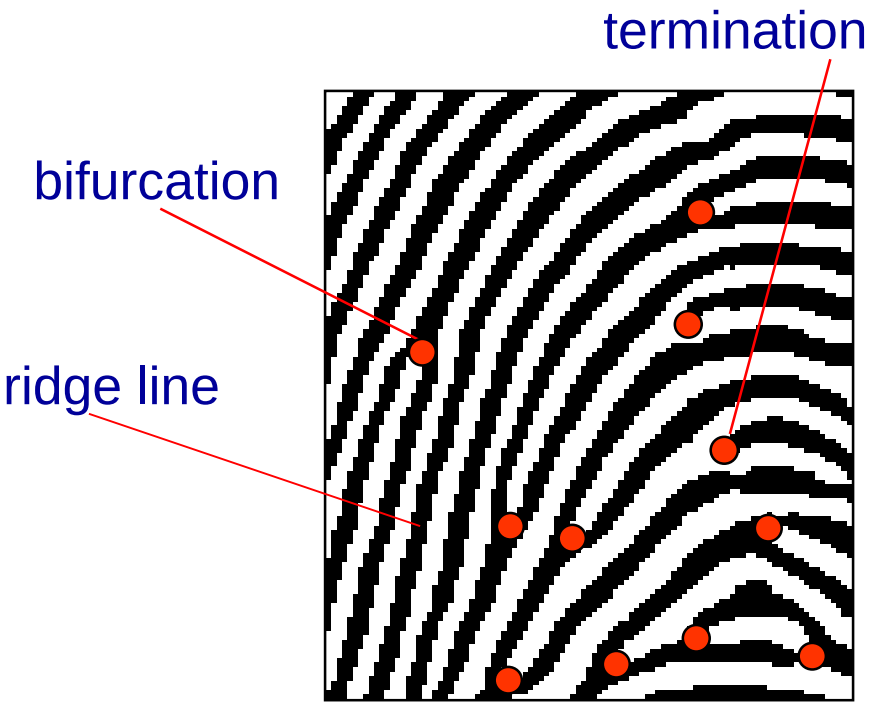


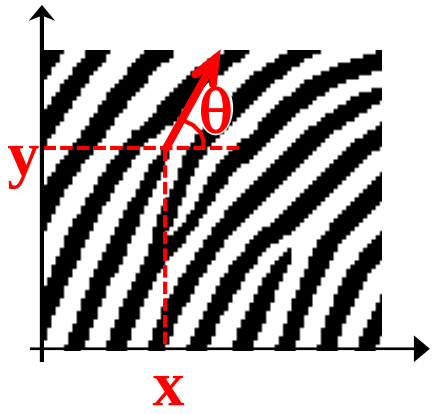
whorl



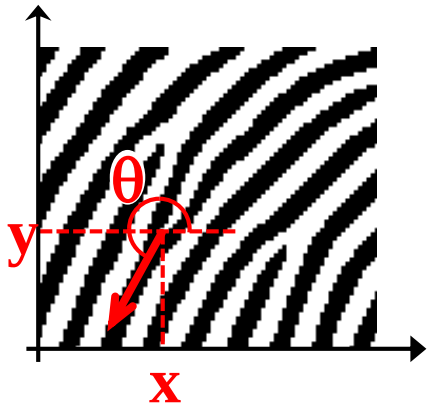
# Minutiae

Minutiae are determined by the termination or the bifurcation of the ridge lines and usually are represented the coordinates $(x, y)$, the angle $\theta$ between the minutia tangent and the horizontal axis and the type (termination/bifurcation).

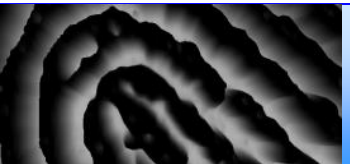



termination




bifurcation

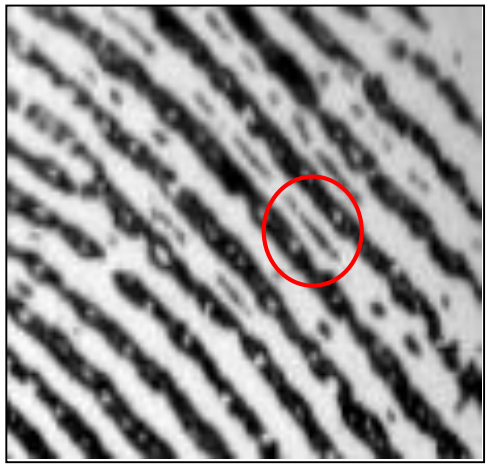


# Sweat pores

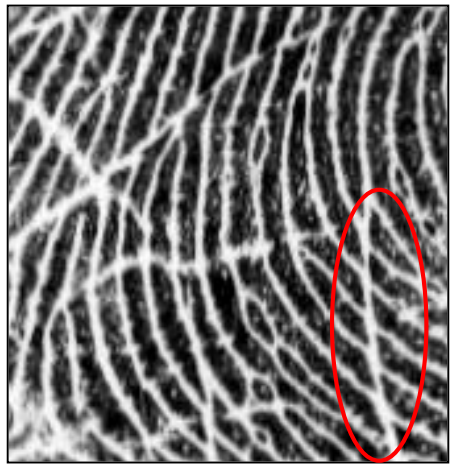
At the very-fine level (e.g., acquisition at 1000 dpi) it is possible to identify sweat pores (from 60 to 250 μm), incipient ridges, creases, etc.

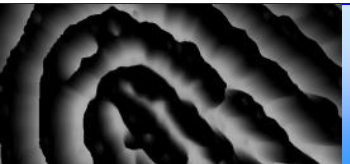
sweat pores

incipient ridges

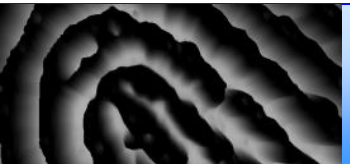


creases

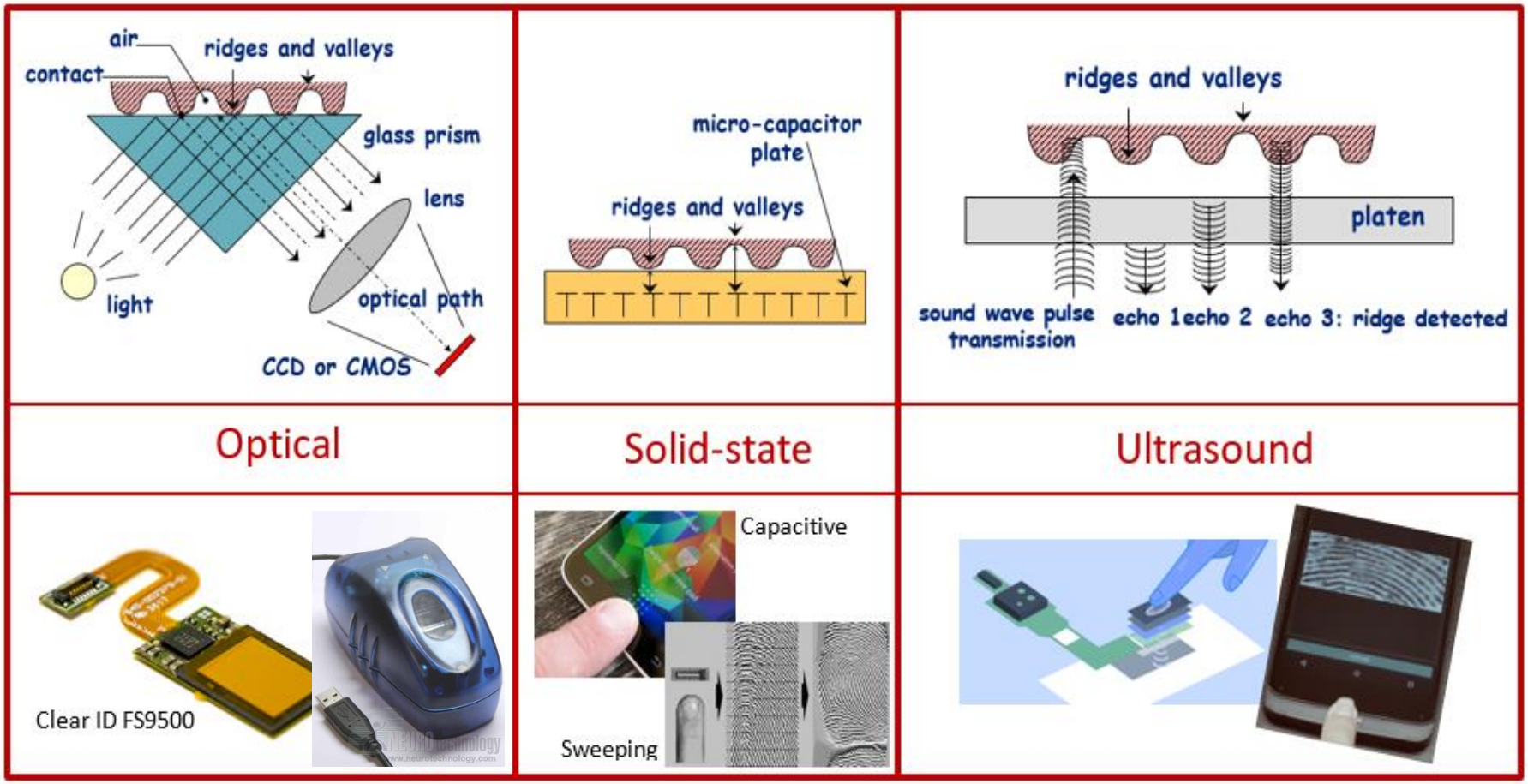




# Video



# Online fingerprint acquisition (1)



# Online fingerprint acquisition (2)

## Optical

HiScan

Verifier 300 LC 2.0

MSO350

UareU 4000

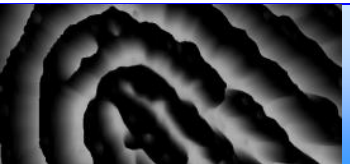
## Capacitive

TouchChip TCS1

AES 4000

## Thermal

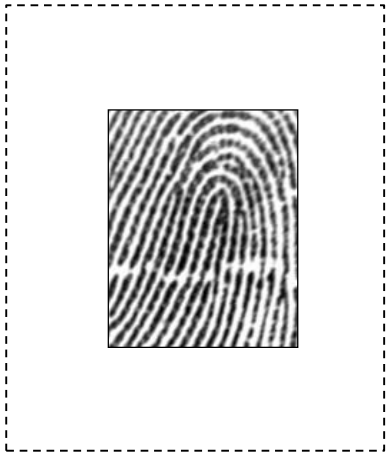
FingerChip AT77C101B



# Main device parameters



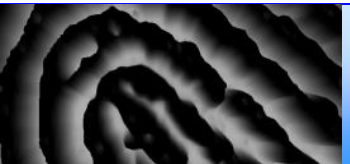
Resolution



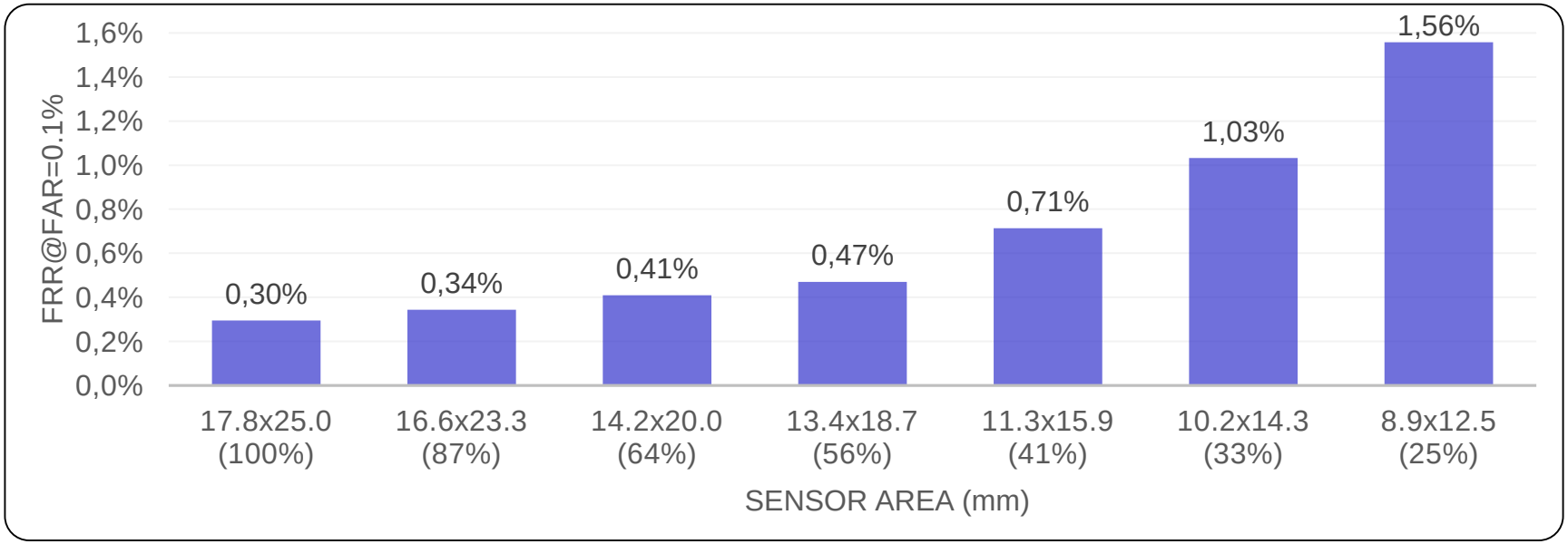
Acquisition area

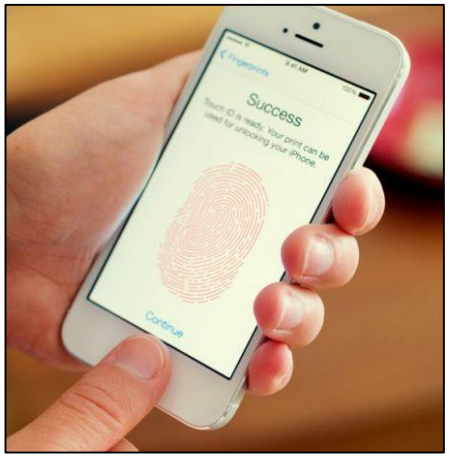
Dynamic range

Geometric accuracy



# Problems with small area sensors



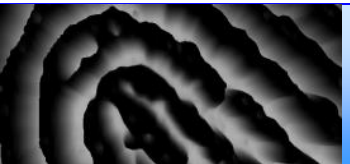




"Comparing small patches increases the risk of false matches"

Roy, Memon & Ross

MasterPrint: Exploring the Vulnerability of Partial Fingerprint-based Authentication Systems

IEEE Transactions on Information Forensics & Security, 2017

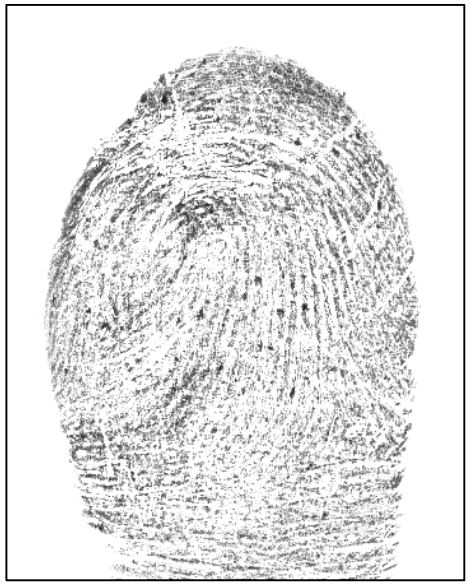


# Optical Coherence Tomography (OCT) sensor

In particular scenarios, imaging below fingertip surface might be a useful alternative to traditional fingerprint sensing:

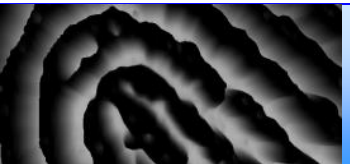
- altered fingerprints (intentional/unintentional)
- fake fingerprints

Optical scanner
(fingertip surface)



Optical Coherence Tomography
(below fingertip surface)

After one hour of sand paper!



# Smartphone camera

Fingerprint acquisition using a high resolution smartphone camera could be a suitable solution in specific scenarios such as:

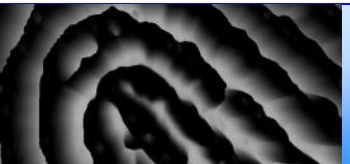
- border control
- eDocument verification
- smartphone login

Main problems:

- low contrast
- complex background
- natural lighting
- finger distance and rotation with respect to the camera

Optical scanner

Smartphone camera



# Image quality

Low quality fingerprints:

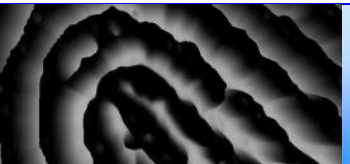
- scarcely prominent ridge lines (manual workers, elderly people)
- too dry or to wet fingerprints

Good quality

Dry fingerprint

Wet fingerprint

Intrinsically low quality image



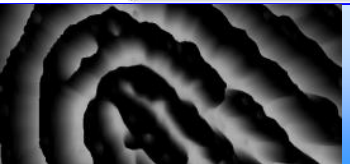
# NFIQ

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

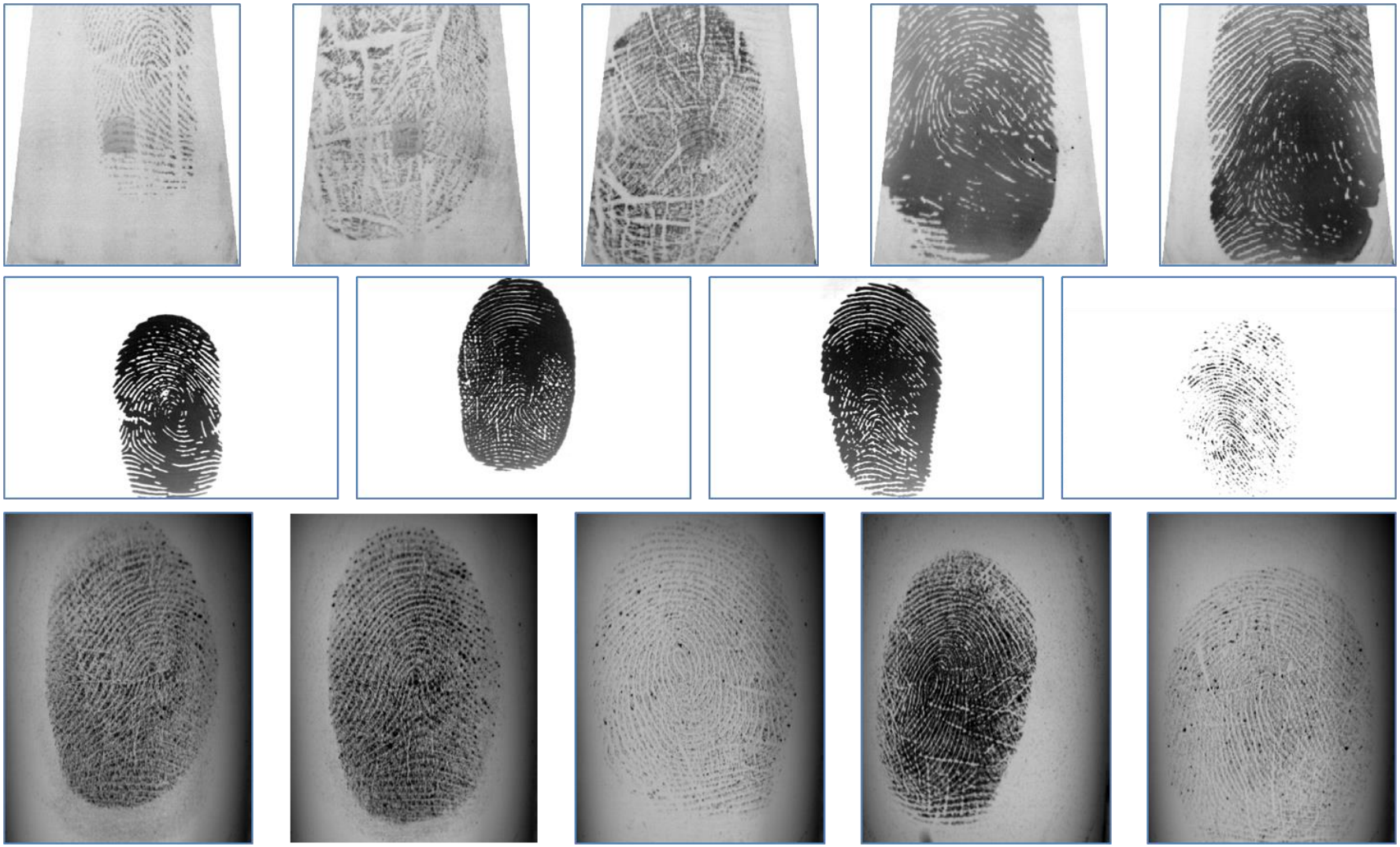
NFIQ (1.0) assigns to a fingerprint a value in {1,2,3,4,5} which is in inverse proportion with its quality.

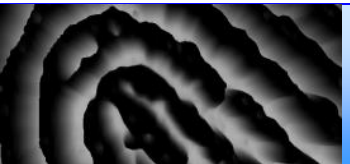
NFIQ is an operational quality aimed at predicting automatic fingerprint recognition performance:

- 1 → excellent quality → small errors → high accuracy
- 5 → poor quality → high errors → low accuracy

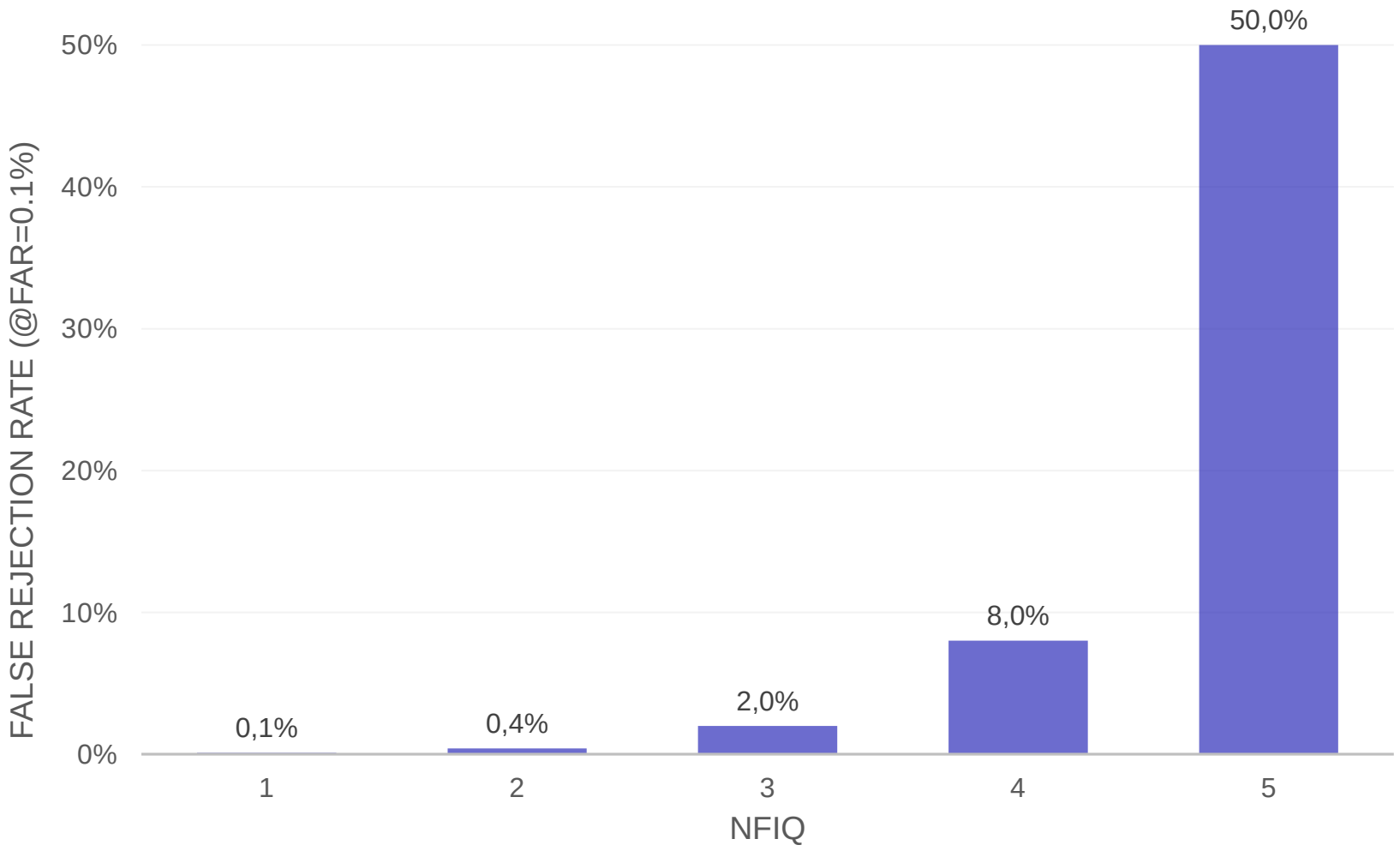



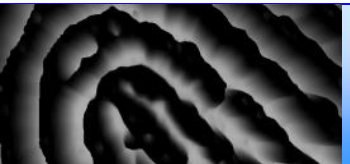
# NFIQ=5 examples





# Quality/accuracy tradeoff



# NFIQ 2.0

Released April 2016 (open source)

NFIQ 2.0 quality value is in [0..100]

- 0 lowest quality value
- 100 highest quality value

Quality features

- 155 evaluated
- 14 selected (e.g., orientation certainty, ridge valley uniformity, …)

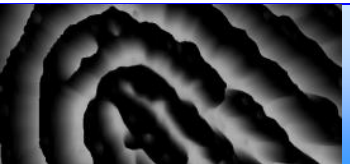
91

61

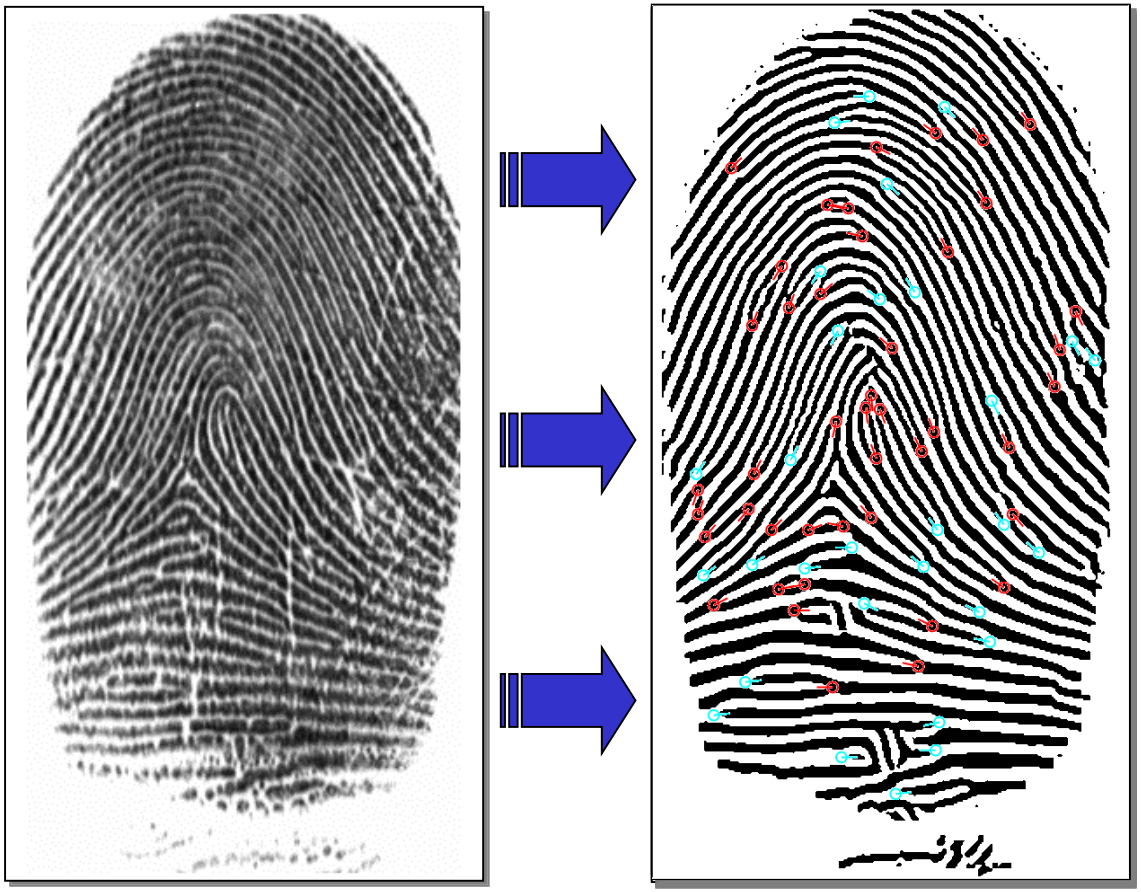
41

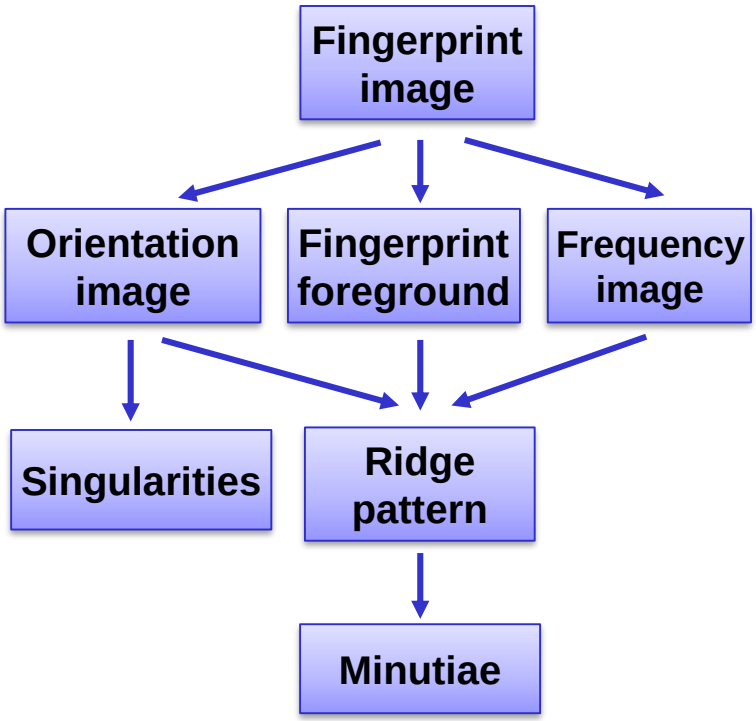
21

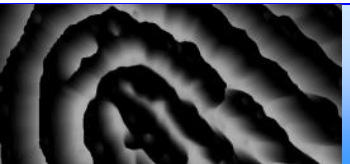
1



# Feature extraction: main steps



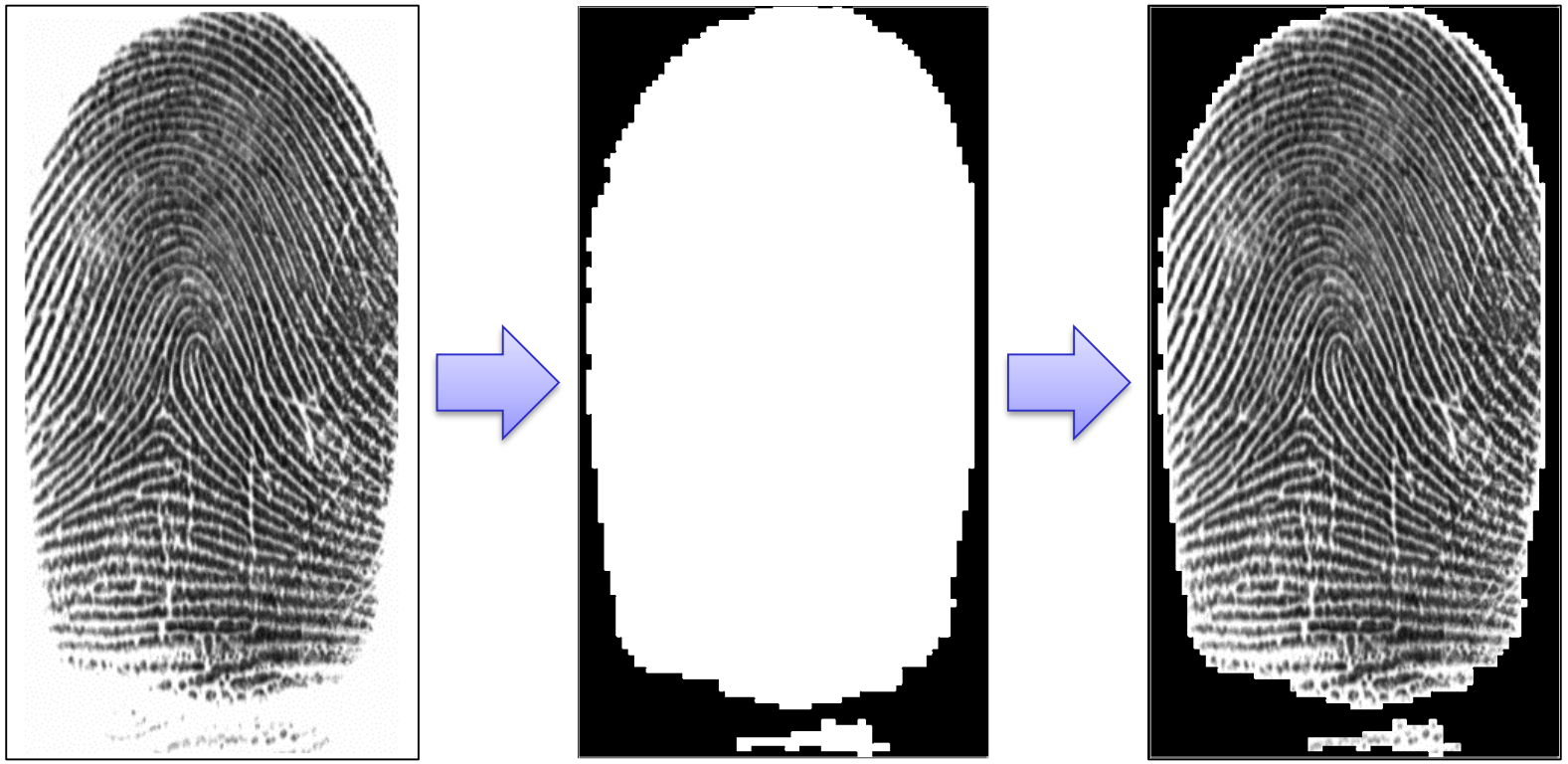


# Segmentation

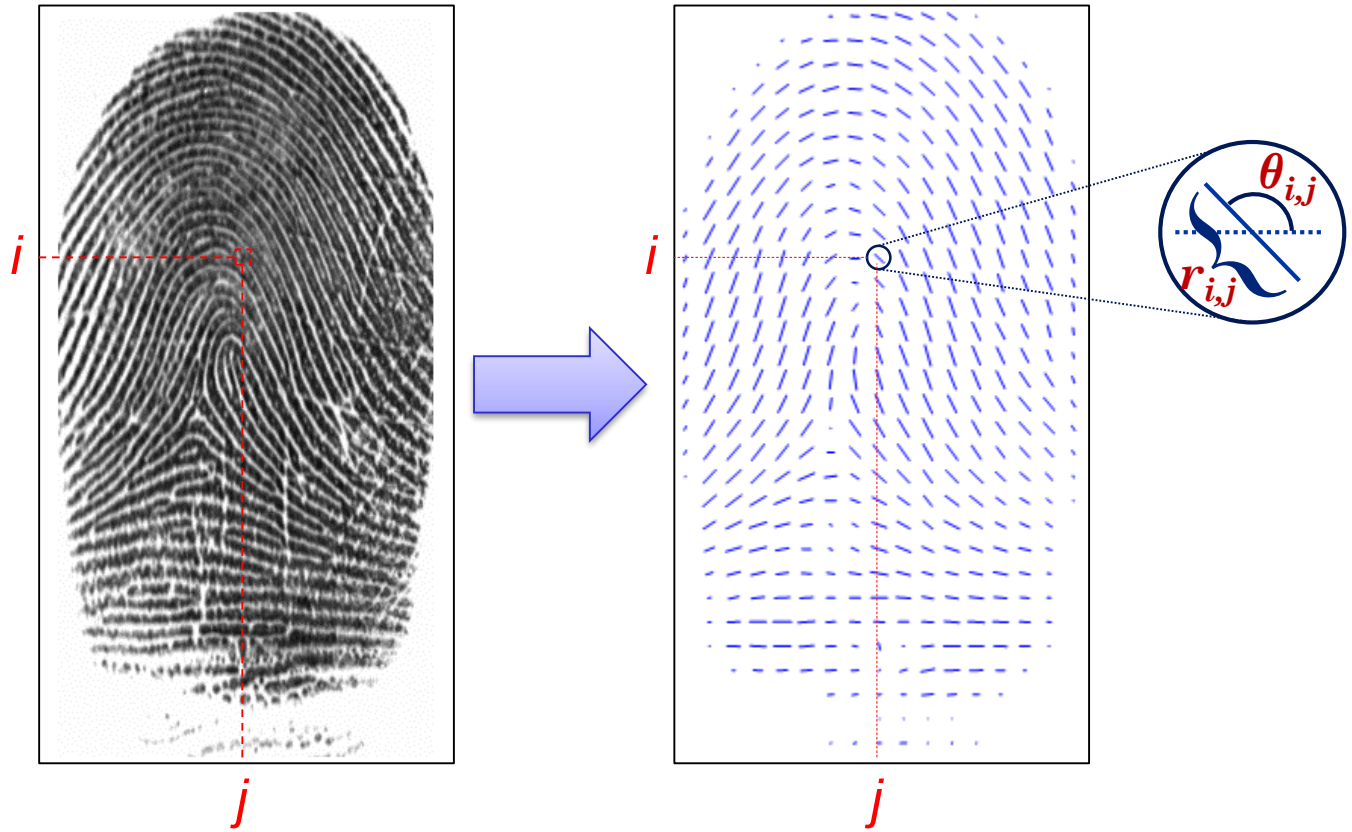
The segmentation stage is aimed to separate the fingerprint area (foreground) from the image background.

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

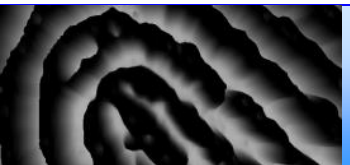


# Local ridge orientation

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 $[i, j]$.



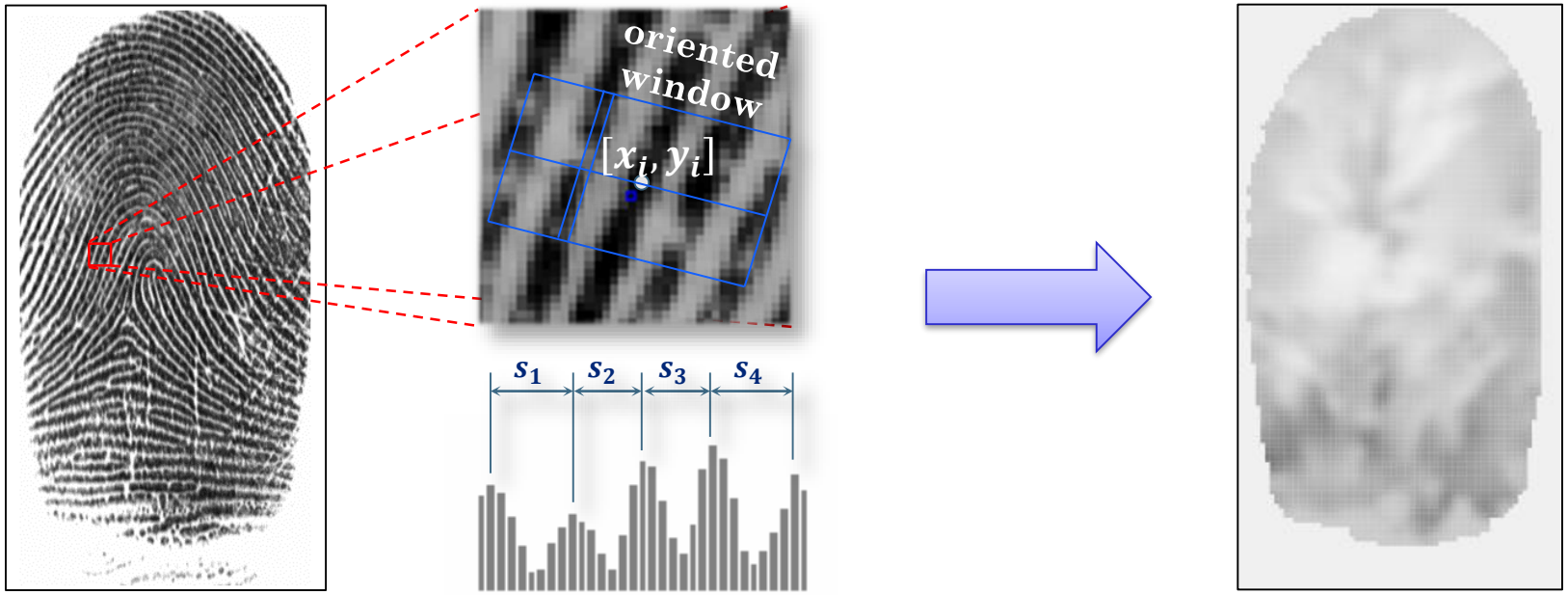

The simplest approach to extract local ridge orientations is based on computation of gradient phase angles.



# Local ridge frequency

The local ridge frequency $f_{xy}$ 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 $\theta_{xy}$.

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.



# Enhancement (1)

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

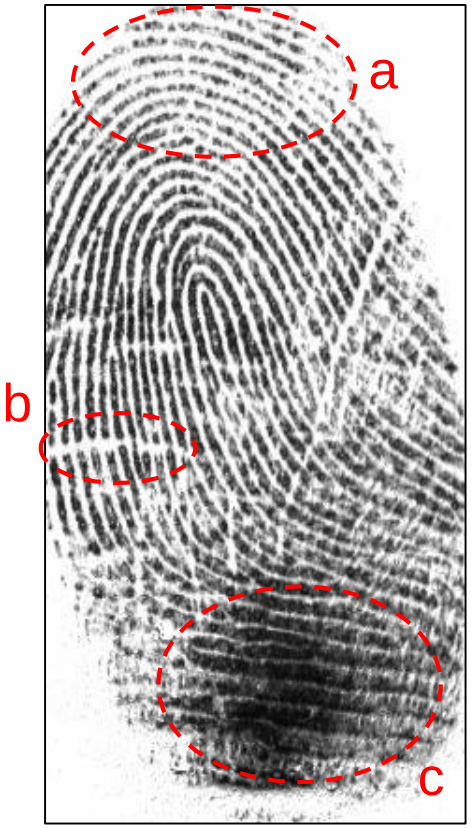
The objective of enhancement techniques is to improve the fingerprint image quality.

Typical degradations:

a. ridge lines are not continuous;

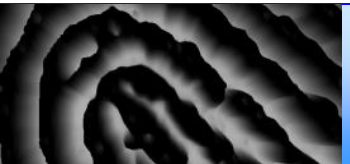
b. cuts, creases and bruises on the finger;

c. parallel ridges are not well separated.



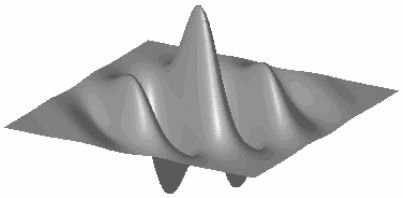

The most widely used technique for fingerprint enhancement is based on contextual filters.

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

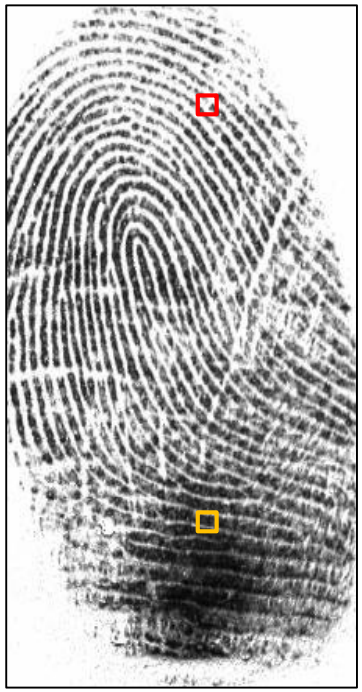


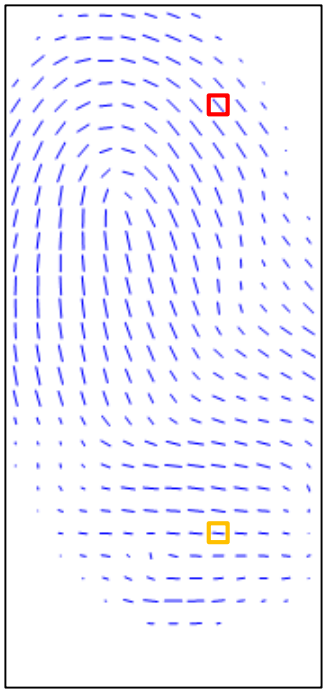
# Enhancement (2)

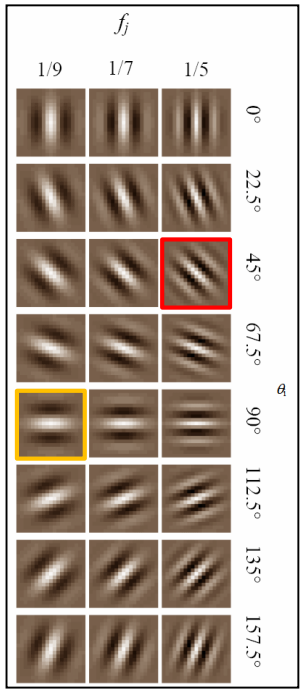
The local context of a fingerprint is represented by the ridge orientation and frequency.

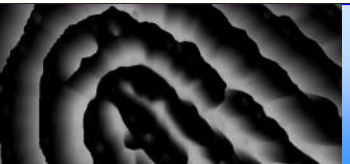


Gabor filter: sinusoidal plane wave tapered by a Gaussian.

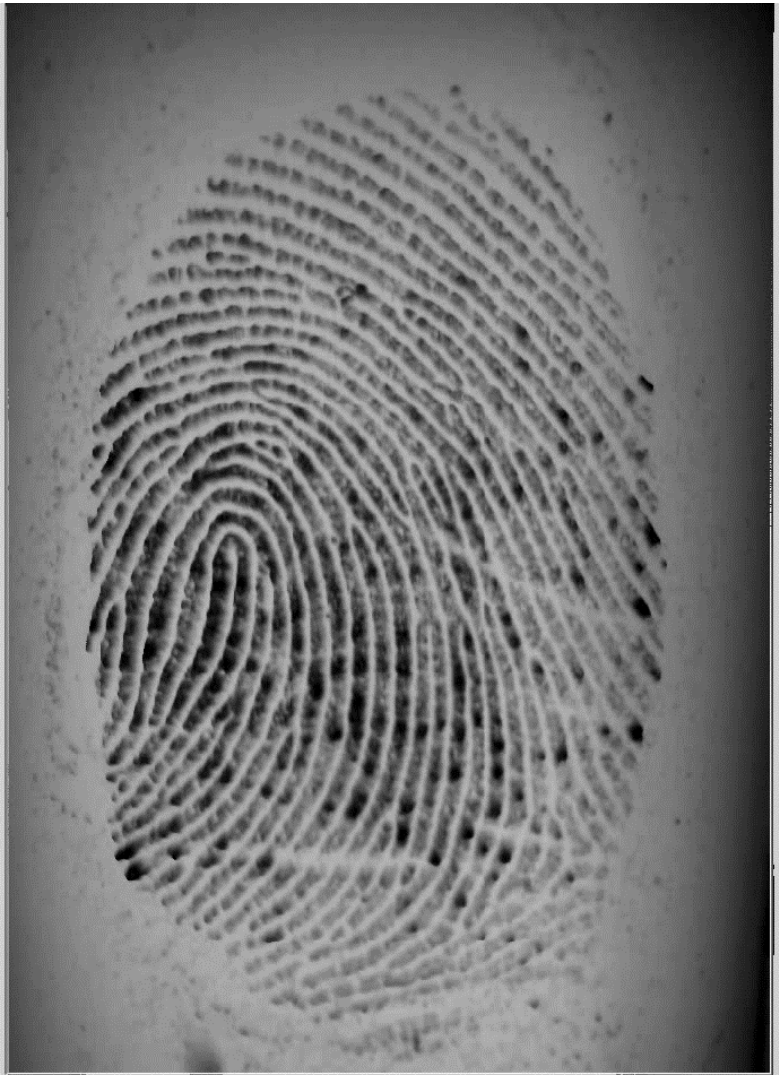


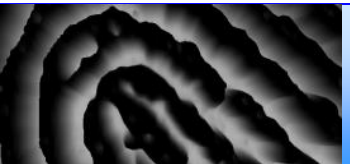




# Enhancement (3)





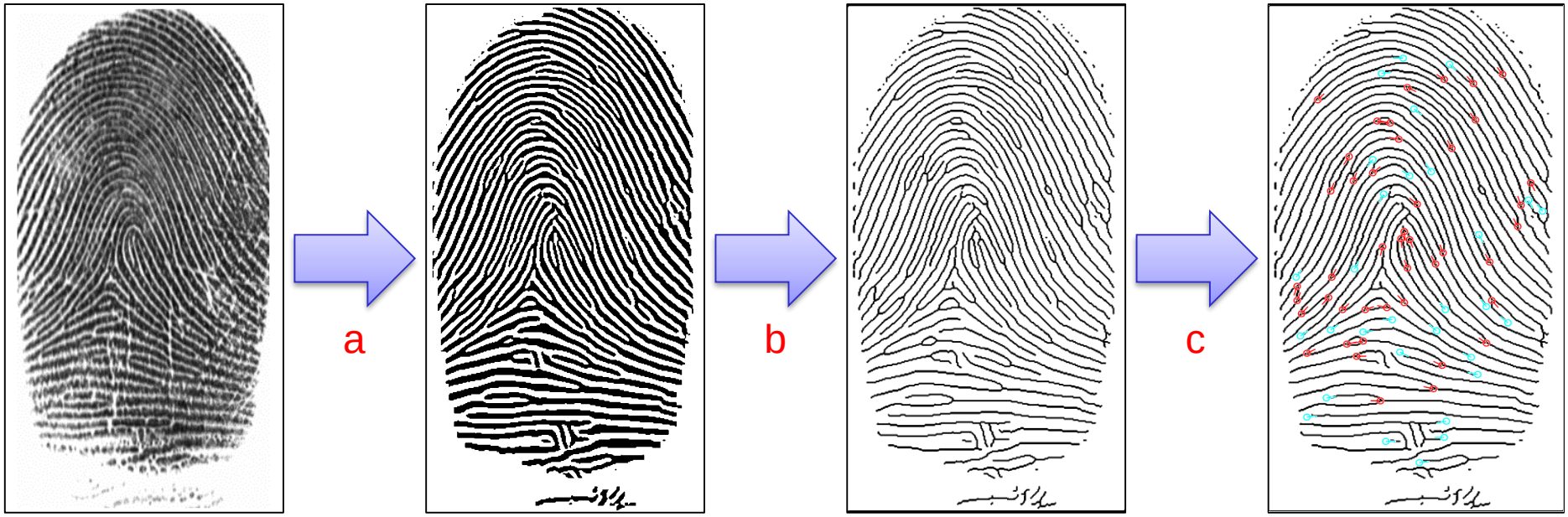
# Minutiae detection (1)

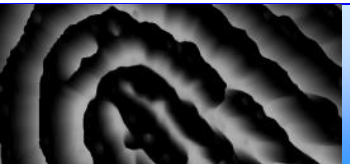
Traditional approach:

a. Enhancement/Binarization: conversion into a binary image;

b. Thinning: the binary image is submitted to a thinning stage aimed to reduce the ridge thickness to one pixel;

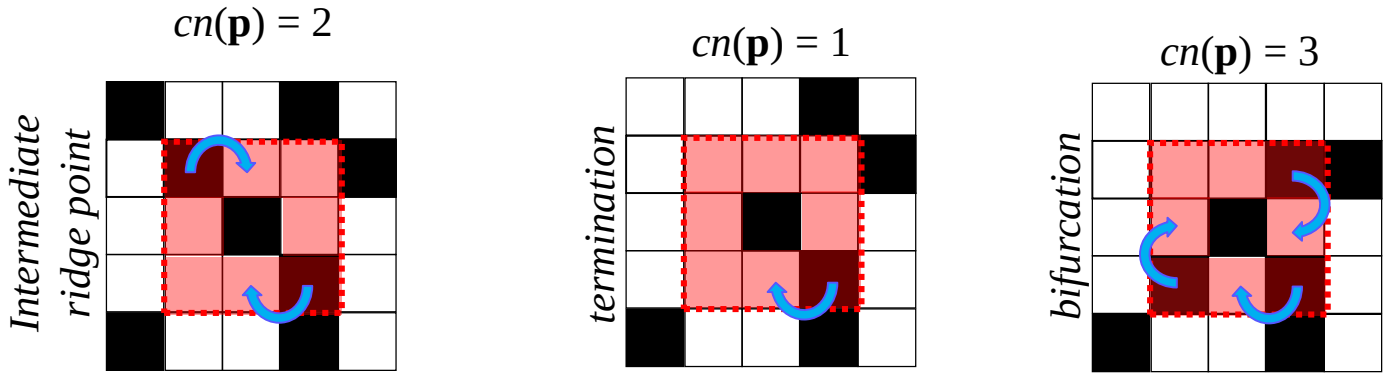
c. Detection: an image scan then allows to detect minutiae.



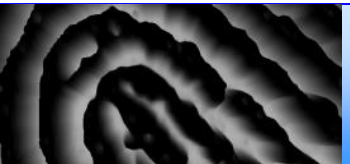
# Minutiae detection (2)

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




It is simple to note that a pixel black **p**:

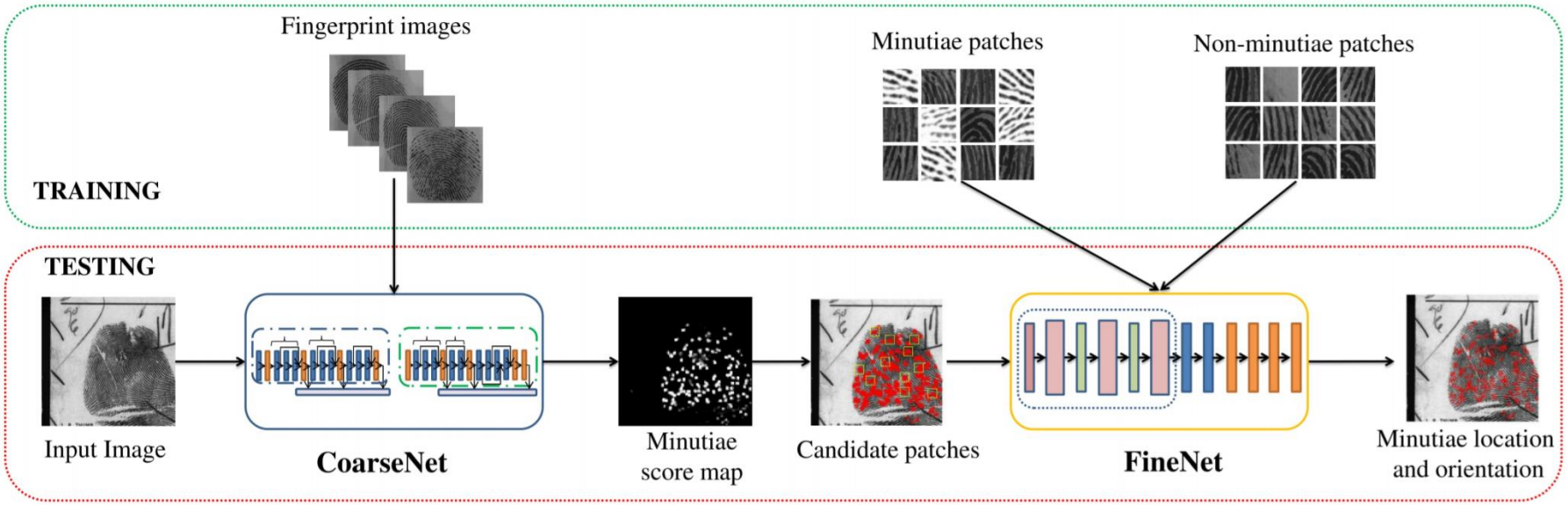
- is an intermediate ridge point if *cn*(**p**)=2;
- is a termination if *cn*(**p**)=1;
- is bifurcation if *cn*(**p**)=3;
- belongs to a more complex minutiae if *cn*(**p**)> 3.



# Minutiae Extraction with CNN

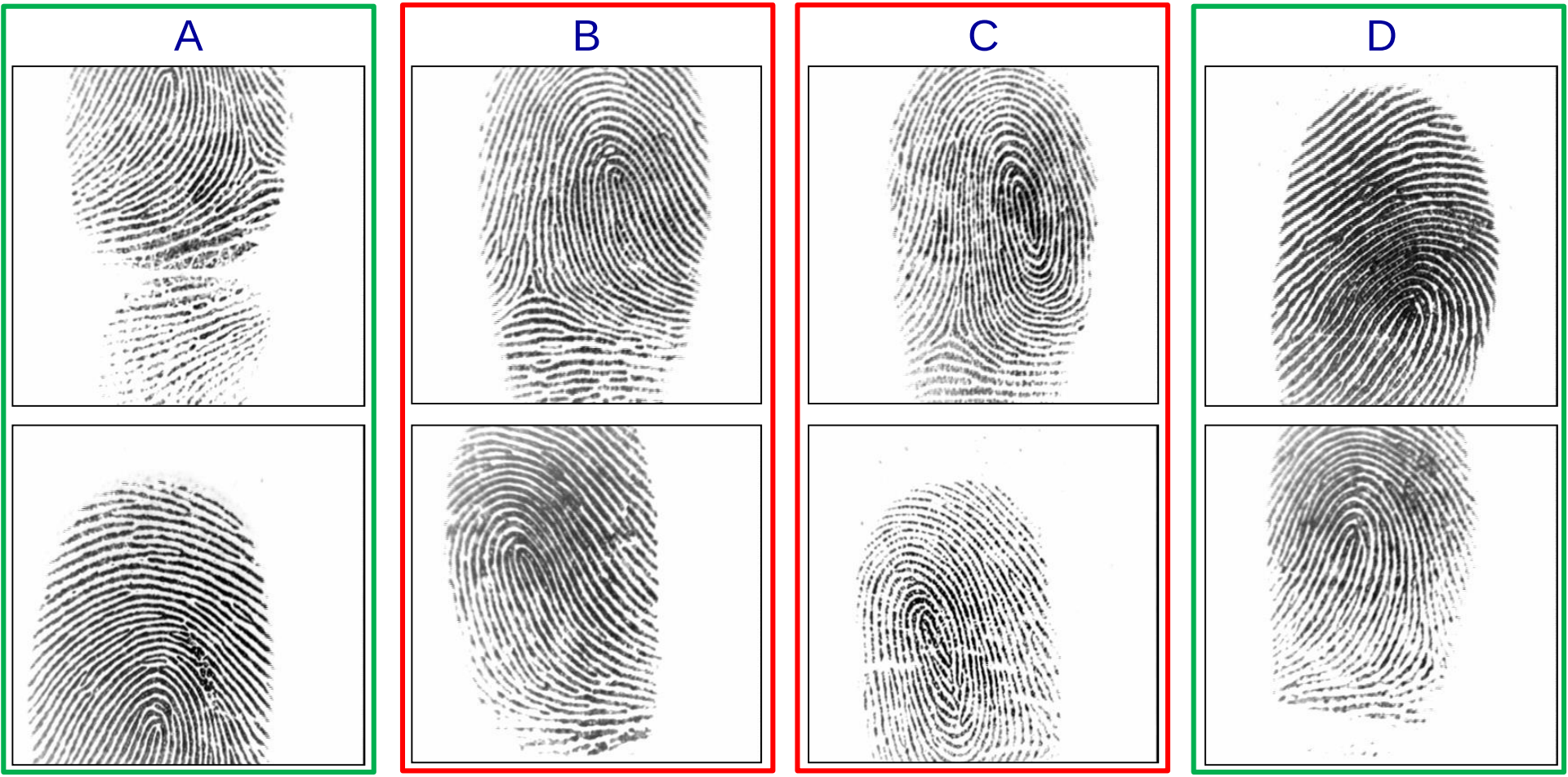
Dinh-Luan Nguyen, Kai Cao, Anil K. Jain, “Robust Minutiae Extractor: Integrating Deep Networks and Fingerprint Domain Knowledge”, ICB 2018.

- Classification of many patches is slow
- Object detection is not appropriate for minutiae patches
- Segmentation + Fine Classification is a smart approach

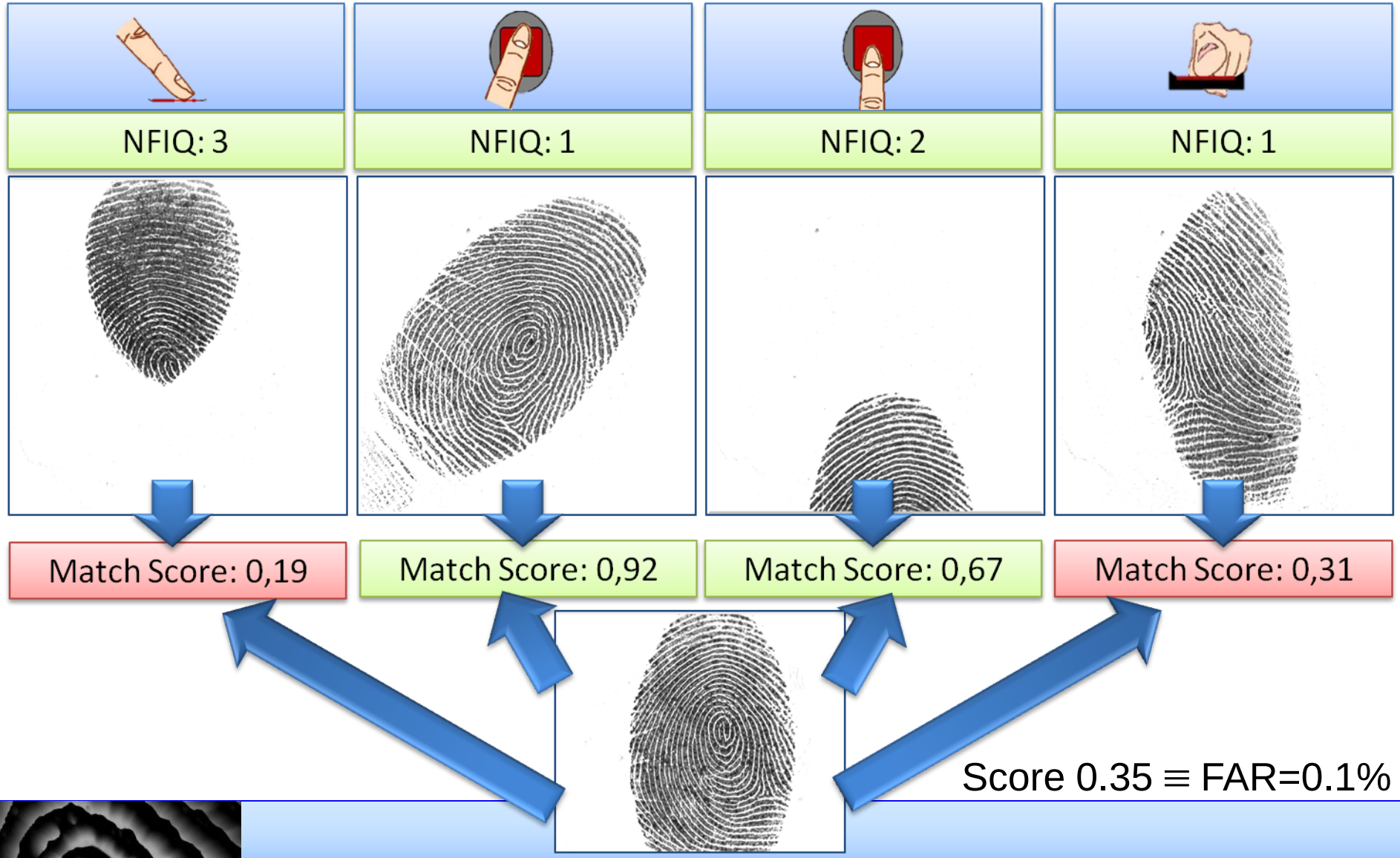


# Fingerprint comparison

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

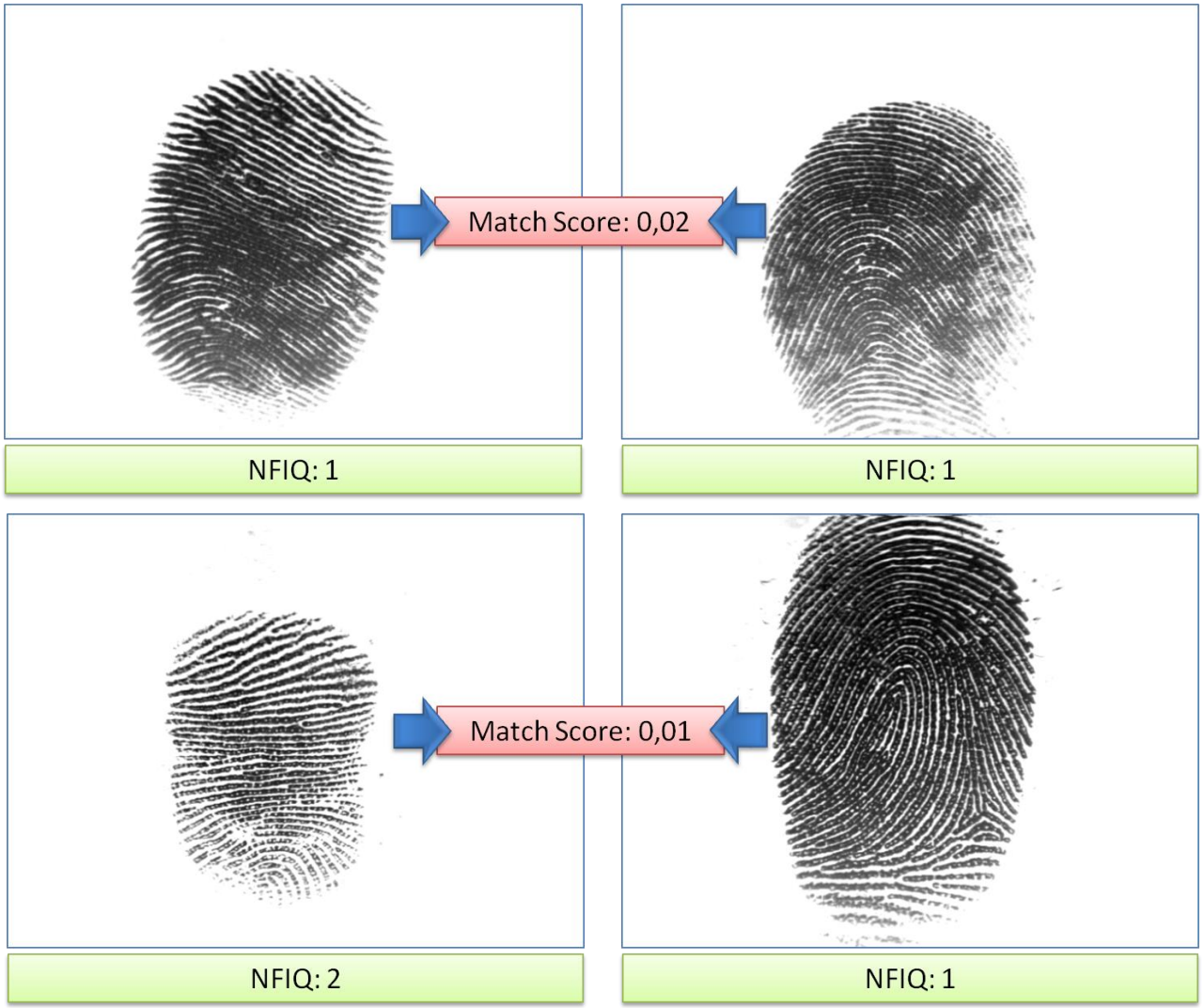


# Bad positioning



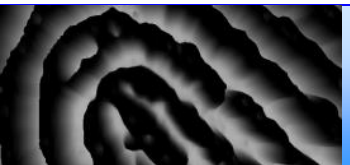

Score 0.35 ≡ FAR=0.1%

# Non-linear distortions



# Bad skin conditions and wrong pressure

| Normal | Dry finger | Wet finger | Low pressure |
|---|---|---|---|
| NFIQ: 1 | NFIQ: 5 | NFIQ: 3 | NFIQ: 2 |
|  |  |  |  |
| Match Score: 0,94 | Match Score: 0,37 | Match Score: 0,70 | Match Score: 0,71 |



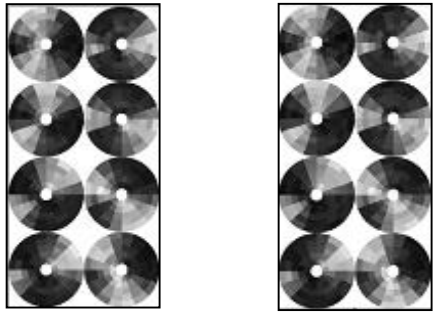
# Approaches (1)

## Minutiae-based

It consists in finding the maximum number of minutiae pairs between two minutiae templates.

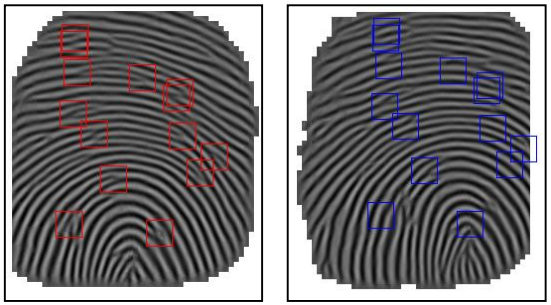
## Ridge feature-based

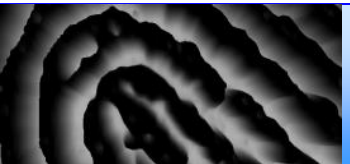
Other features of the fingerprint ridge pattern may be extracted more reliably than minutiae in low-quality images.



## Correlation-based

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



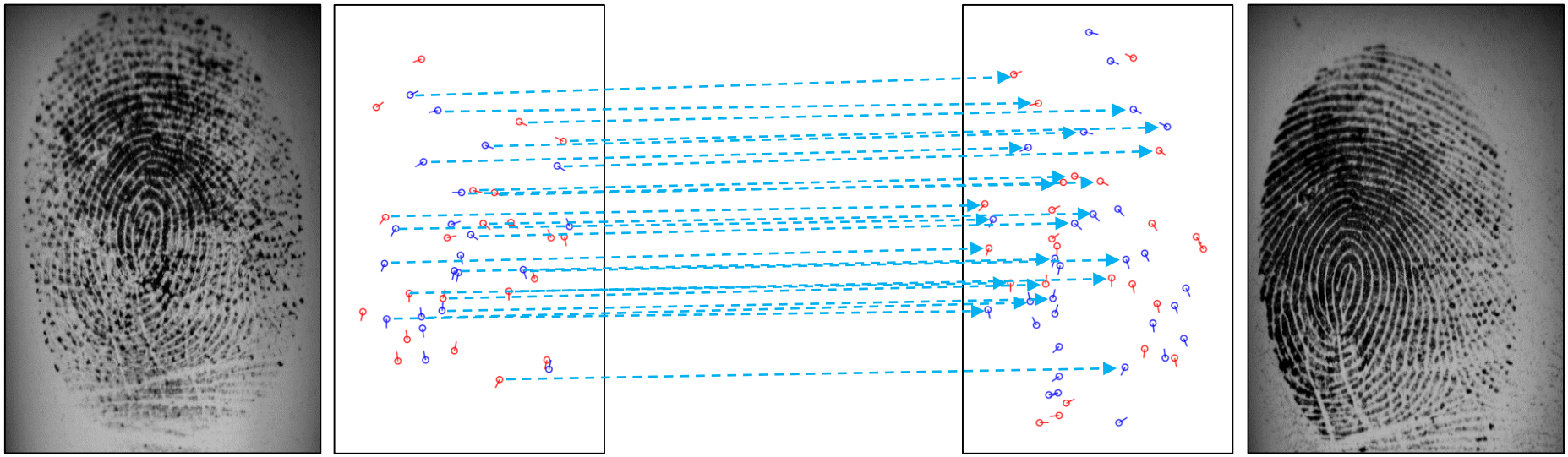


# Minutiae-based (1)

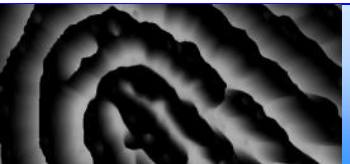
In minutiae-based comparison, the fingerprint is represented by a feature vector of variable length whose elements are the fingerprint minutiae.

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

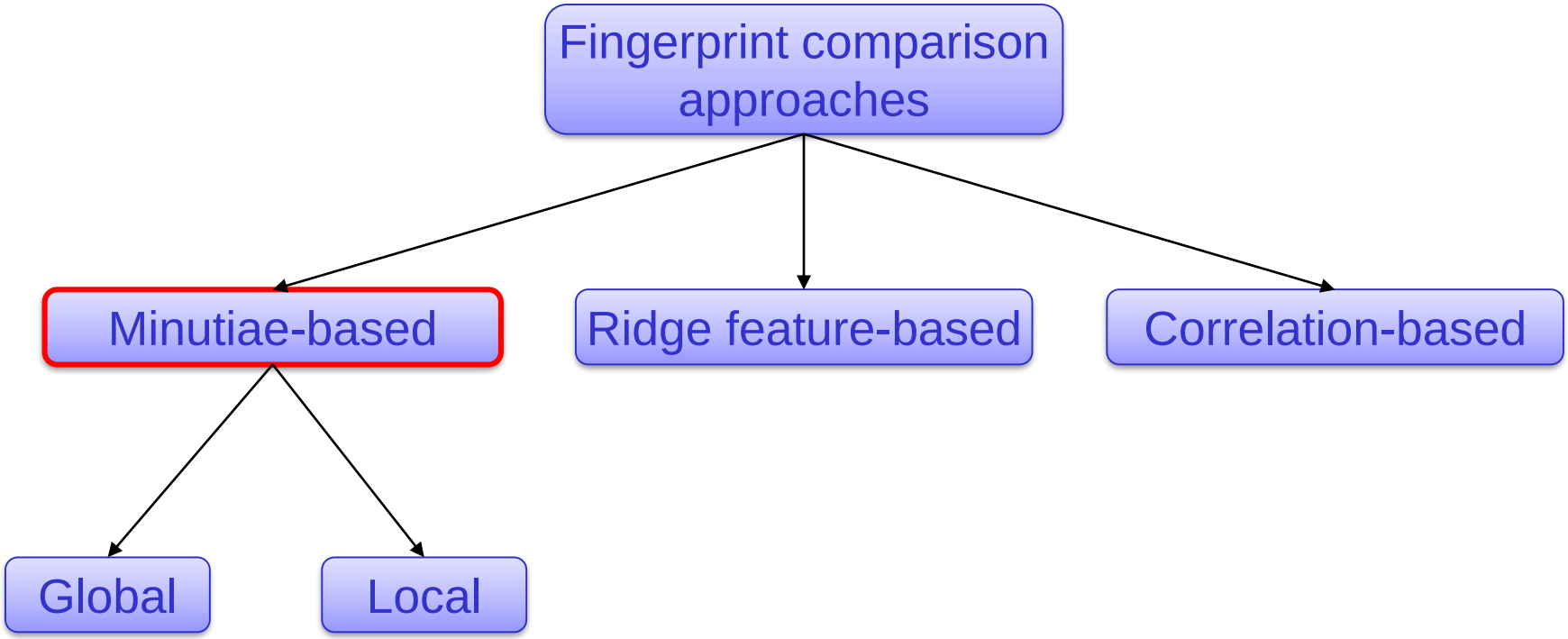
$T_1 = \{m_1, m_2, \ldots, m_u\}$ $T_2 = \{m'_1, m'_2, \ldots, m'_v\}$

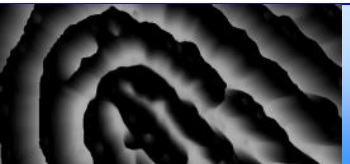


$$score = \frac{\#pairs}{(u+v)/2}$$



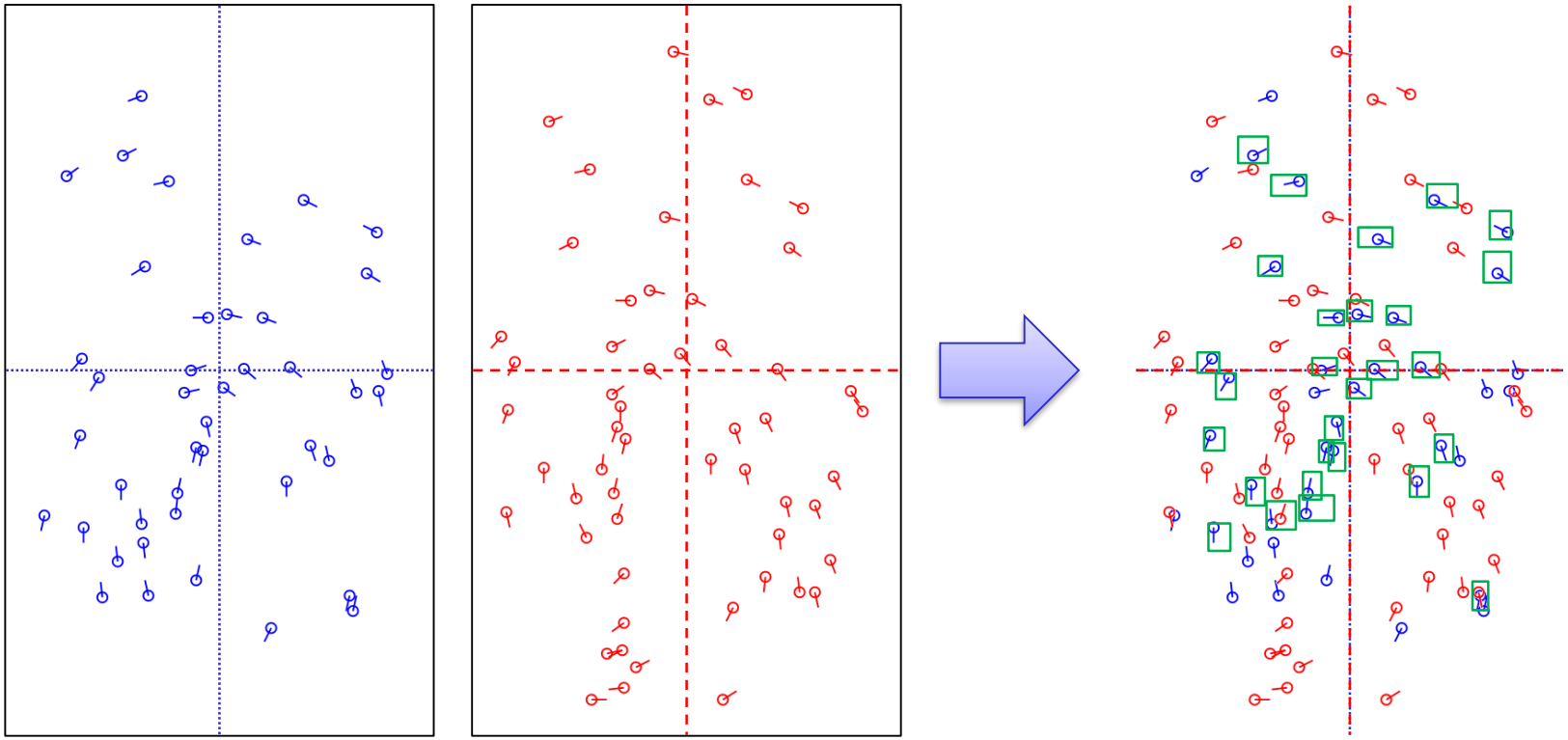
# Minutiae-based (2)



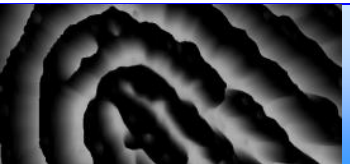



# Global minutiae-based

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



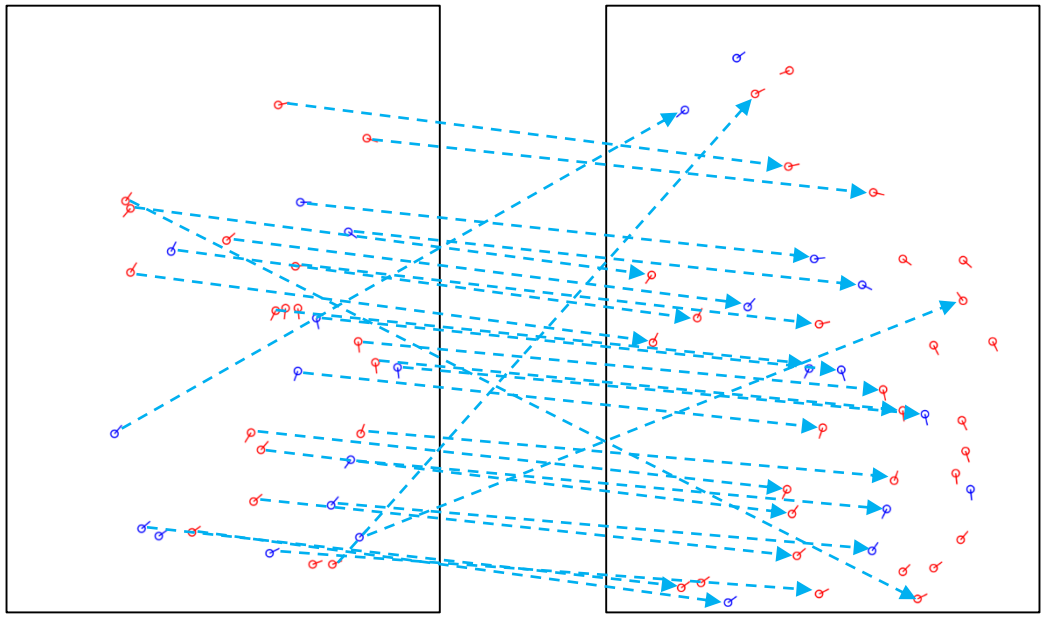
Some works in the literature propose to use the Hough transform (or Ransac implementations) to find the best rigid transformation to align two minutiae template.

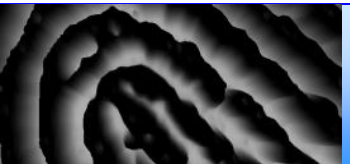


# Local minutiae-based (1)

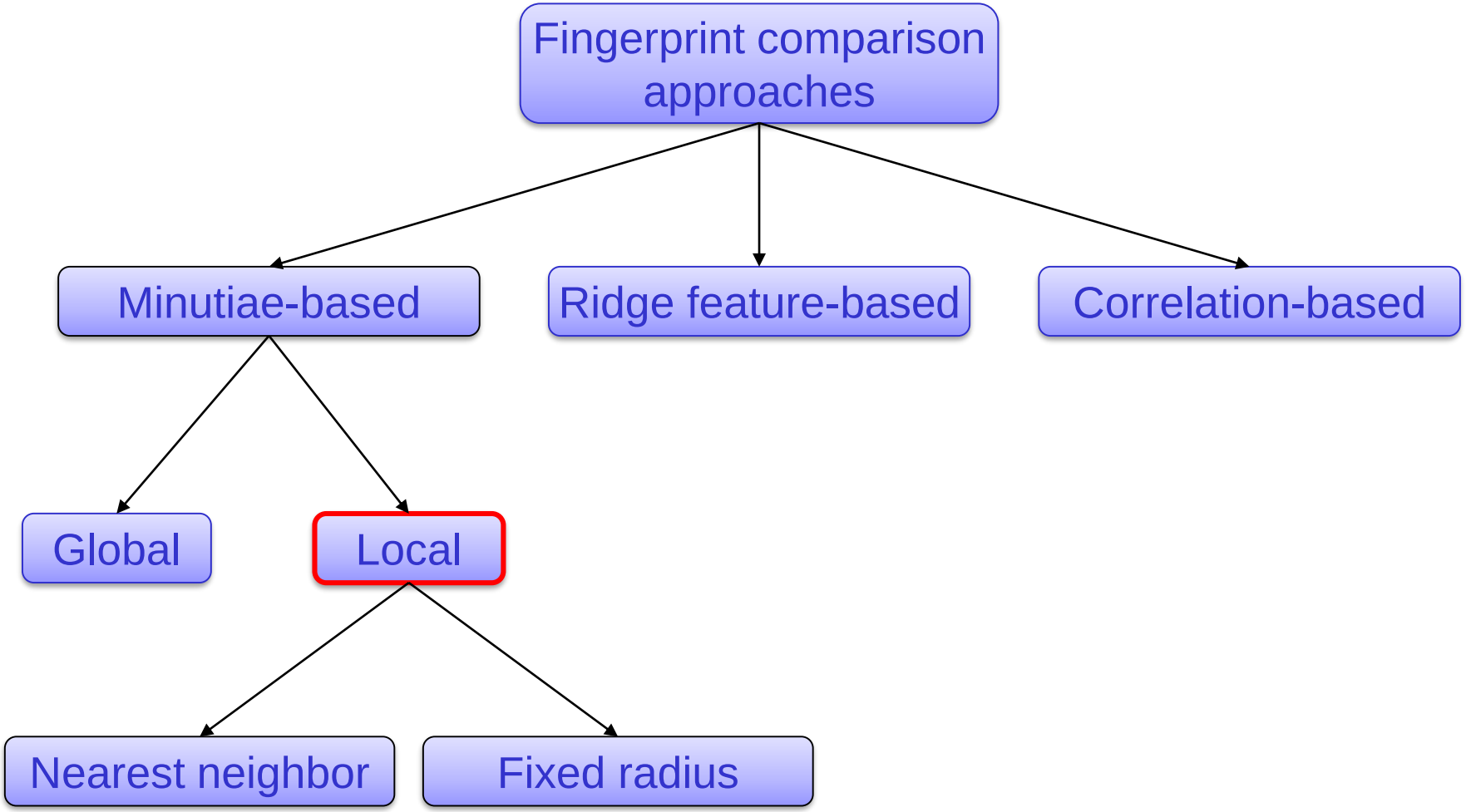
The objective of local minutiae-based approaches is to pair minutiae using local minutiae features invariant to global transformations without a pre-alignment step. Usually they are based on the following steps:

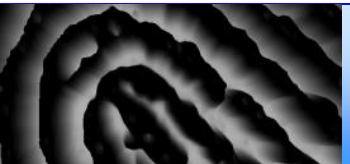
1. for each minutia local features are computed from local minutiae neighborhoods.
2. the minutiae are paired according to local features (fast, robust to distortion but less distinctive).
3. a consolidation step is performed to verify if local matches hold at global level.





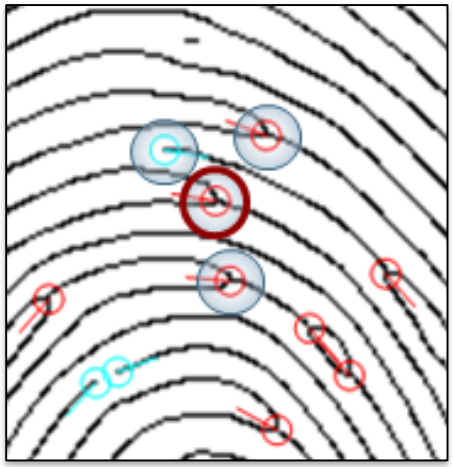
# Local minutiae-based (2)



# Nearest neighbor-based local structures

The neighbors of the central minutia are formed by its *K* closest minutiae.

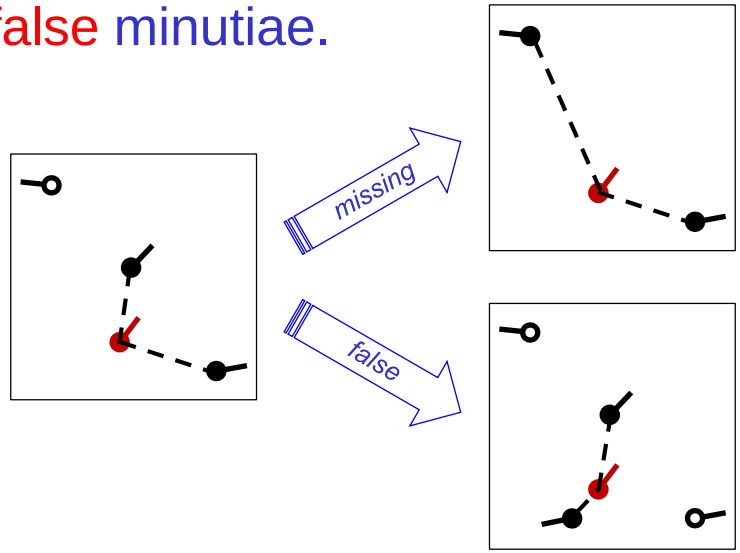


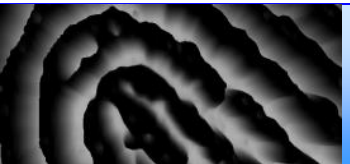
**Advantages**

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

**Drawbacks**

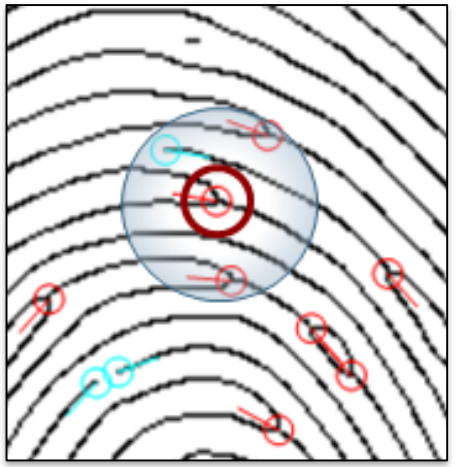
- possibility of exchanging nearest neighbor minutiae due to missing or false minutiae.



# Fixed radius-based local structures

The neighbors are defined as all the minutiae that are closer than a given radius R from the central minutia.

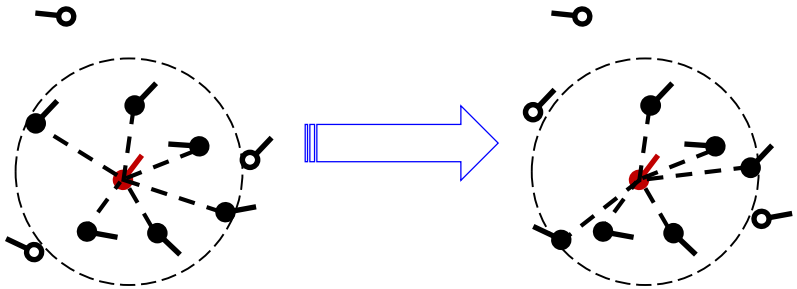


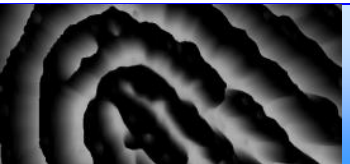
**Advantages**

- missing and false minutiae are better tolerated.

**Drawbacks**

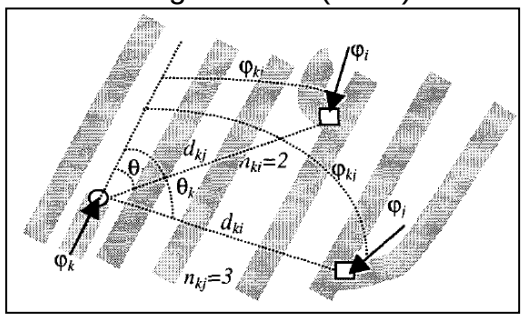
- the descriptor length is variable and depends on the local minutiae density leading to a more complex comparison.
- minutiae close to the border can be mismatched because of different local distortion or location inaccuracy.



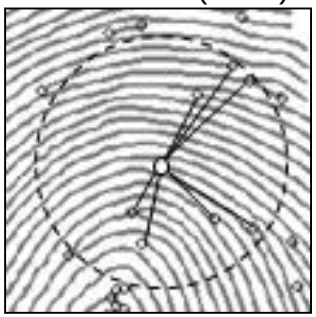


# Local structures: examples

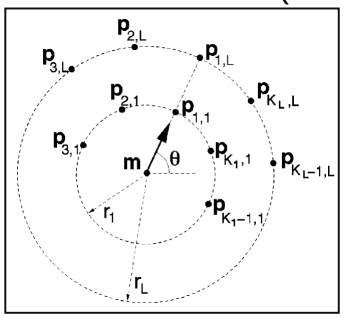
Jiang and Yau (2000)



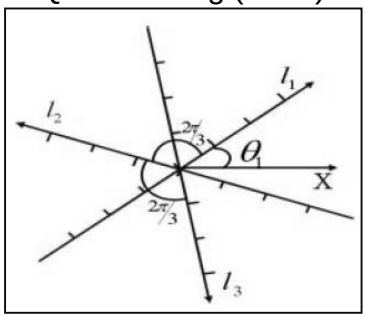

Ratha et al. (2000)



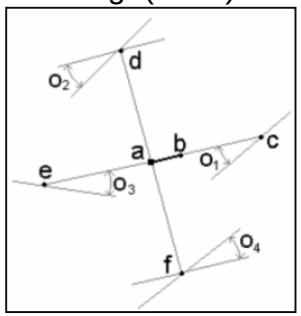
Tico and Kuosmanen (2003)



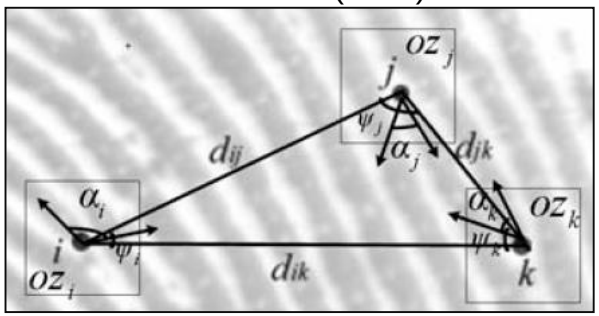

Qi and Wang (2004)



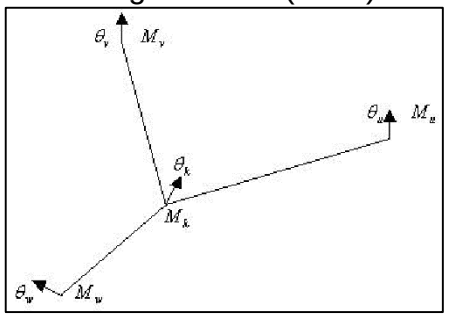

Ng (2004)



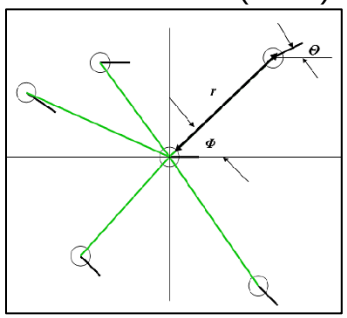

Chen et al. (2005)



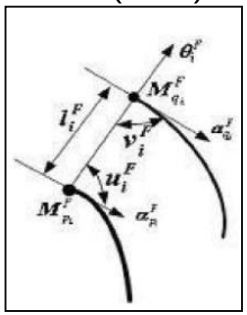

Deng and Huo (2005)



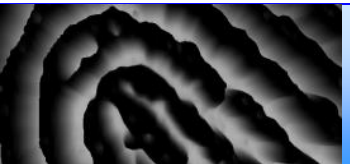

Chikkerur et al. (2006)




He (2006)



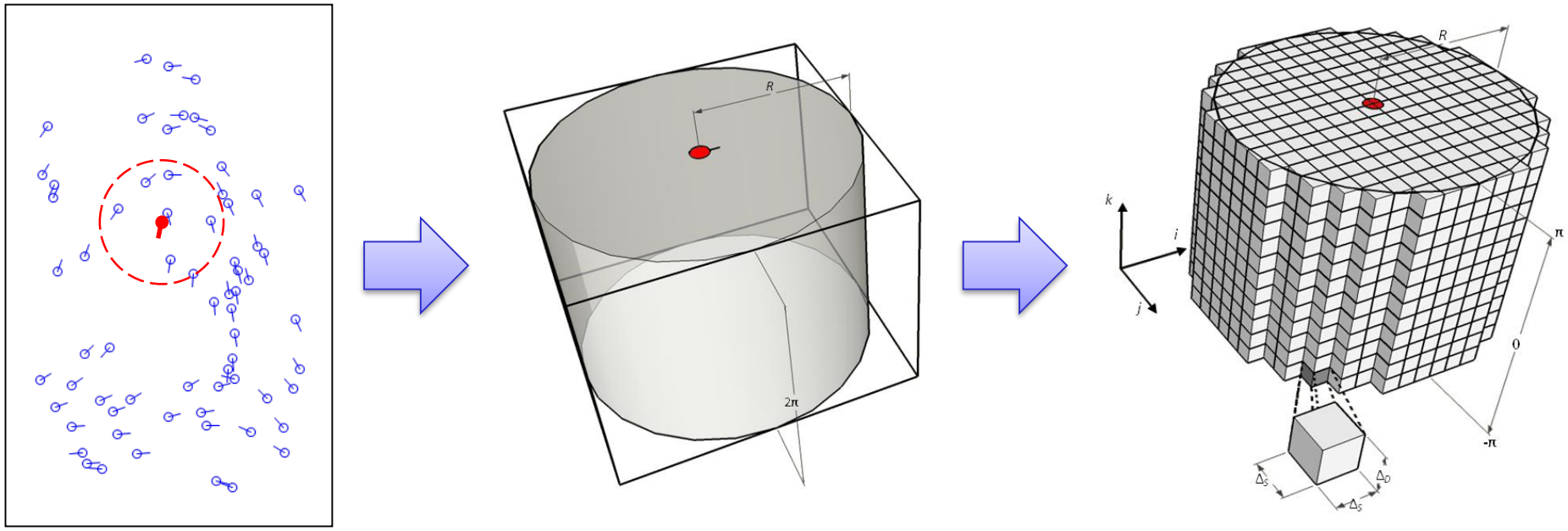

Feng (2008)

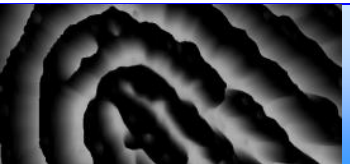


# Minutia Cylinder-Code (MCC) (1)

The main advantages of MCC are:

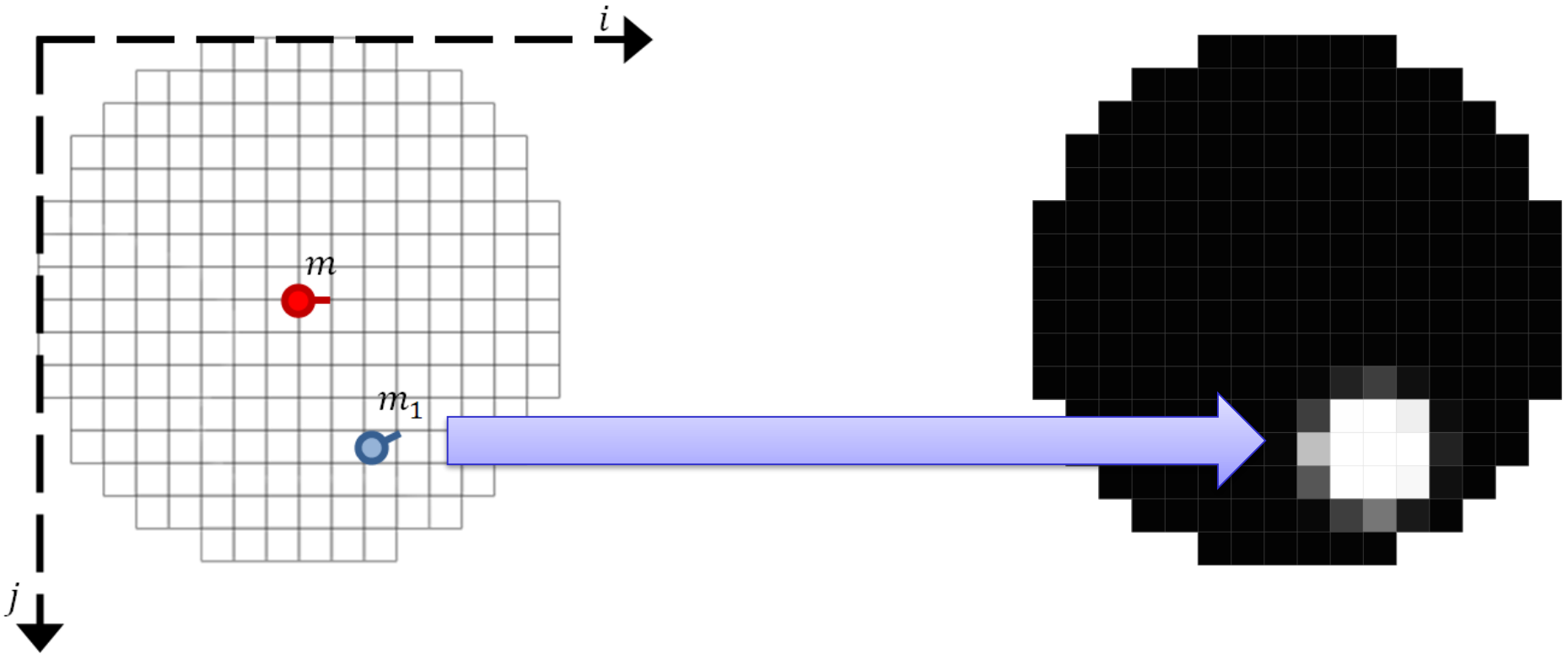
- fixed radius structure;
- fixed-length descriptors;
- toleration of local distortion and small feature extraction errors;
- bit-oriented coding;
- fast and simple local structure comparison phase;



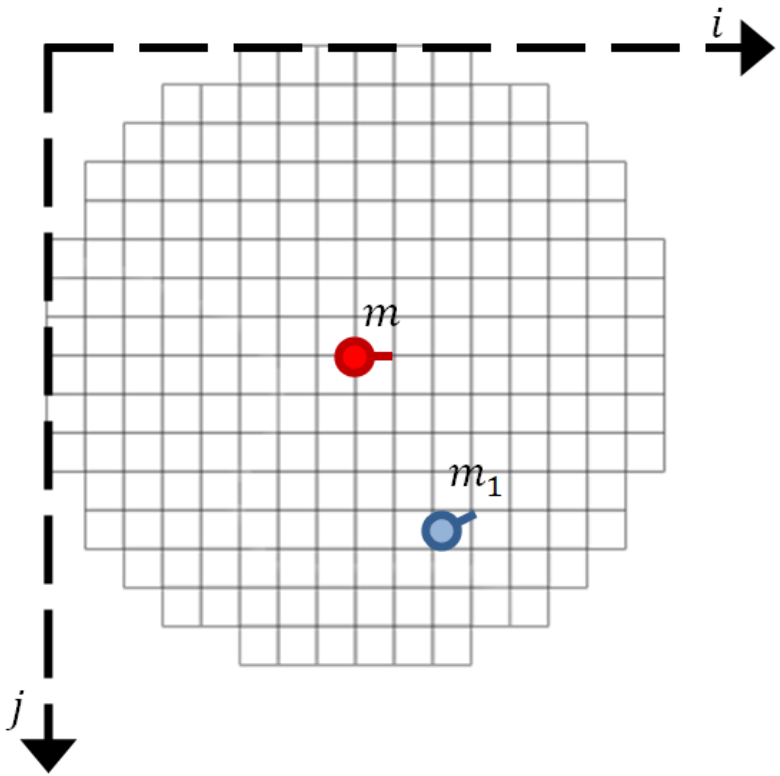



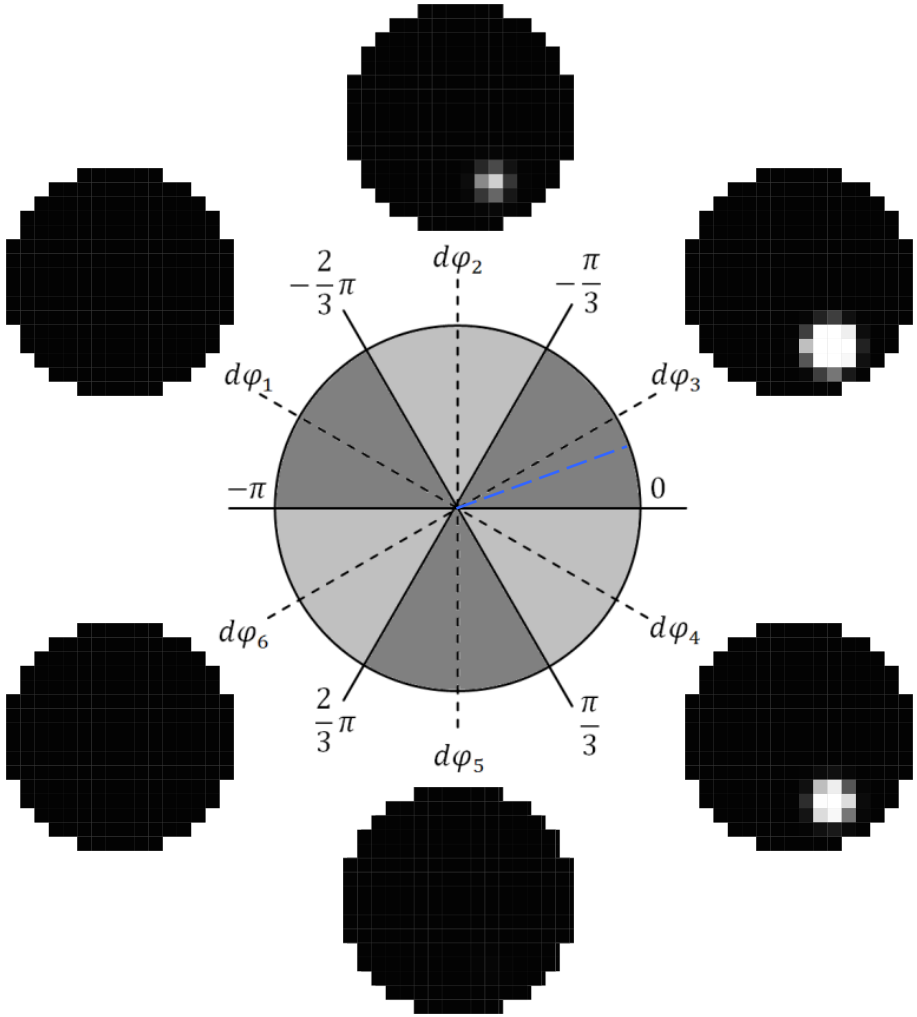
# Minutia Cylinder-Code (MCC) (2)

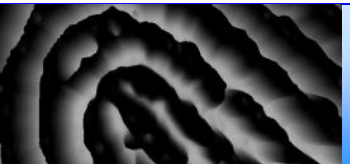
The spatial contribution of the neighbor minutia is spread over cells near its position.



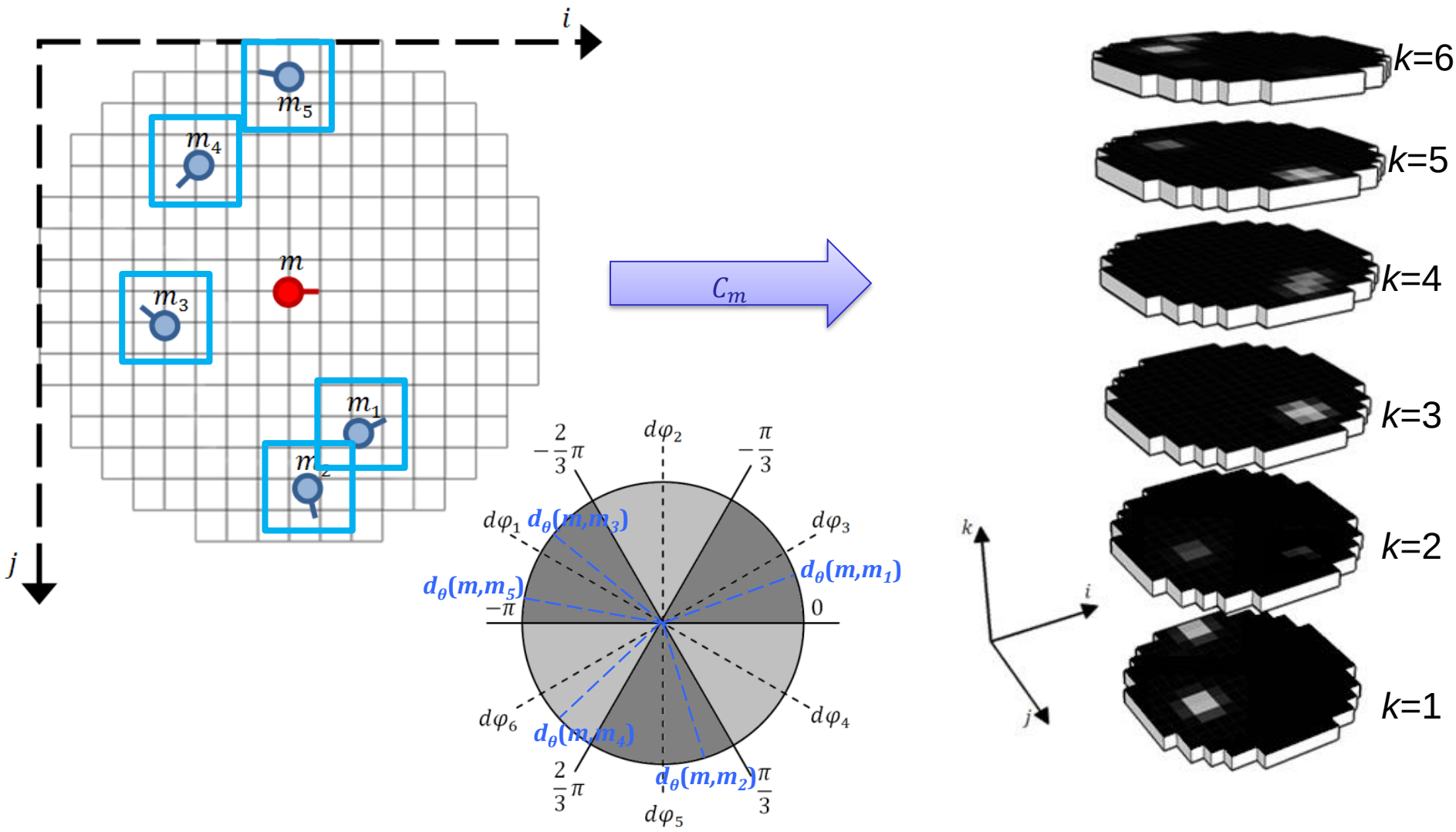
# Minutia Cylinder-Code (MCC) (3)

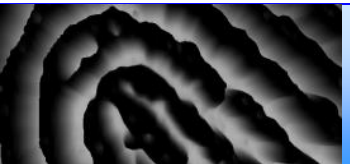


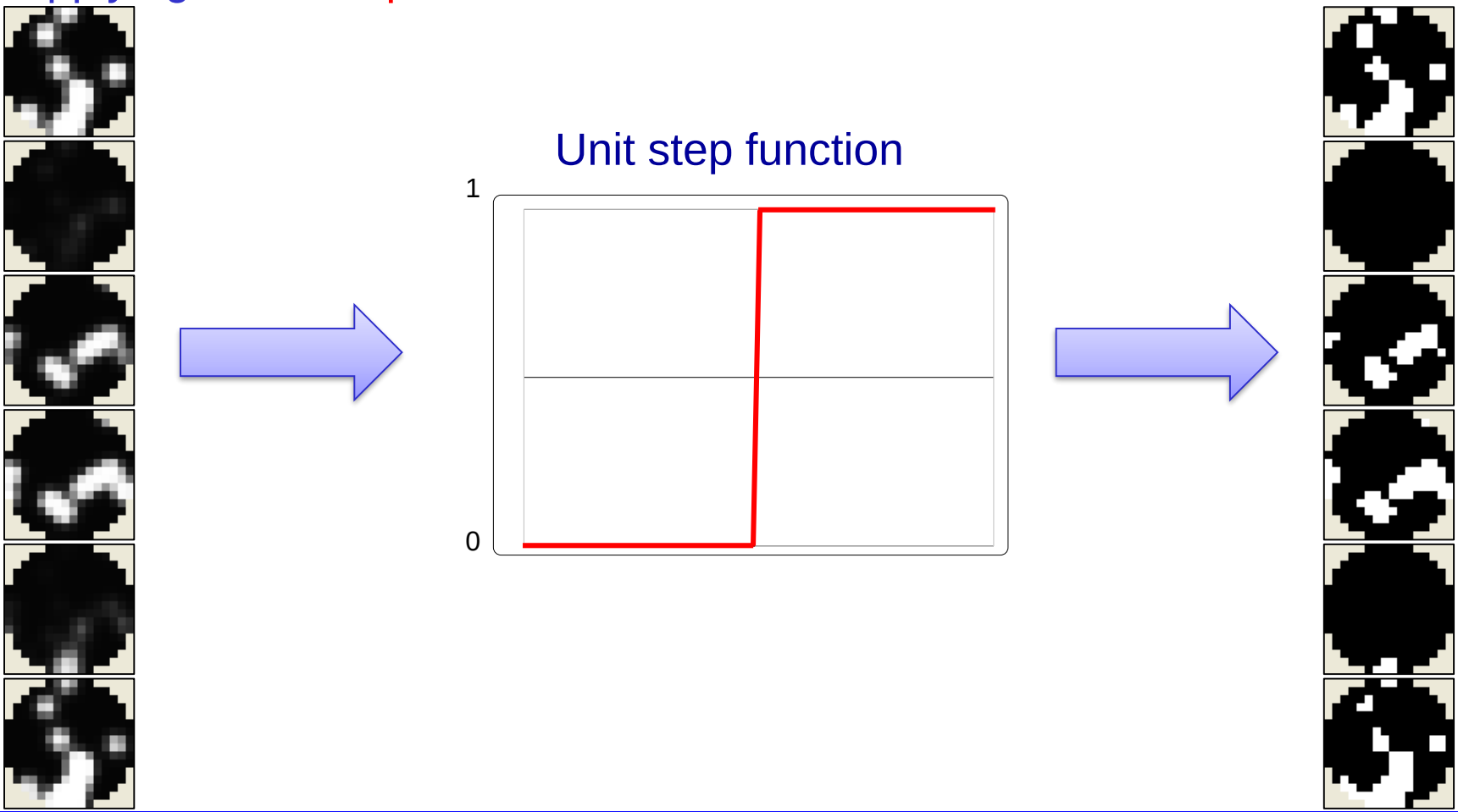
# Minutia Cylinder-Code (MCC) (4)



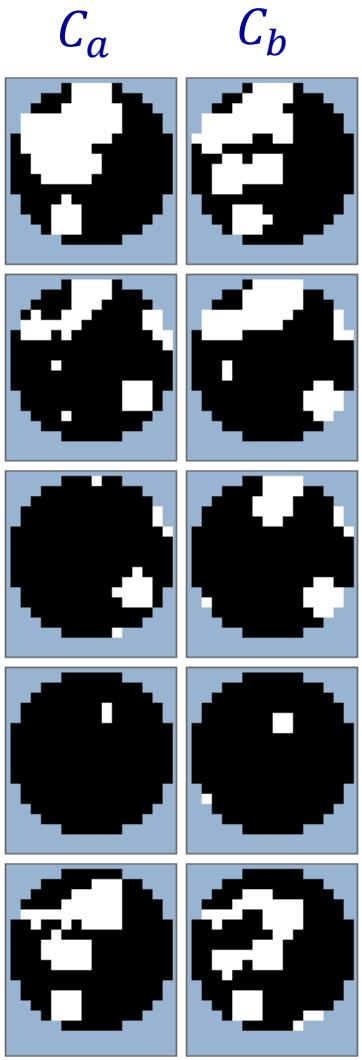



# Minutia Cylinder-Code (MCC) (5)

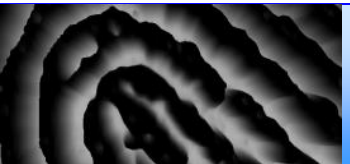
The cylinders can be conveniently converted into bit vectors by applying a unit step function.



# Minutia Cylinder-Code (MCC) (6)




$$\gamma(a,b) = 1 - \frac{\|C_a \text{ XOR } C_b\|}{\|C_a\| + \|C_b\|} = 0.64$$

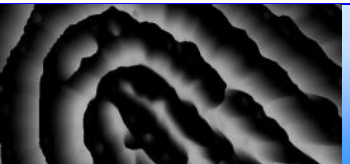


# Minutia Cylinder-Code (MCC) (7)

## MCC speed performance

Test: 100 identification queries on a 1M database

| Version | System configuration | Comparisons per second |
|---|---|---|
| Free MCC SDK<br>Single core, no SSE optimizations<br>Download at:<br>http://biolab.csr.unibo.it/mccsdk.html | Intel CPU E5-2650 @ 2GHz, 64 bit O.S. | 18 K |
| SSE4 Optimized for CPU | Intel CPU E5-2650 @ 2GHz, 64 bit O.S.<br>2 processors, 32 cores | 6980 K (~7 M) |
| GPU (CUDA) and CPU Optimized | Intel CPU E5-2650 @ 2GHz, 64 bit O.S.<br>2 processors, 32 cores<br>4 Nvidia Tesla C2075 GPUs | 42373 K (~ 42 M) |

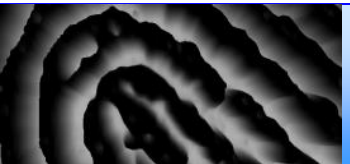


# Fingerprint Verification Competitions (FVC)

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

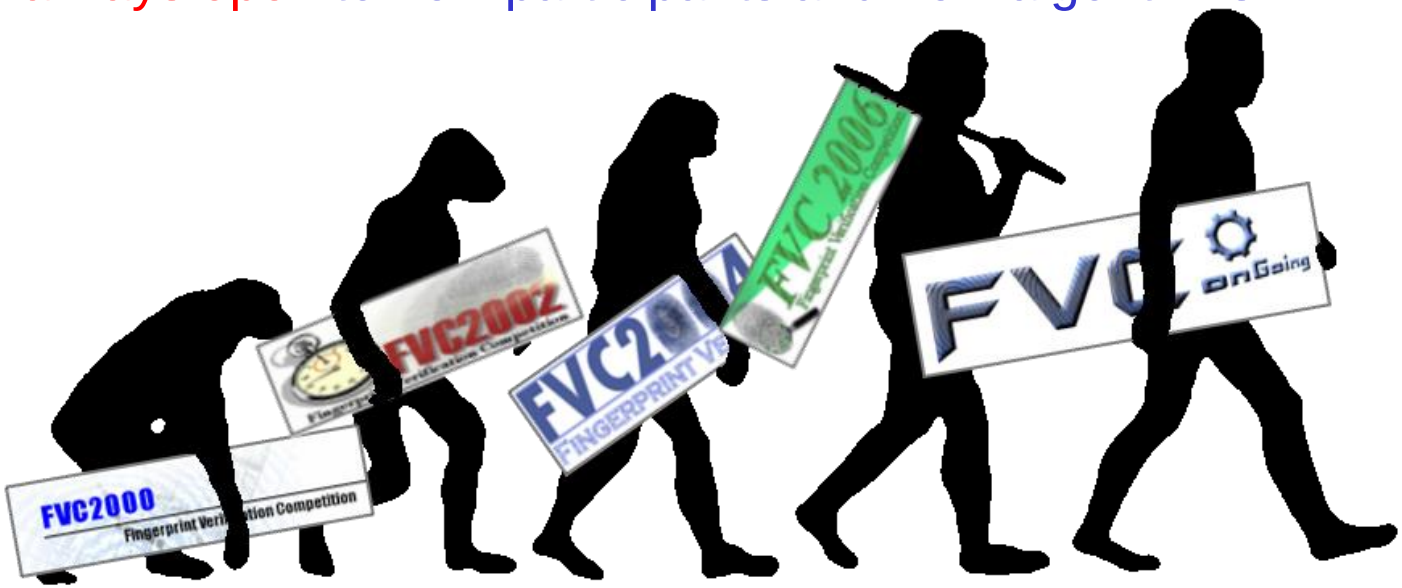
- track the state-of-the-art
- to provide benchmarks and testing protocols for a fair evaluation.


| | FVC2000 | FVC2002 | FVC2004 | FVC2006 |
|---|---|---|---|---|
| # Participants registered | 25 | 48 | 110 | 150 |
| # Algorithms evaluated | 11 | 31 | 67 | 70 |
| # Databases | 3 real, 1 synthetic | | | |
| # Fingers per database | 100 | | | 140 |
| # Samples per finger | 8 | | | 12 |



# FVC-onGoing (1)

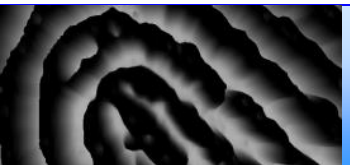
In 2009 started FVC-onGoing, a fully automated web-based evaluation system always open to new participants and new algorithms.




Not only limited to fingerprint verification algorithms but also for:

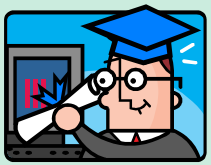
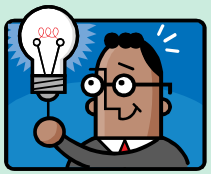
- other fingerprint modules (e.g., local orientation extraction, fingerprint indexing)
- other biometric problems (e.g., palmprint verification, face morphing detection)

http://biolab.csr.unibo.it/fvcongoing

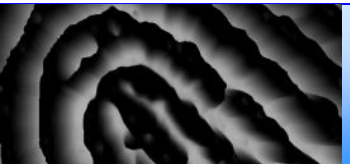


# FVC-onGoing (2)

Statistics - updated December 2019:

| Registered Participants (1608) | | |
|---|---|---|
|  | Academic Research Groups | 263 |
|  | Companies | 260 |
|  | Independent Developers | 1085 |

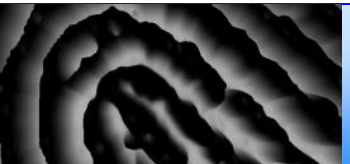
| Fingerprint Benchmark Area | Algorithm Evaluated (5419) | Algorithm Published (199) |
|---|---|---|
| Fingerprint Verification | 1940 | 69 |
| Fingerprint ISO Template Matching | 2598 | 98 |
| Fingerprint Orientation Extraction | 610 | 14 |
| Fingerprint Indexing | 211 | 10 |
| Secure Template Fingerprint Verification | 60 | 8 |



# FV: Fingerprint Verification

## Benchmark FV-STD-1.0 (Top Algorithms @ Dec 2019):

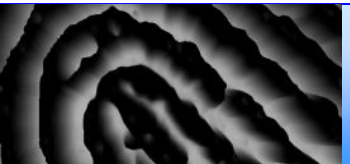
| Published on | Benchmark | Participant | Type | Algorithm | Version | EER ▲ | $FMR_{1000}$ | $FMR_{10000}$ | Show details |
|---|---|---|---|---|---|---|---|---|---|
| 27/07/2017 | FV-STD-1.0 | Beijing Hisign Bio-info Institute | Company | HXKJ | 2.4 | 0.022 % | 0.007 % | 0.036 % | |
| 24/01/2019 | FV-STD-1.0 | Neurotechnology | Company | MM_FV | 11.0 | 0.027 % | 0.011 % | 0.043 % | |
| 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 % | |



# FMISO: Fingerprint ISO Template Matching

## Benchmark FMISO-STD-1.0 (Top Algorithms @ Dec 2019):

| Published on | Benchmark | Participant | Type | Algorithm | Version | EER ▲ | $FMR_{1000}$ | $FMR_{10000}$ | Show details |
|---|---|---|---|---|---|---|---|---|---|
| 12/06/2014 | FMISO-STD-1.0 | Neurotechnology | Company | MM_FMISO | 5.1 | 0.194 % | 0.328 % | 0.776 % | |
| 15/05/2011 | FMISO-STD-1.0 | AA Technology Ltd. | Company | EMB9200 | 2.41 | 0.234 % | 0.292 % | 0.444 % | |
| 24/03/2011 | FMISO-STD-1.0 | UnionCommunity | Company | Triple_M_ISO | 1.2 | 0.234 % | 0.361 % | 0.620 % | |
| 22/09/2015 | FMISO-STD-1.0 | Xiamen Toyonway Intellectual Technology Co. Ltd, China | Company | TW2F_ISO | 0.2 | 0.252 % | 0.314 % | 0.556 % | |
| 15/12/2010 | FMISO-STD-1.0 | Suprema, Inc. | Company | SFCore | 1.0 | 0.258 % | 0.346 % | 0.639 % | |
| 09/03/2014 | FMISO-STD-1.0 | Tiger IT Bangladesh | Company | TigerAFIS | v1.2-ISO/MINEX | 0.296 % | 0.422 % | 0.837 % | |
| 17/10/2016 | FMISO-STD-1.0 | Decatur Industries, Inc. | Company | Decatur | 1.3.2 | 0.300 % | 0.415 % | 0.700 % | |
| 12/10/2009 | FMISO-STD-1.0 | Tiger IT Bangladesh | Company | Tiger ISO | 0.1 | 0.317 % | 0.447 % | 0.866 % | |
| 05/12/2019 | FMISO-STD-1.0 | Beijing Hisign Bio-info Institute | Company | HXKJ | 3.05 | 0.342 % | 0.437 % | 0.617 % | |
| 31/12/2015 | FMISO-STD-1.0 | BKIC Laboratory - Hanoi University of Science and Technology | Academic Research Group | BKAFIS | 0.4 | 0.346 % | 0.491 % | 0.696 % | |

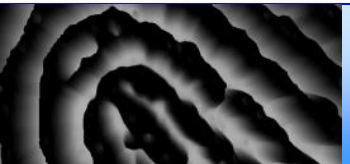


# What can we learn?

## Characteristics of algorithms published on FV area:

| | Algorithm | | | EMB9200 2.3 | Triple_ M 1.1 | MntModel 1.0 | MiraFinger 2.2 | GBFRSW 1.3.2.0 | SourceAFIS 1.1 | MM_FV 3.0 | STAR 1.0 | JF_FV 1.21a |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Preprocessing | Segmentation | | | X | X | X | | X | X | X | X | X |
| | Enhancement | | | X | X | X | | | X | X | X | X |
| | Binarization | | | X | X | X | | X | X | X | X | X |
| Feature Used | Minutiae | | | X | X | X | X | X | X | X | X | X |
| | Singular Points | | | | | | | | | X | X | X |
| | Ridge Shape | | | | | | | X | | | | |
| | Ridge Counts | | | X | | | | | | X | | |
| | Orientation Field | | | X | X | X | | X | | X | X | X |
| | Local Ridge Frequency | | | | X | | | X | | X | X | |
| | Texture | | | | | | X | | | | X | |
| Matching | Matching Strategy | Minutiae-Based | Local | X | X | X | X | X | X | X | X | X |
| | | | Global | X | X | X | | X | X | X | X | X |
| | | Based on Geometry Ridge Features | | | | | | X | | | | X |
| | Alignment Model | Displacement | | X | X | X | X | X | X | X | X | X |
| | | Rotation | | X | X | X | X | X | X | X | X | X |
| | | Scale | | | | | X | | | | X | X |
| | | Non-linear Distortion | | X | X | | X | X | | X | X | |

| For the most effective algorithms |
|---|
| enhancement / binarization based on contextual filtering |
| alignment mainly relies on minutiae |
| matching with multiple features (minutiae, frequency, orientation) |
| minutia alignment/matching with two stage: local matching + global consolidation |

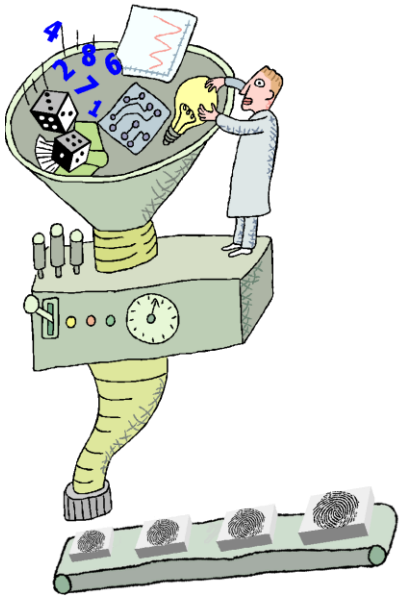


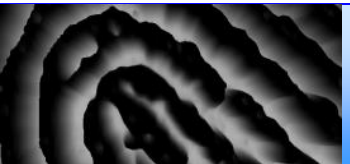
# Synthetic fingerprint generation

Collecting large databases of fingerprint images is:

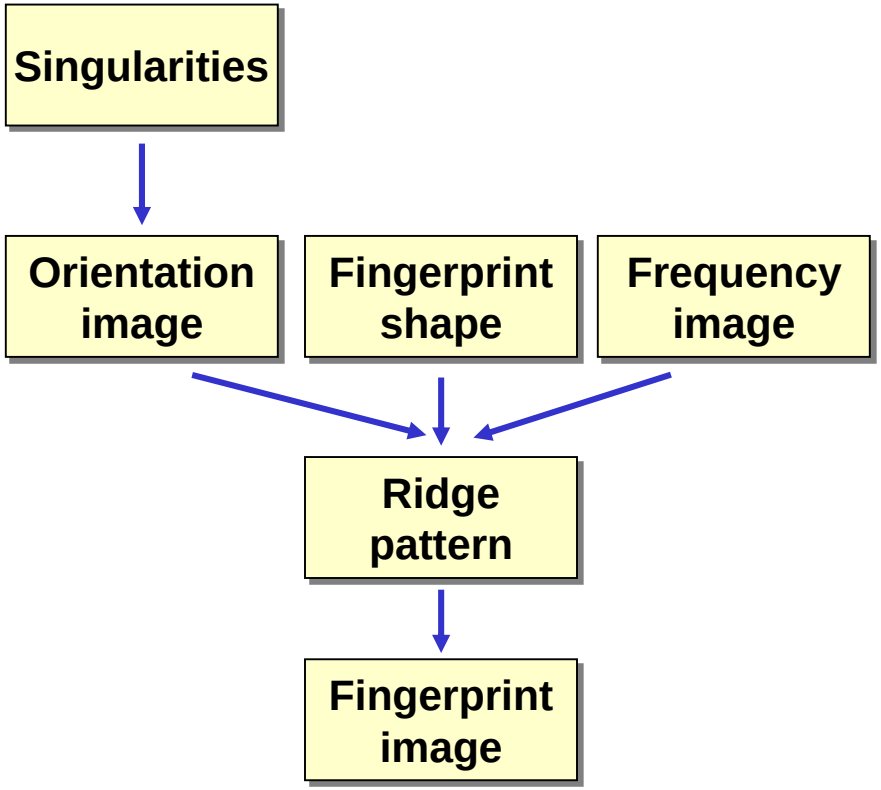
- expensive both in terms of money and time
- boring for both the people involved and for the volunteers, which are usually submitted to several acquisition sessions at different dates
- problematic due to the privacy legislation which protects such personal data

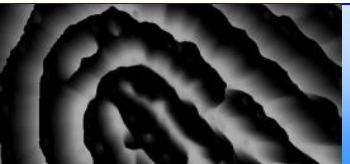
A method able to *artificially* generate realistic fingerprint-images could be used in several contexts to avoid collecting databases of real fingerprints



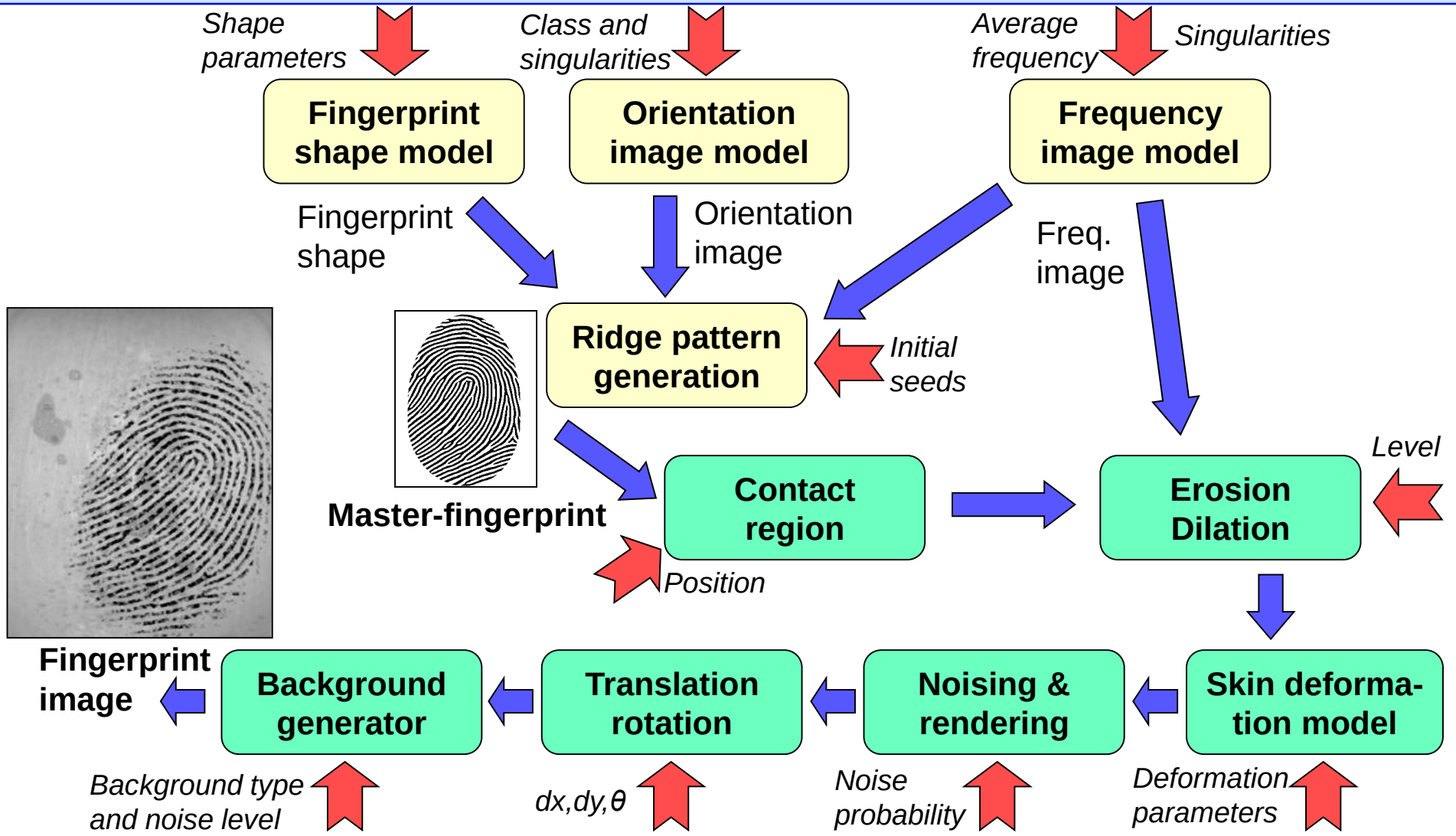


# How SFinGe works (1)



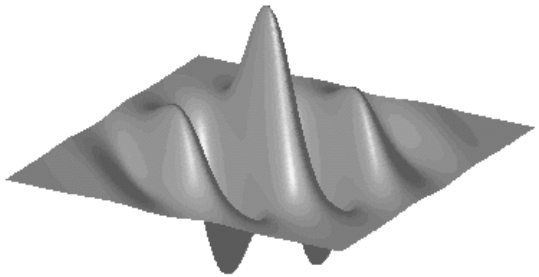
# How SFinGe works (3)



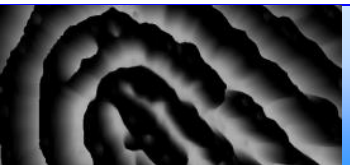
# Ridge pattern generation

Gabor-like filters are iteratively applied to an initially-white image, enriched with few random points.

The filters orientation and frequency are locally adjusted according to the orientation and frequency images.

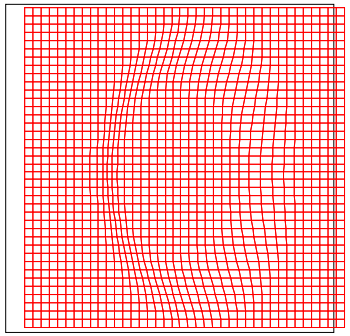


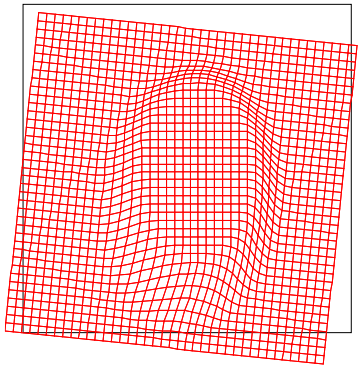
Realistic minutiae appear at random positions

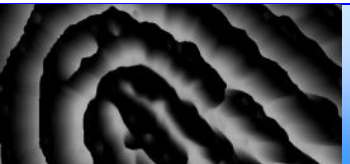


# Simulating skin distortion

The skin distortion model is applied to randomly generate realistic impressions of the same “synthetic finger”





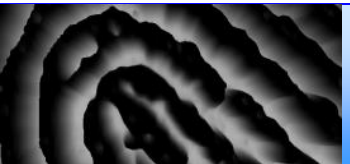


# Noising and rendering

Several factors contribute to deteriorate the quality of real fingerprints:

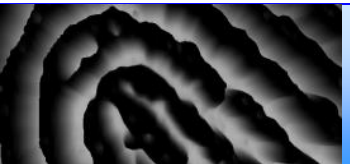
- irregularity of the ridges and their different contact with the sensor surface
- small cuts or abrasions on the fingertip
- presence of small pores within the ridges

SFinGe adds specific noise and applies an ad-hoc smoothing process to simulate real-fingerprints irregularities

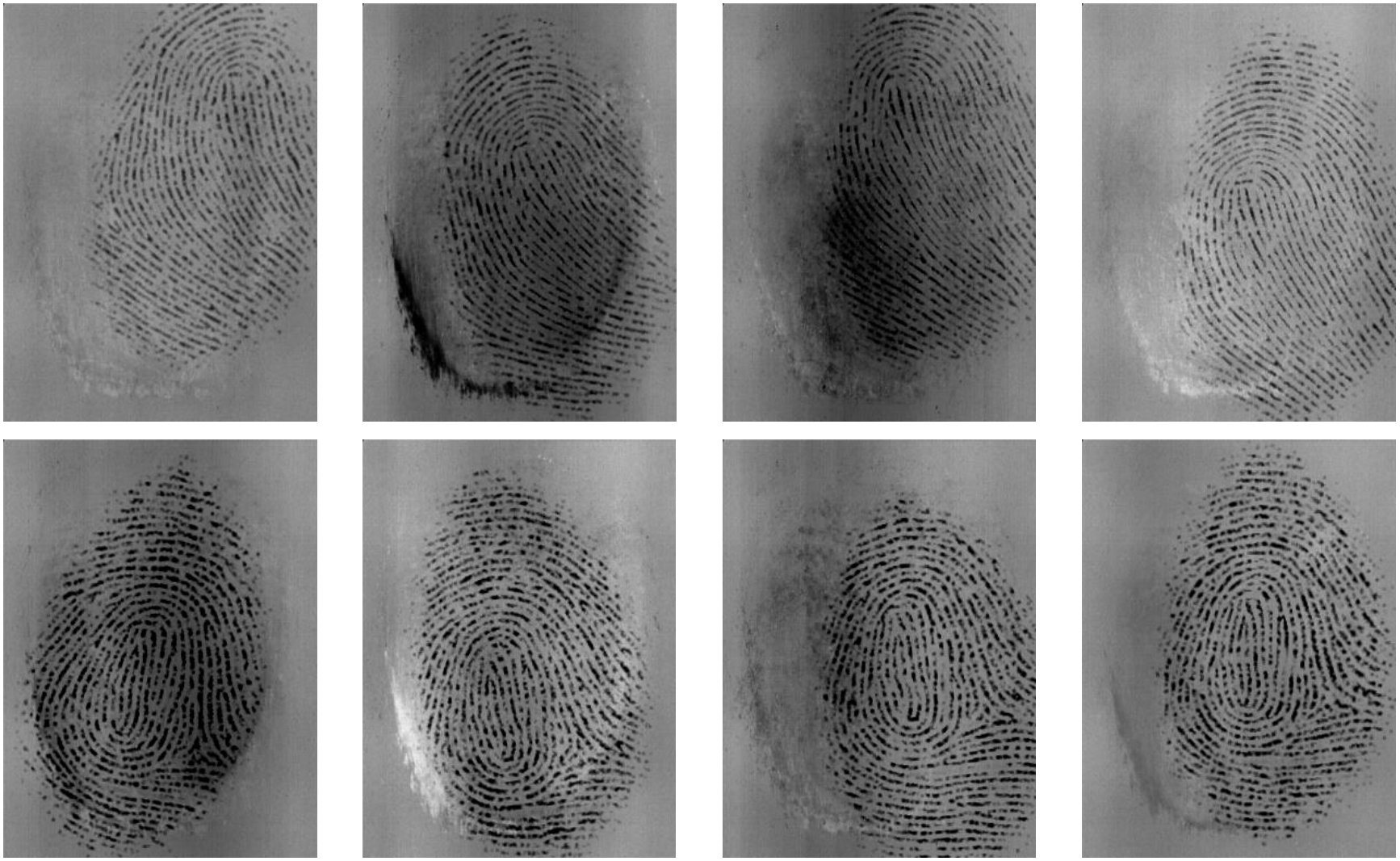


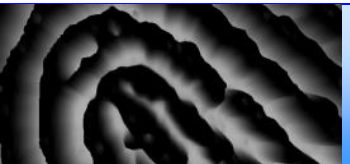
# Examples


Generated by Sfinge - © 2000 BioLab
University of Bologna - ITALY



# Examples (2)

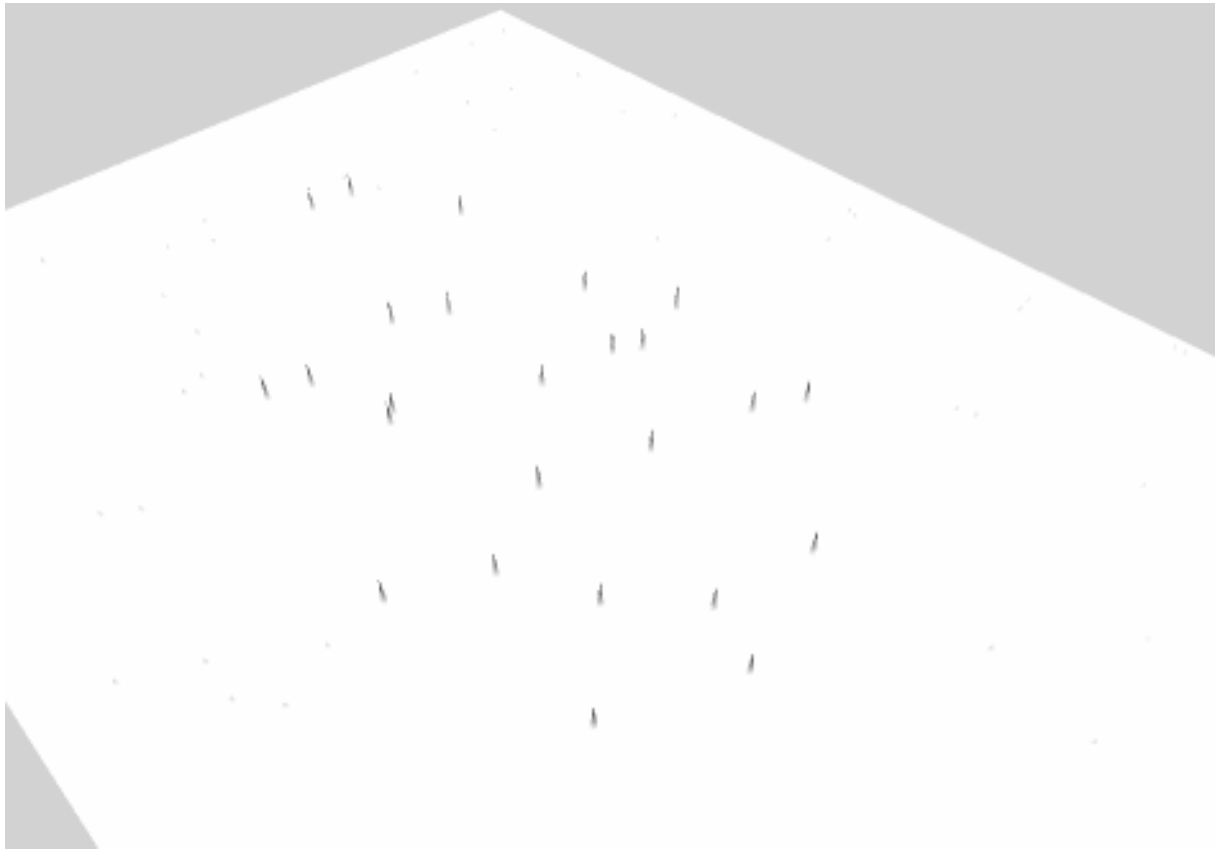


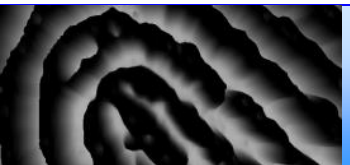


# SFinGe: generation of minutiae ground-truth

SfinGe “master fingerprints” are “ideal” fingerprint patterns

SfinGe “master fingerprints” are well-suited for applying the precise minutiae extraction procedures that are being proposed as ANSI and ISO standards.





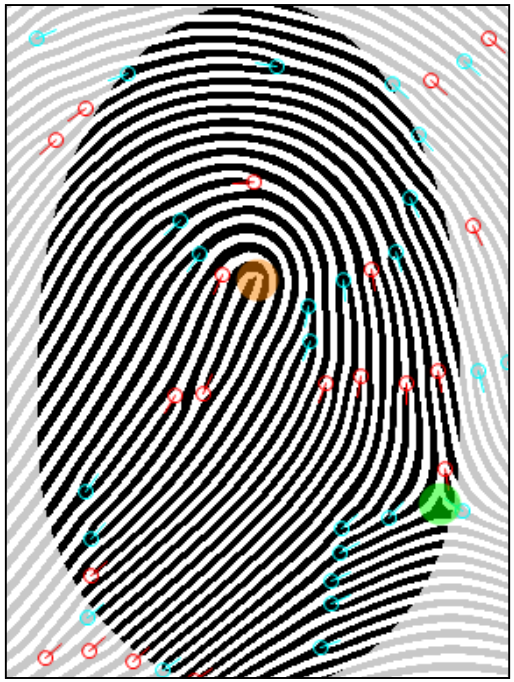
# Automatic generation of the *ground-truth*

Master-fingerprint

*SFinGe impression-generation steps*

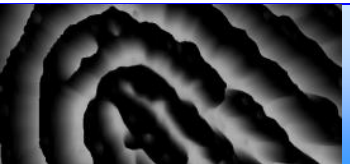
Fingerprint image

***Standard-compliant*** *feature extraction*



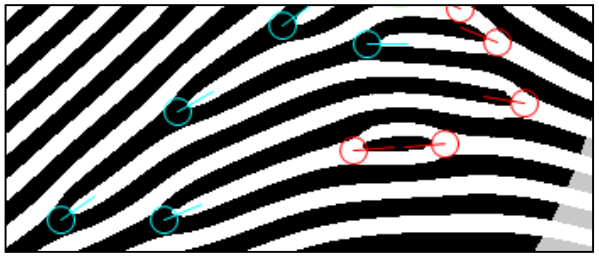
Master-fingerprint minutiae

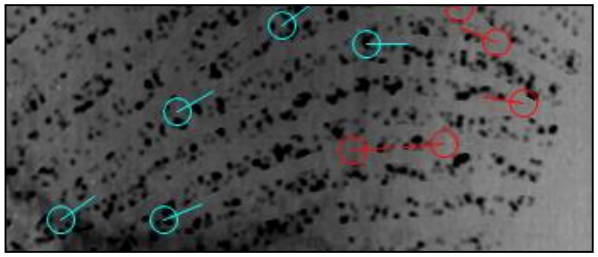
Ground-truth minutiae

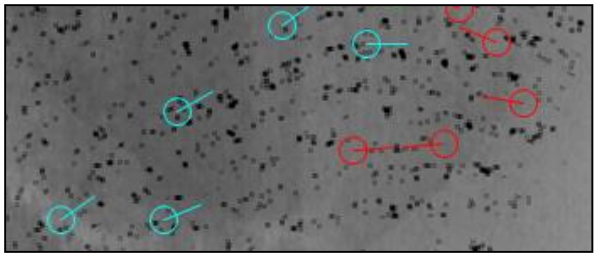


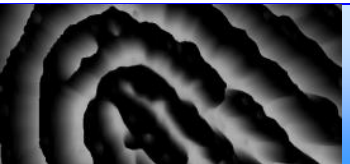
# Advantages of SFinGe minutiae ground-truth

- Automatic generation of large fingerprint databases with ground-truth minutiae
  - Features can be extracted by applying the standard procedures easily and without ambiguities (extraction occurs on a binary image without noise)
- The main fingerprint characteristics can be controlled
  - e.g. Fingerprint class, ridge line density, finger placement, skin distortion, fingerprint quality, ...
  - Datasets to test the impact of a given parameter (e.g. fingerprint quality) can be easily generated
- The ground truth is always unique and sound, even when the quality of the final image is very low









# SFinGe validation (1)

Fingerprint images generated by SFinGe appear very realistic

About 90 people (many of them having a good background in fingerprint analysis) have been asked to find a synthetic fingerprint image among 4 images (3 of which were real fingerprints).
The synthetic image proved to be not distinguishable from the others

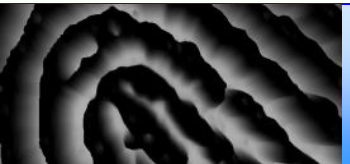

A


B


C

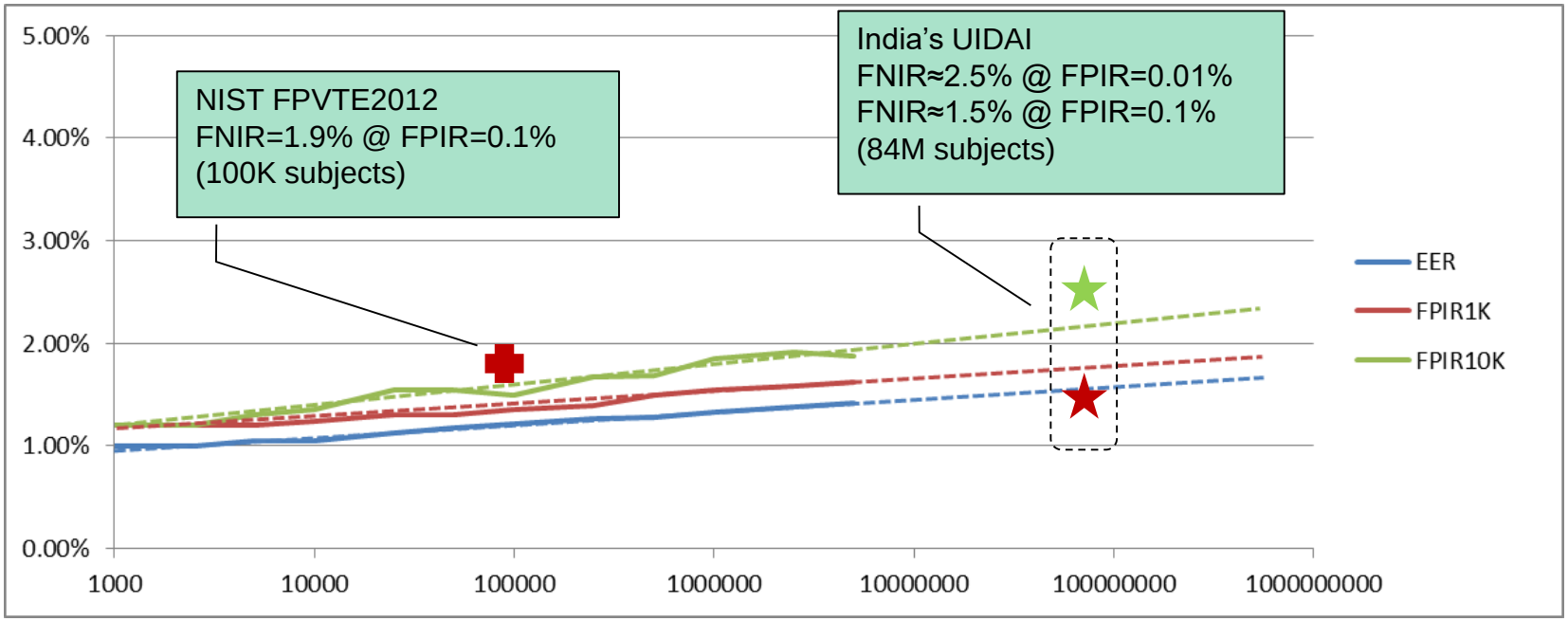

D

| *Poll results* | |
|---|---|
| A | 23% |
| B | 27% |
| C | 21% |
| D | 29% |



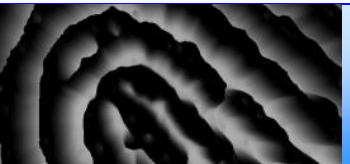
# SFinGe validation (2)

## Predicting fingerprint identification accuracy with synthetic data [Fidelity Project – EU]




20K queries (10K mates, 10K non-mates)

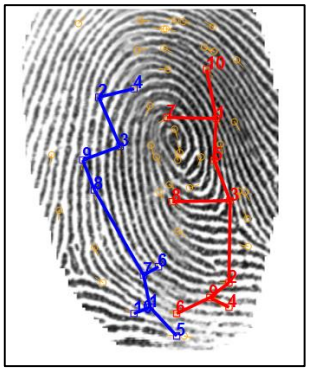
For this experiment: ≈ 200 billion fingerprint comparisons (carried out on a single PC in less than 11 hours, thanks to other Fidelity developments)



# Main challenges

Nowadays research on fingerprints is mainly active on:

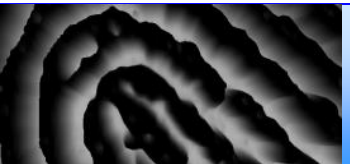
Double-identity fingerprints



Fake fingerprints

Altered fingerprints

Latent fingerprints

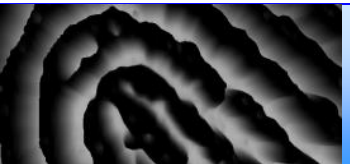


# Fake fingerprints

The idea of using fake fingerprints to fool biometric recognition is not new.

Diamonds are Forever
**(1971)**


*Bond goes undercover as Peter Franks, a diamond smuggler...*

# How to make a fake fingerprint?

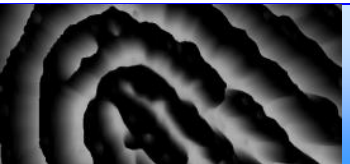
Making a fake finger is not easy, but it is possible with the right knowledge and the appropriate materials.

1) Press the finger into a putty-like material

2) Negative mold of the fingerprint

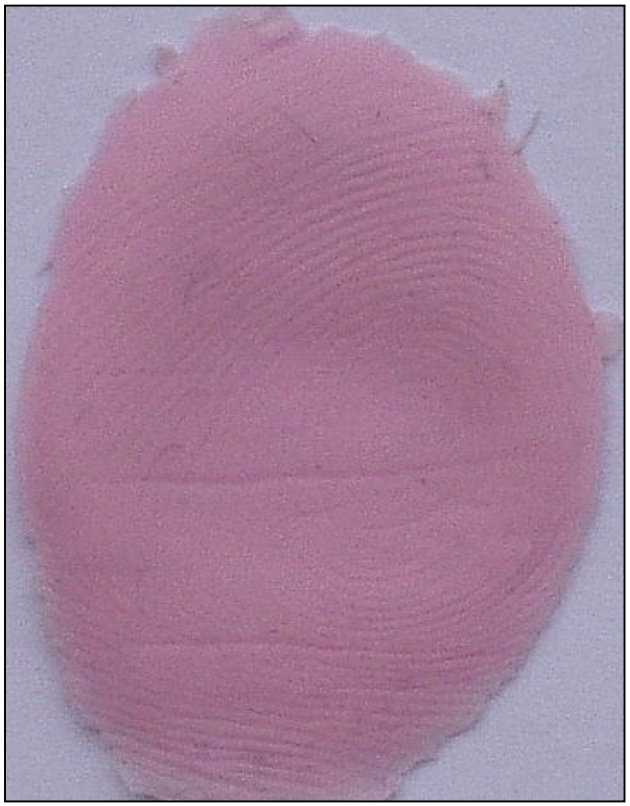
3) Pour the gelatine onto the mold

4) Fake fingerprint



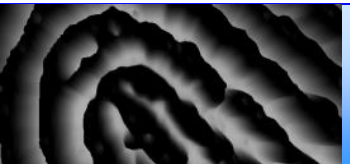
# Examples

Gelatine



Silicone

Latex



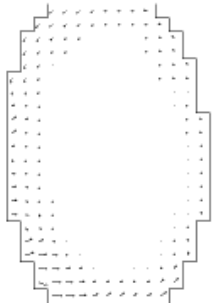
# Fake finger detection by distortion analysis

The user is required to place a finger onto the scanner surface and to apply some pressure while rotating the finger

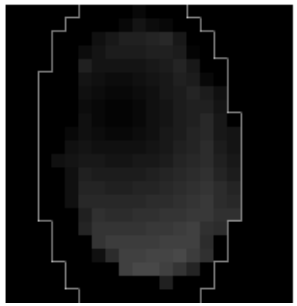
Real finger

Fake finger

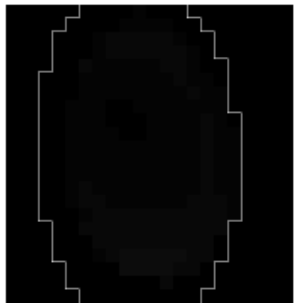
Source frame



Optical Flow



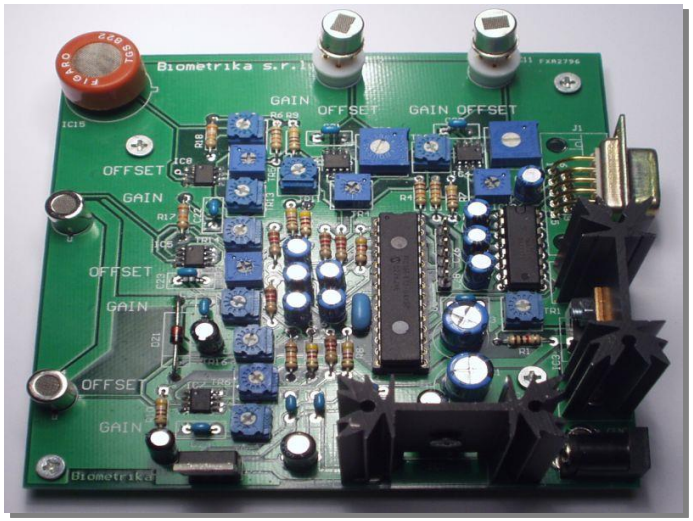
Distortion Map

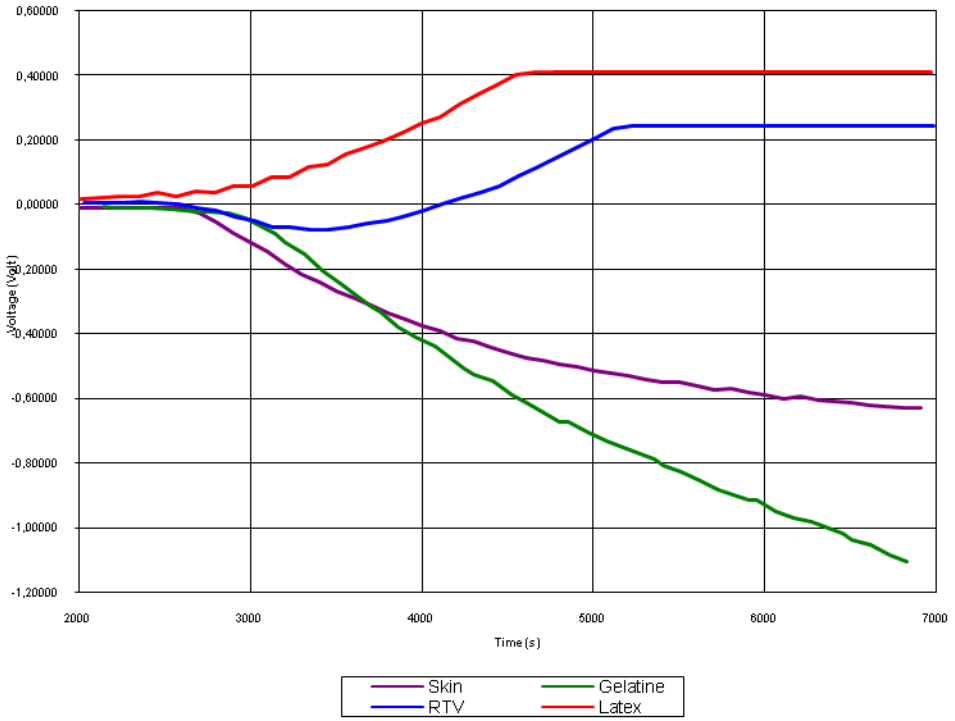


Integrated DM

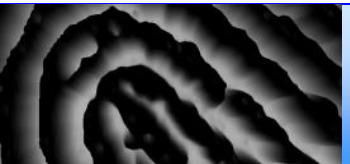
DistortionCode

# Fake finger detection by odor analysis




- The idea:
  - Using one or more odor sensors (*electronic noses*) to detect materials usually adopted to make fake fingers
    - Electronic nose: array of chemical sensors designed to detect and discriminate complex odors



# Solutions & Open issues

## Current solutions

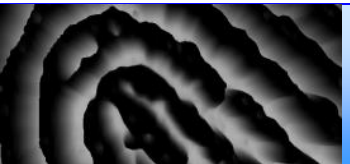
Fake finger detection methods based on properties of a live finger:

- temperature
- electrical conductivity
- skin elasticity
- skin color
- odor
- optical properties
- sub-surface properties
- pulsation
- blood pressure
- perspiration
- texture

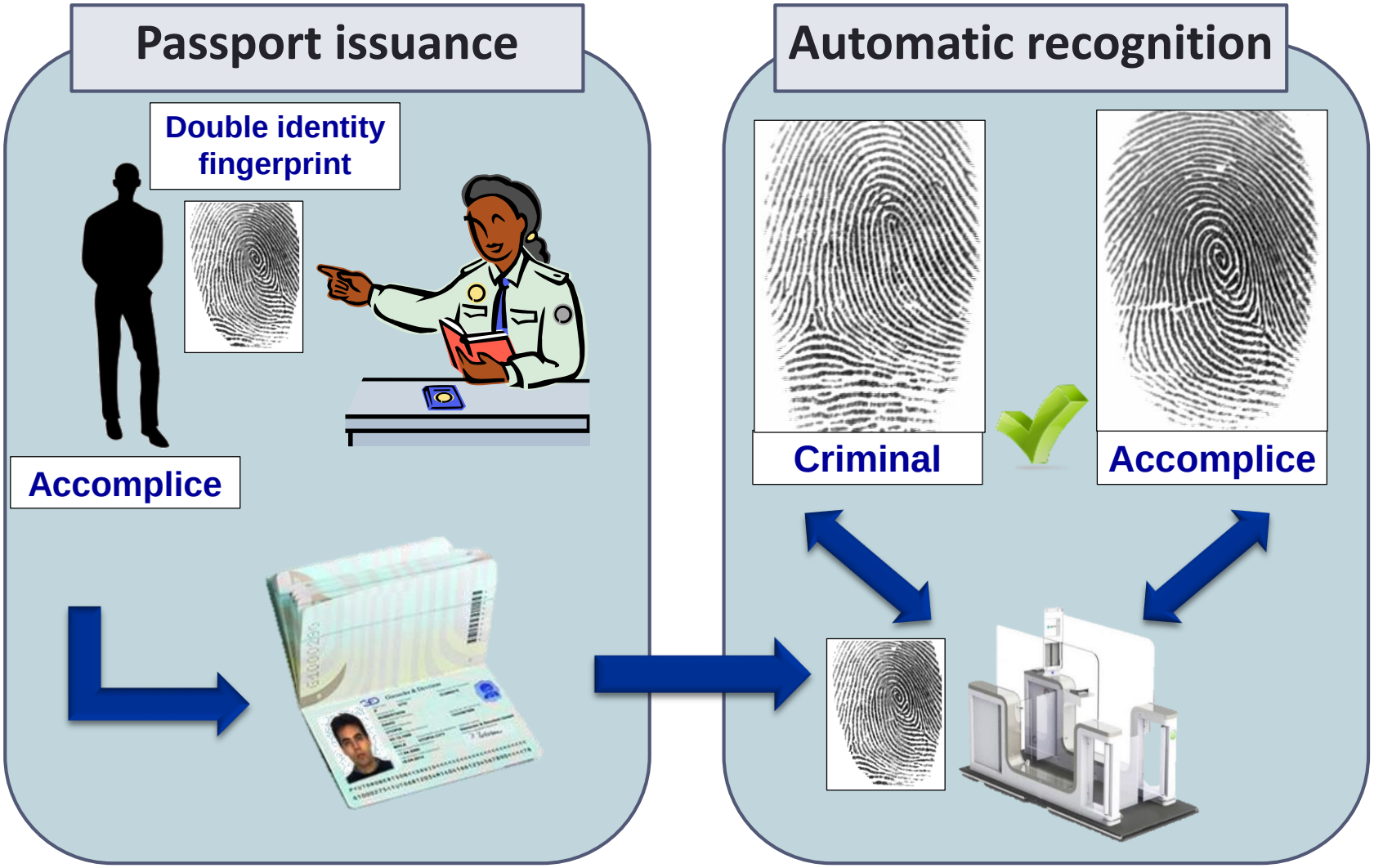
Since 2009 an independent competition called LivDet to compare biometric liveness detection approaches is organized every two years.

## Open issues

If the fake detection approach used by a fingerprint system is known, it is quite easy to imagine a fake finger attack able to fool this specific system.

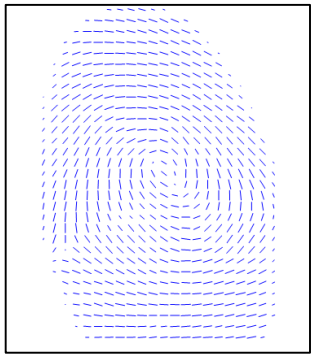


# Double-identity fingerprint attack

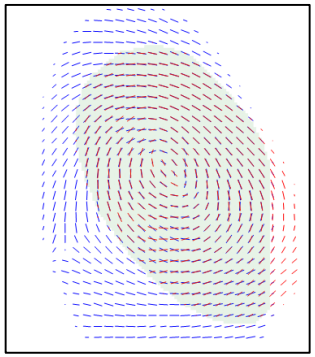


# Double-identity fingerprint generation

1. Fingerprint selection



2. Local orientations

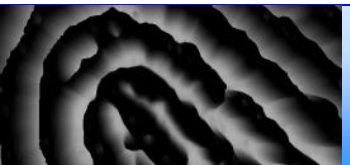


3. Best alignment

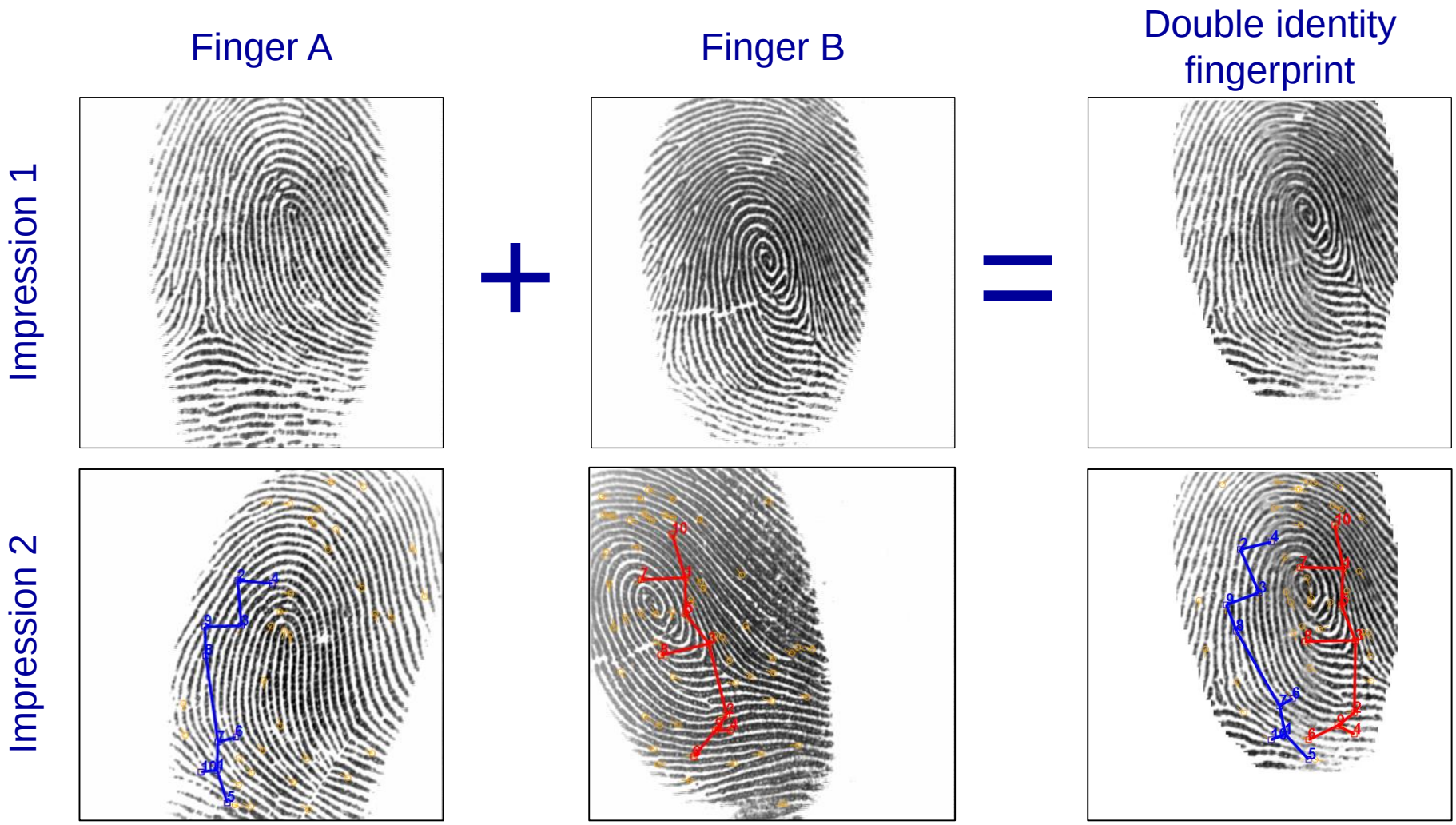
4. Fingerprint superimposition

5. Optimal cutline

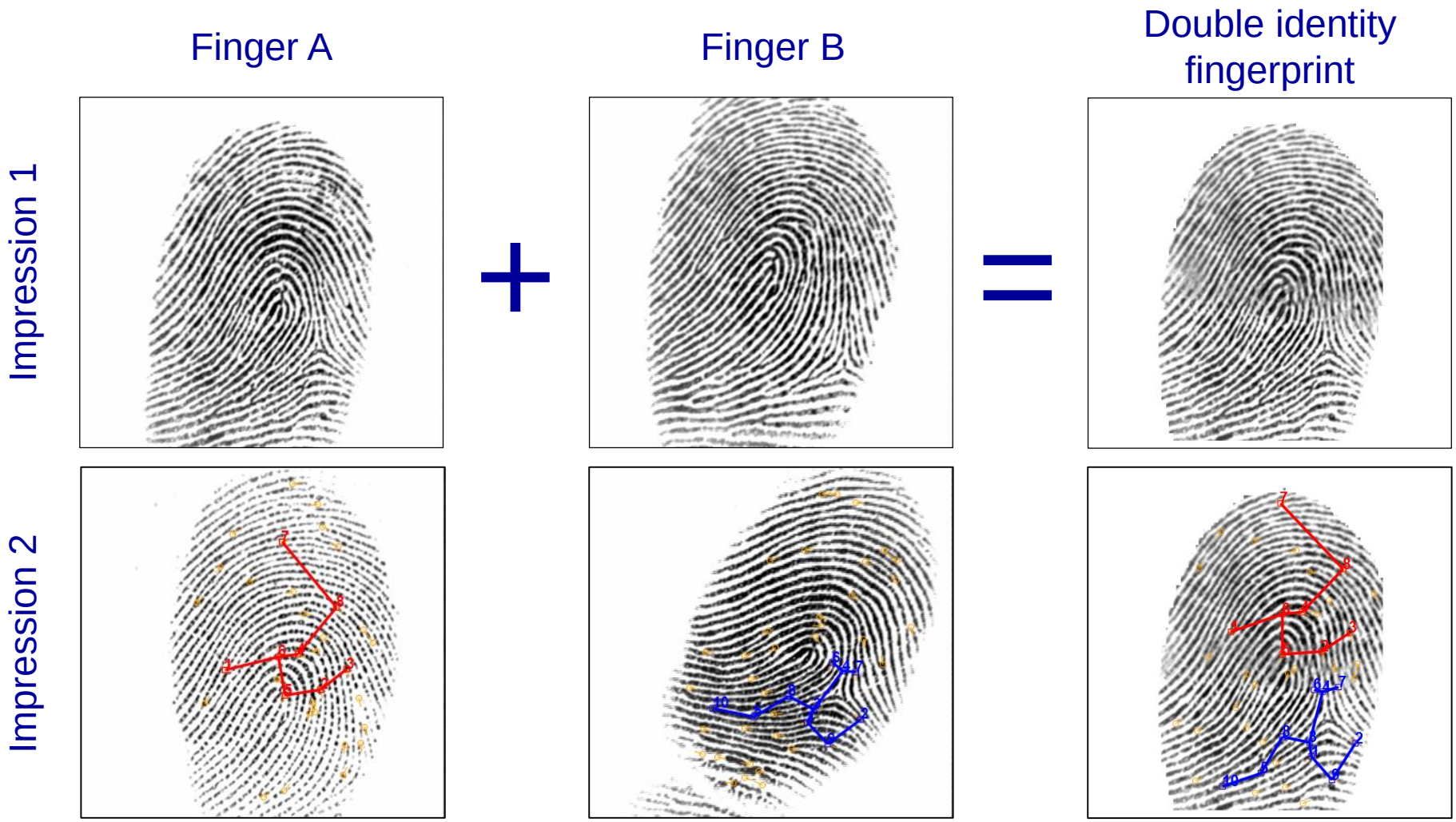
6. Fingerprint generation



# Examples (1)

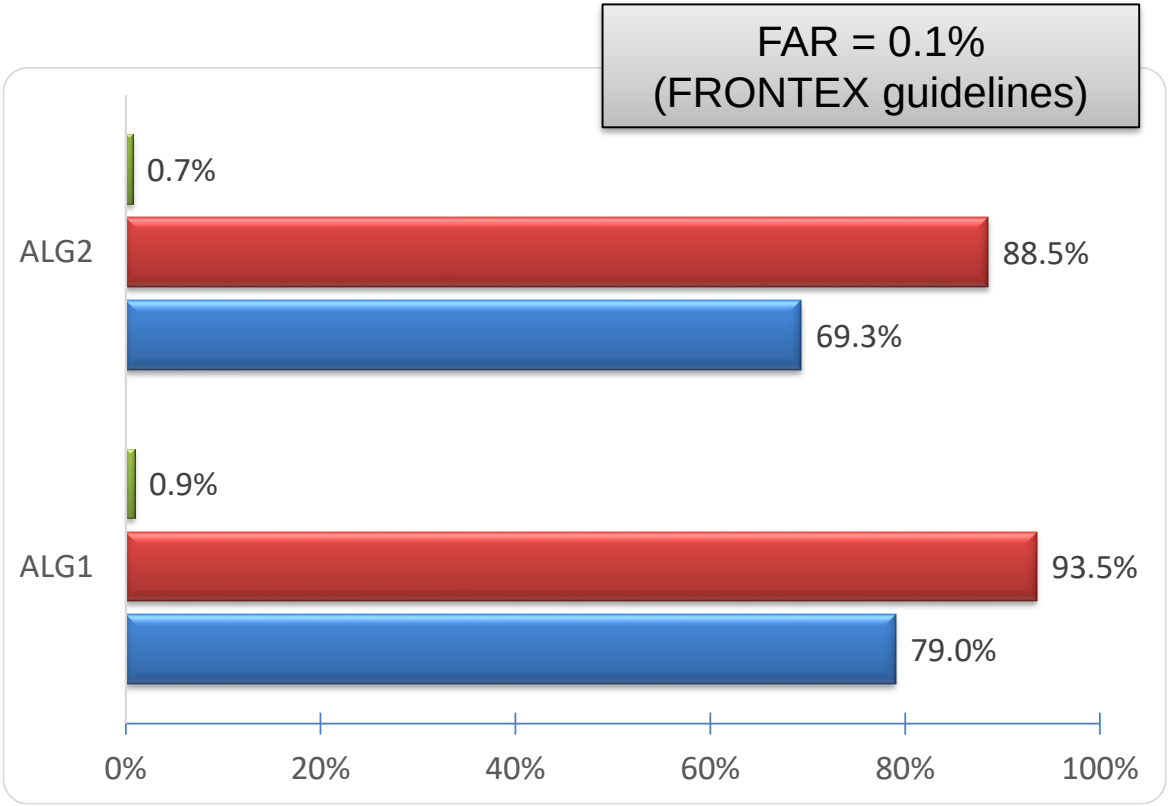

Finger A
Finger B
Double identity fingerprint
Impression 1
Impression 2
+
=

# Examples (2)


Finger A
Finger B
Double identity fingerprint
Impression 1
Impression 2

# Double-identity fingerprint experiments

Experiments have been conducted with two state-of-the-art fingerprint recognition algorithms on the FVC2002 DB1A database, containing 800 fingerprints from 100 fingers (8 impressions per finger) by performing 1400 attack attempts.




## Current solutions

None

## Open issues

- Double identity fingerprint detection methods
- Fingerprint recognition approaches able to deal with double identity attack

# Why alter fingerprints?

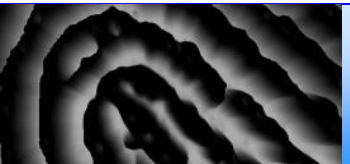
Criminals who want to avoid identification will try almost any method to irreversibly alter their fingerprints.

Transplanted

Bitten

Burnt with acid


Surgically altered

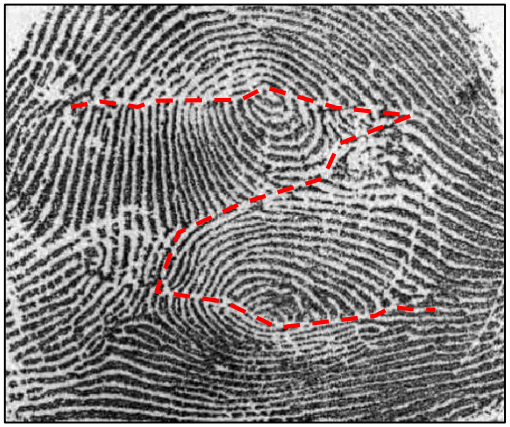


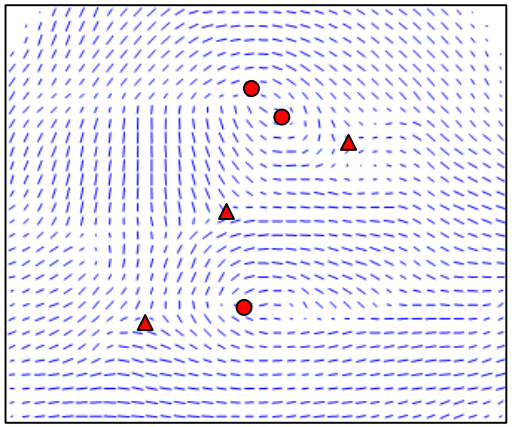
# Alterations

The alterations can be classified into three categories according to the resulting fingerprint pattern and not to the alteration process applied.

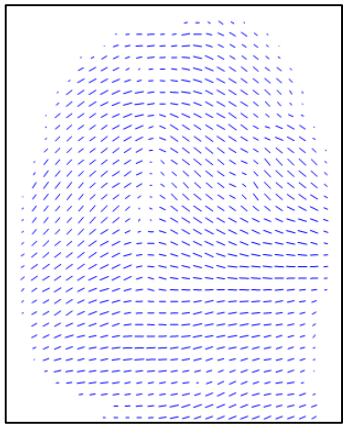
Obliteration

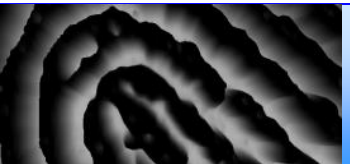
Distortion





Imitation





# Solutions & Open issues

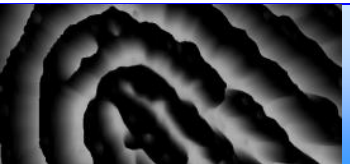
**Current solutions**

Altered fingerprint detection methods based on:

- ridge quality map
- singularity pattern analysis
- scar detection
- local orientation map analysis
- minutiae distribution analysis

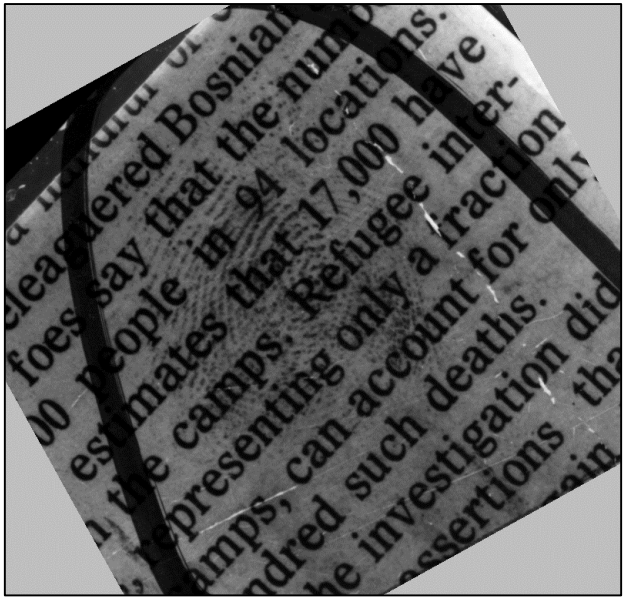
**Open issues**

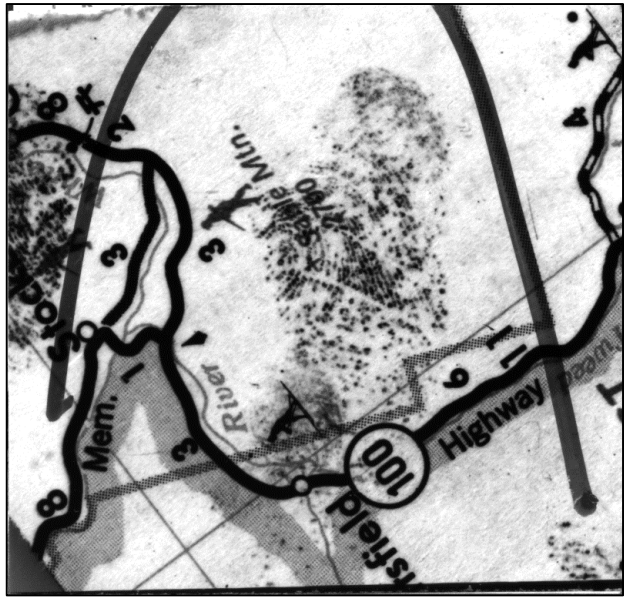
- reconstruct original fingerprint from the given altered one
- compare altered fingerprints to original ones



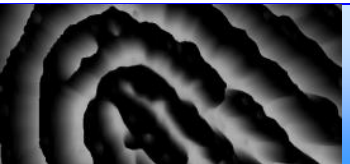
# What is a latent fingerprint?

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)



# Automatic Latent Processing

- Fully automatic ("lights-out") and highly accurate latent matching is one the major objectives of FBI's Next Generation Identification (NGI) program.
  - Automatic Minutiae extraction on noisy fingerprints is still a problem
    - Segmentation
    - Orientation and Frequency Estimation

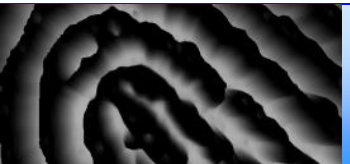
K. Cao and A. K. Jain, "Automated Latent Fingerprint Recognition", IEEE tPAMI, 2018

- Machine learning techniques are being introduced:

  2012…2014: dictionary-based techniques to estimate orientation field

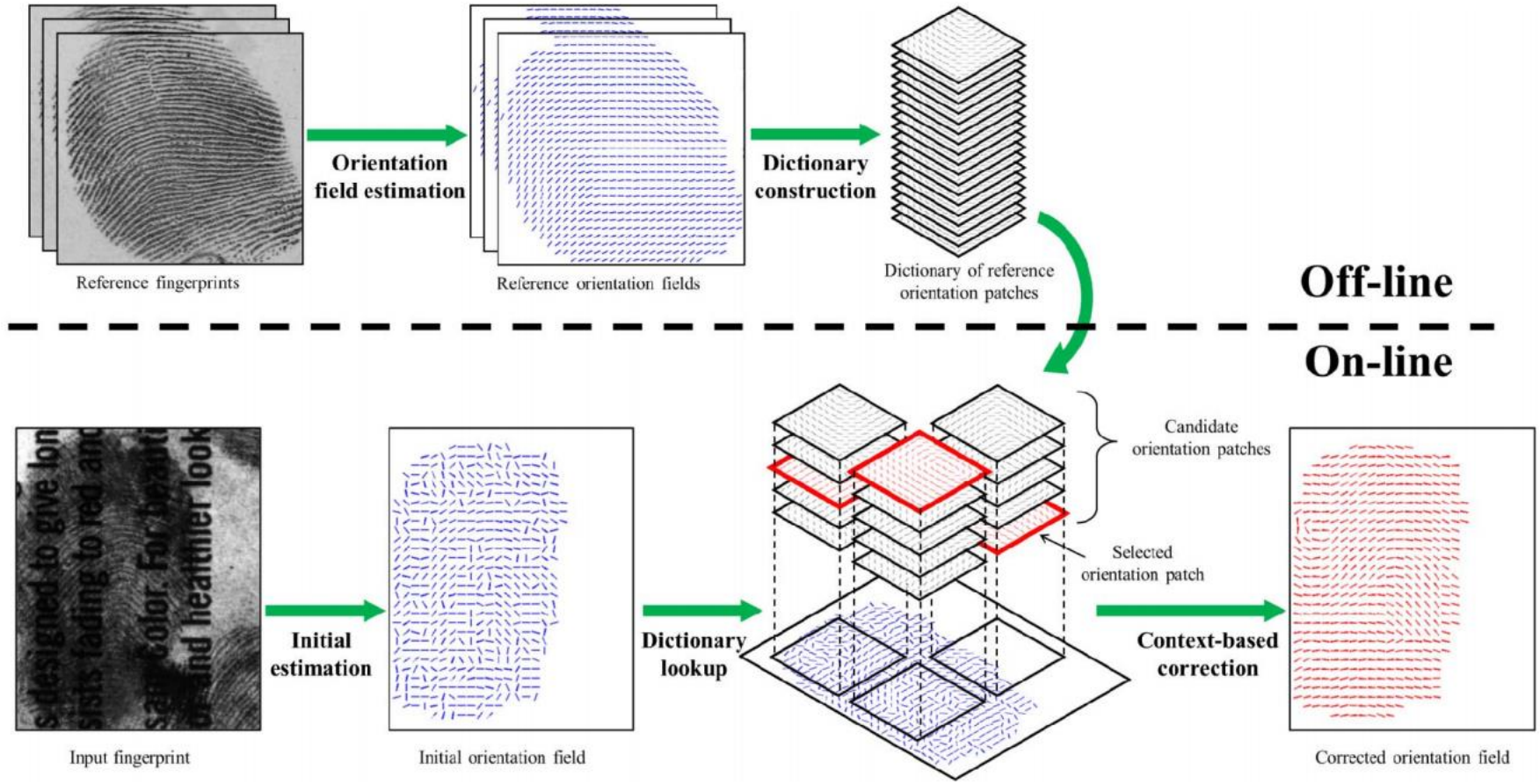
  2014…2018: deep learning approaches:

  - CNN (Convolutional Neural Networks) for orientation extraction, minutiae extraction, minutiae filtering and minutiae descriptors.
  - Autoencoders (denoising), GAN (Generative Adversarial Networks)



# Global Orientation Dictionary

J. Feng, J. Zhou, and A. K. Jain, "Orientation Field Estimation for Latent Fingerprint Enhancement", IEEE Trans. PAMI, 2013.

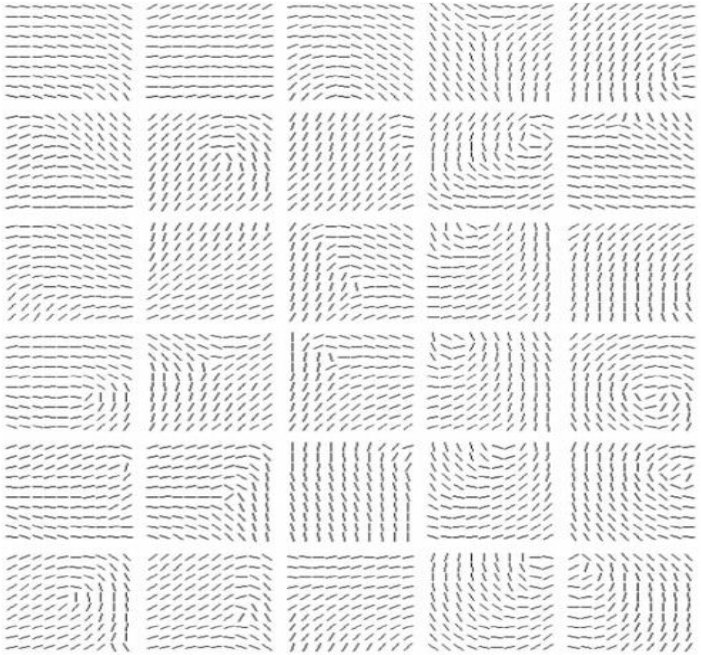


# Ridge Structure Dictionary

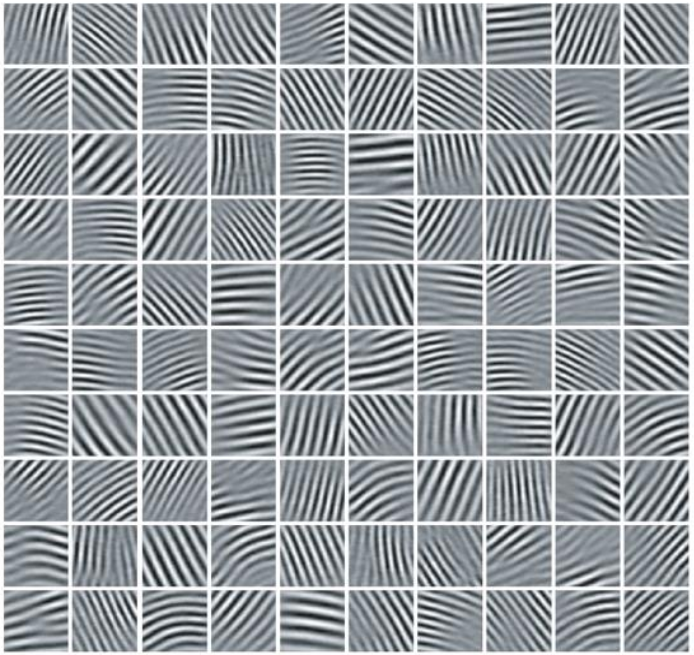
K. Cao, E. Liu and A. K. Jain, "Segmentation and Enhancement of Latent Fingerprints: A Coarse to Fine Ridge Structure Dictionary", IEEE Trans. PAMI, 2014.

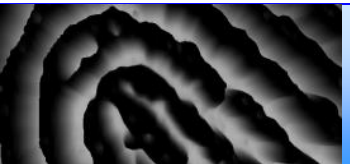
- Ridge-frequency can be estimated as well.

Orientation patches



Ridge structure patches

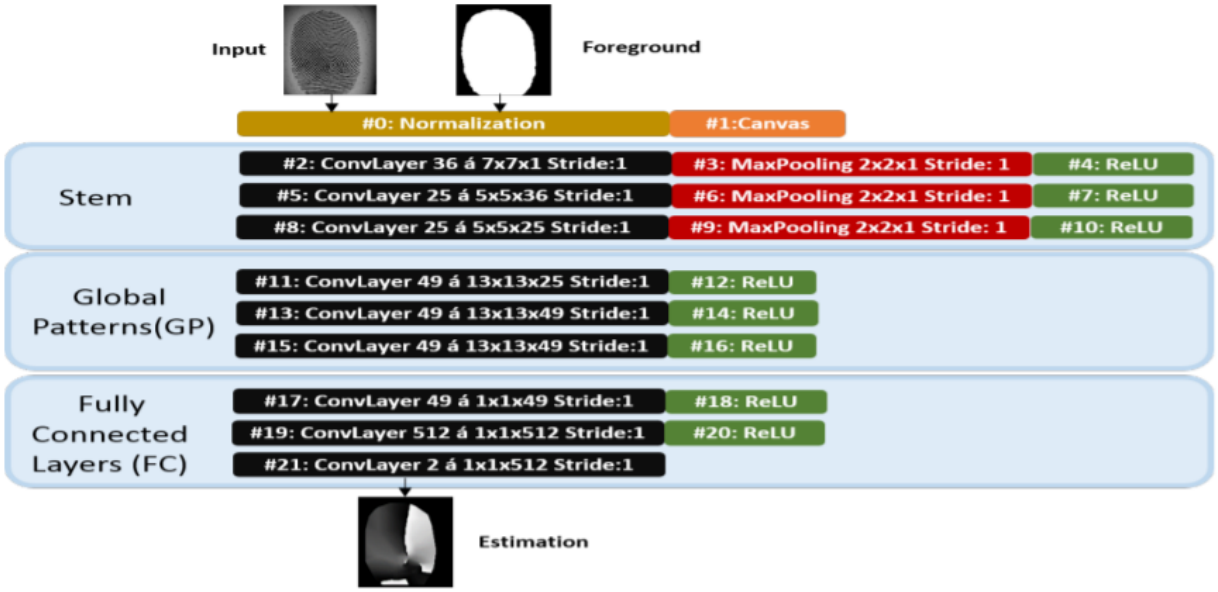


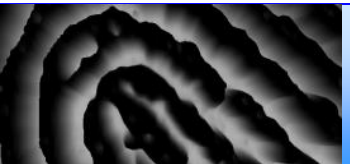


# Orientation Extraction with CNN

P. Schuch, S. D. Schulz and C. Busch, "Deep expectation for estimation of fingerprint orientation fields," IJCB, Denver, CO, 2017.

- Best Performing Approach (May 2018) on FVC-onGoing FOE
- In principle orientation estimation is a regression problem, but classification often proved to be better.
- Deep Expectation: weighted mean instead of winner take all



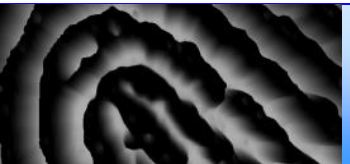
# Solutions & Open issues

**Current solutions**

- Semi-automatic tools supervised by human experts.
- Techniques based on prior knowledge of fingerprint structure.
- Novel approaches based on convolutional neural networks.

**Open issues**

Fully automatic (“lights-out”) and highly accurate latent comparison is one the major objectives of FBI’s Next Generation Identification (NGI) program.



# Thank you for your attention

http://biolab.csr.unibo.it
annalisa.franco@unibo.it

# References (1)


## Books

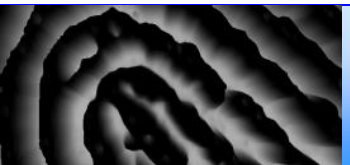
- D. Maltoni, D. Maio, A.K. Jain and S. Prabhakar, “Handbook of Fingerprint Recognition,” *Springer*, 2009.

## Fingerprint acquisition

- R. Cappelli, M. Ferrara and D. Maltoni, "On the Operational Quality of Fingerprint Scanners", *IEEE Transactions on Information Forensics and Security*, vol.3, no.2, pp.192-202, June 2008.
- A. Alessandroni, R. Cappelli, M. Ferrara and D. Maltoni, "Definition of Fingerprint Scanner Image Quality Specifications by Operational Quality", in *European Workshop on Biometrics and Identity Management (BIOID 2008)*, Roskilde, Denmark, May 2008.
- A. Roy, N. Memon and A. Ross, "MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 9, pp. 2013-2025, Sept. 2017.

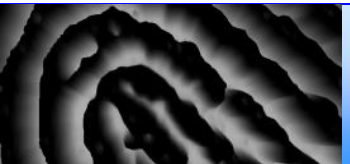
## Feature extraction

- B. M. Mehtre, N.N. Murthy, S. Kapoor, B. Chatterjee, “Segmentation of Fingerprint Images Using the Directional Image”, *Pattern Recognition*, vol. 20, no. 4, pp. 429-435, 1987.
- M. Kass, A. Witkin, “Analysing oriented patterns”, *Computer Vision Graphics and Image Processing*, vol. 11, no. 2, pp. 362-385, 1987.
- L. Hong, Y. Wan, A.K. Jain, “Fingerprint Image Enhancement Algorithms and Performance Evaluation”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 777-789, 1998.

# References (2)


- N.K. Ratha, S.Y. Chen, A.K. Jain, “Adaptive Flow Orientation-based Feature Extraction in Fingerprint Images”, *Pattern Recognition*, vol. 28, no. 11, pp. 1657-1672, 1995.
- D. Maio, D. Maltoni, “Direct Gray-Scale Minutiae Detection in Fingerprints”, *IEEE Transaction on Pattern Analysis and Machine Intelligence*, vol. 19, no. 1, 1997.
- L. Hong, Y. Wan and A. Jain, "Fingerprint image enhancement: algorithm and performance evaluation," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 777-789, Aug 1998.
- L. Jong, Y. Wan, A.K. Jain, “Fingerprint Image enhancement: Algorithms and Performance Evaluation”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, pp. 777-789, 1998.
- D. Maio and D. Maltoni, "Ridge-Line Density Estimation in Digital Images", in *14th International Conference on Pattern Recognition (ICPR)*, Brisbane, Australia, pp.534-538, August 1998.
- A. M. Bazen and S. H. Gerez, “Segmentation of Fingerprint Images,” in *12th Annual Workshop on Circuits, Systems and Signal Processing,* pp. 276-280, Veldhoven, The Netherlands, 2001.
- F. Turroni, D. Maltoni, R. Cappelli and D. Maio, "Improving Fingerprint Orientation Extraction", *IEEE Transactions on Information Forensics and Security*, vol.6, no.3, pp.1002-1013, September 2011.
- L. Jiang, T. Zhao, C. Bai, A. Yong and M. Wu, "A direct fingerprint minutiae extraction approach based on convolutional neural networks," in *International Joint Conference on Neural Networks (IJCNN)*, pp. 571-578 Vancouver, 2016.
- NIST. (2018, January) Development of NFIQ 2.0 web site. [OnLine] http://www.nist.gov/services-resources/software/development-nfiq-20

# References (3)

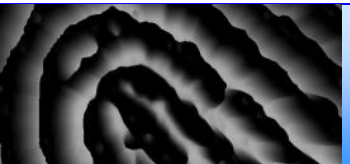
## Fingerprint comparison


- N.K. Ratha, K. Karu, S. Chen, A.K. Jain, “A Real-Time Matching System for Large Fingerprint Databases”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 18, no. 8, pp. 799-813, 1996.
- N.K. Ratha, V.D. Pandit, R.M. Bolle, V. Vaish, “Robust Fingerprint Authentication Using Local Structural Similarity”, in *Workshop on Applications of Computer Vision*, pp. 29-34, 2000.
- A.K. Jain, S. Prabhakar, L. Hong, S. Pankanti, “Filterbank-Based Fingerprint Matching”, *IEEE Transactions on Image Processing*, vol. 9, pp. 846-859, 2000.
- X. Jiang, W.Y. Yau, “Fingerprint Minutiae Matching Based on the Local and Global Structures”, in *International Conference on Pattern Recognition*, vol. 2, pp. 1042-1045, 2000.
- M. Tico, P. Kuosmanen, “Fingerprint Matching Using an Orientation-Based Minutia Descriptor”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 8, pp. 1009-1014, 2003.
- R. Cappelli, M. Ferrara and D. Maltoni, "Minutia Cylinder-Code: a new representation and matching technique for fingerprint recognition", *IEEE Transactions on Pattern Analysis Machine Intelligence*, vol.32, no.12, pp.2128-2141, December 2010.
- J. Feng and J. Zhou, "A Performance Evaluation of Fingerprint Minutia Descriptors," *2011 International Conference on Hand-Based Biometrics*, pp. 1-6, Hong Kong, 2011.
- R. Cappelli, M. Ferrara and D. Maltoni, "Large-scale fingerprint identification on GPU", *Information Sciences*, vol.306, pp.1-20, June 2015.
- D. Peralta et al., “A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation”, *Information Sciences*, vol. 315, pp. 67-87, September 2015.
- BioLab. (2018, January). MCC SDK web site. [Online]. http://biolab.csr.unibo.it/mccsdk.html.


# References (4)

## Performance evaluation


- D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman and A.K. Jain, "FVC2000: Fingerprint Verification Competition", *IEEE Transactions on Pattern Analysis Machine Intelligence*, vol.24, no.3, pp.402-412, March 2002.
- D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman and A.K. Jain, "FVC2002: Second Fingerprint Verification Competition", in *16th International Conference on Pattern Recognition (ICPR2002)*, Québec City, vol.3, pp.811-814, August 2002.
- D. Maio, D. Maltoni, R. Cappelli, J.L. Wayman and A.K. Jain, "FVC2004: Third Fingerprint Verification Competition", in *International Conference on Biometric Authentication (ICBA04)*, Hong Kong, pp.1-7, July 2004.
- R. Cappelli, M. Ferrara, A. Franco and D. Maltoni, "Fingerprint verification competition 2006", Biometric Technology Today, vol.15, no.7-8, pp.7-9, August 2007.
- B. Dorizzi, R. Cappelli, M. Ferrara, D. Maio, D. Maltoni, N. Houmani, S. Garcia-Salicetti and A. Mayoue, "Fingerprint and On-Line Signature Verification Competitions at ICB 2009", in *International Conference on Biometrics (ICB)*, Alghero, Italy, pp.725-732, June 2009.
- BioLab. (2018, January) FVC2000 web site. [Online]. http://bias.csr.unibo.it/fvc2000.
- BioLab. (2018, January) FVC2002 web site. [Online]. http://bias.csr.unibo.it/fvc2002.
- BioLab. (2018, January) FVC2004 web site. [Online]. http://bias.csr.unibo.it/fvc2004.
- BioLab. (2018, January) FVC2006 web site. [Online]. http://bias.csr.unibo.it/fvc2006.
- BioLab. (2018, January) FVC-onGoing web site. [Online]. http://biolab.csr.unibo.it/fvcongoing.
- BioLab. (2018, January) SFinGe web site. [Online]. http://biolab.csr.unibo.it/sfinge.html.

# References (5)


## Fake fingerprints

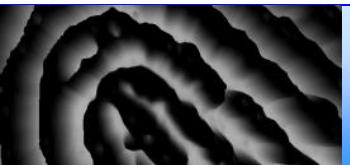
- T. Matsumoto, H. Matsumoto, K. Yamada and S. Hoshino, "Impact of artificial "gummy" fingers on fingerprint systems," *Proc. SPIE 4677, Optical Security and Counterfeit Deterrence Techniques IV*, vol. 4677, pp. 275-289, April 2002.
- A. Antonelli, R. Cappelli, D. Maio and D. Maltoni, "Fake Finger Detection by Skin Distortion Analysis", *IEEE Transactions on Information Forensics and Security*, vol.1, no.3, pp.360-373, September 2006.
- D. Baldisserra, A. Franco, D. Maio and D. Maltoni, "Fake Fingerprint Detection by Odor Analysis", in *International Conference on Biometrics*, pp. 265-272, 2006.
- (2018, January). LivDet web site. [Online]. http://livdet.org.

## Double-identity fingerprints

- M. Ferrara, R. Cappelli and D. Maltoni, "On the Feasibility of Creating Double-Identity Fingerprints", *IEEE Transactions on Information Forensics and Security*, vol.12, no.4, pp.892-900, April 2017.

## Altered fingerprints

- J. Feng, A. K. Jain and A. Ross, "Detecting Altered Fingerprints," *20th International Conference on Pattern Recognition*, Istanbul, 2010, pp. 1622-1625.
- S. Yoon, J. Feng and A. K. Jain, "Altered Fingerprints: Analysis and Detection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 34, no. 3, pp. 451-464, March 2012.

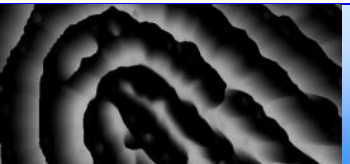
# References (6)

## New sensors


- M. O. Derawi, B. Yang, and C. Busch, “Fingerprint Recognition with Embedded Cameras on Mobile Phones”, in *International Conference on Security and Privacy in Mobile Information and Communication Systems*, 2011.
- R. D. Labati, A. Genovese, V. Piuri, and F. Scotti, “Touchless fingerprint biometrics: a survey on 2D and 3D technologies”, *Journal of Internet Technology*, vol. 15, n. 3, pp. 325-332, May 2014.
- E. Auksorius, and A. C. Boccara, "Fingerprint imaging from the inside of a finger with full-field optical coherence tomography," *Biomed. Optics Express,* 6 (11), 4465-4471, 2015.


## Latent fingerprints


- J. Feng, J. Zhou, and A. K. Jain, "Orientation Field Estimation for Latent Fingerprint Enhancement", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 4, pp. 925-940, April 2013.
- X. Yang, J. Feng and Jie Zhou, “Localized Dictionaries Based Orientation Field Estimation for Latent Fingerprints”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 5, pp. 955-969, May 2014.
- K. Cao, E. Liu and A. K. Jain, "Segmentation and Enhancement of Latent Fingerprints: A Coarse to Fine Ridge Structure Dictionary", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 36, no. 9, pp. 1847-1859, Sept. 2014.
- K. Cao and A. K. Jain, "Latent orientation field estimation via convolutional neural network" in *International Conference on Biometrics (ICB)*, pp. 349– 356, 2015.

# References (7)

## Template protection


- A. Juels and M. Sudan, “A Fuzzy Vault Scheme,” *IEEE International Symposium on Information Theory*, 2002.
- A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security”, *EURASIP Journal on Advances in Signal Processing*, January 2008.
- M. Ferrara, D. Maltoni and R. Cappelli, "Noninvertible Minutia Cylinder-Code Representation", *IEEE Transactions on Information Forensics and Security*, vol.7, no.6, pp.1727-1737, December 2012.
- M. Ferrara, D. Maltoni and R. Cappelli, "A Two-Factor Protection Scheme for MCC Fingerprint Templates", in *International Conference of the Biometrics Special Interest Group (BIOSIG)*, Darmstadt, Germany, September 2014.
- Pradheeba and R. Subban, "Fingerprint template protection techniques — A survey and analysis,“ in *IEEE International Conference on Computational Intelligence and Computing Research*, Coimbatore, pp. 1-6, 2014.