GREYC
E-payment & Biometrics

CNRS

UNICAEN

ENSICAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

How can machines recognize us? The fingerprint case

Christophe Rosenberger

L'École des INGÉNIEURS Scientifiques

OUTLINE

- A short presentation of the GREYC Lab
- Notions on Biometrics
- Focus on fingerprint
- Fingerprint quality assessment
- Protection of fingerprints

GREYC

RESEARCH LAB

Research in Digital Science

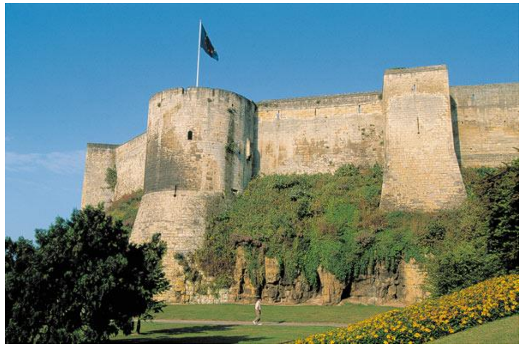
computer security, biometrics, cryptography, machine learning, electronics, image processing, artificial intelligence, Web science...

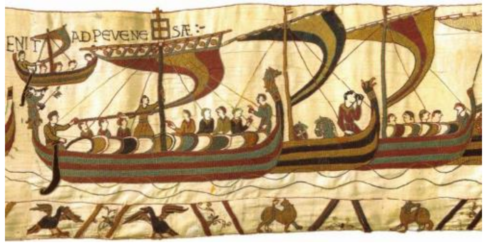
cnrs dépasser les frontières

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

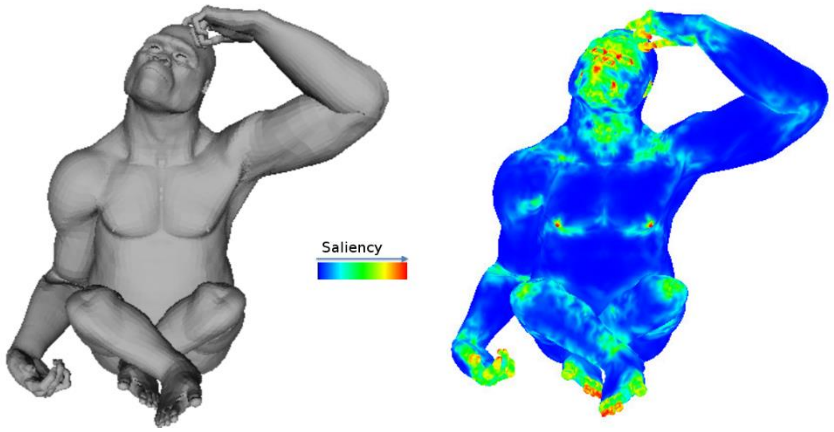
GREYC RESEARCH LAB





GREYC RESEARCH LAB

Research Group in Computer science, Automatics, Image processing and Electronics of Caen



Staff

- 7 CNRS researchers
- 21 Full professors
- 58 Associate professors
- 42 PhD students
- 15 Administrative and technical staffs
- 30 non permanent staffs

GREYC RESEARCH LAB

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

7 research groups:

- AMACC: Computation models, Randomness, Cryptography, Complexity
- CODAG: Constraints, Data mining, Graphs
- HULTECH: Human Language technologies
- MAD: Models, Agents and Decisions
- IMAGE: Image
- ELEC: Electronics
- E-Payment & Biometrics

E-PAYMENT & BIOMETRICS UNIT

Research activities in computer security

Members

2 full professors, 5 associate professors, 12 PhD students, 2 post-docs, 5 R&D engineers

RESEARCH TOPICS

TRUST

Codes & applied cryptography

Architectures & applications with secure element

Random data & information security

BIOMETRICS

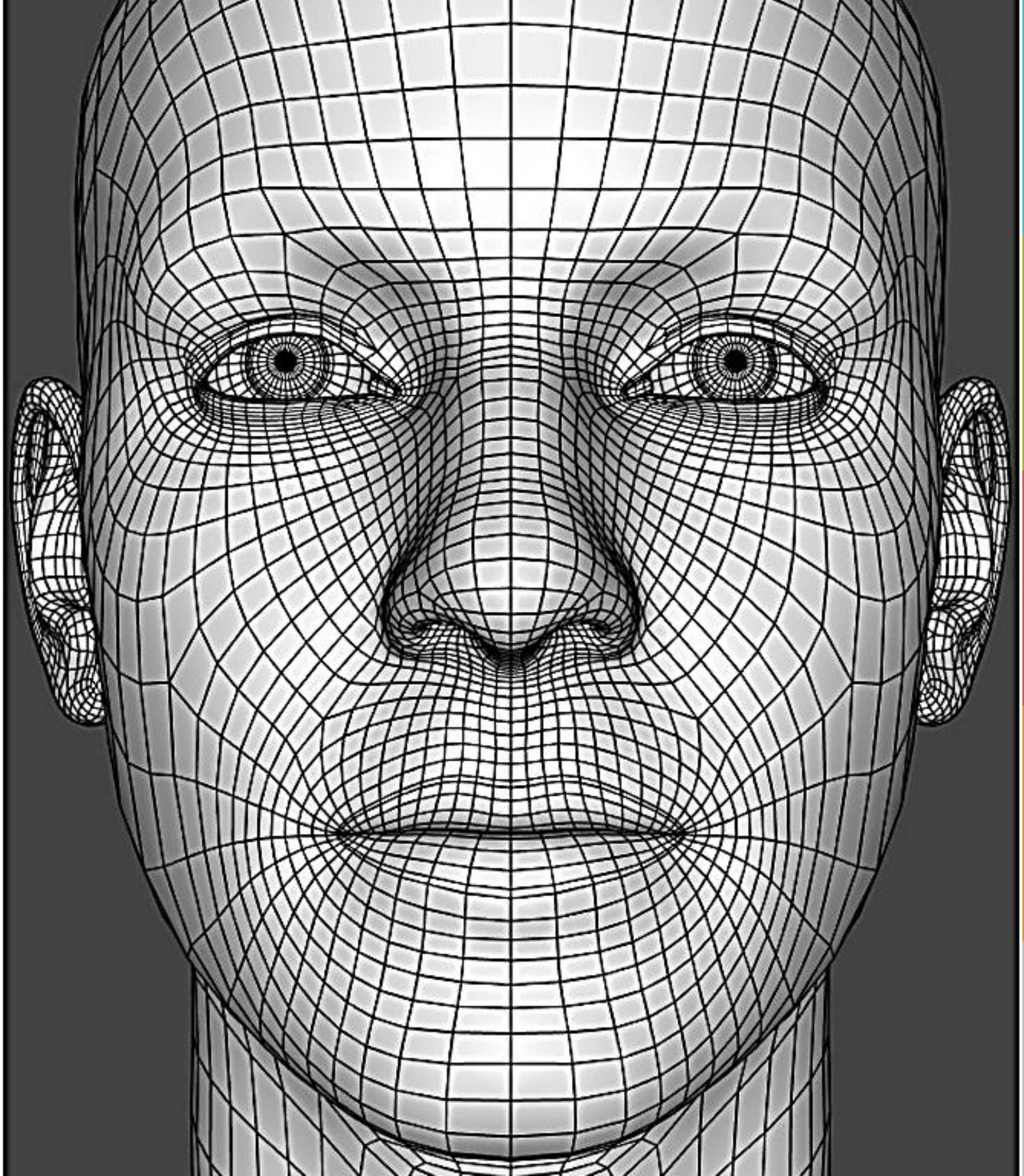
Definition of biometric systems

Evaluation of biometric systems

Protection of biometric data

GREYC

E-payment & Biometrics



GREYC

INTRODUCTION

BIOMETRICS

Automatic identification of an individual or verification of its identity by using morphological or behavioral characteristics

BIOMETRICS

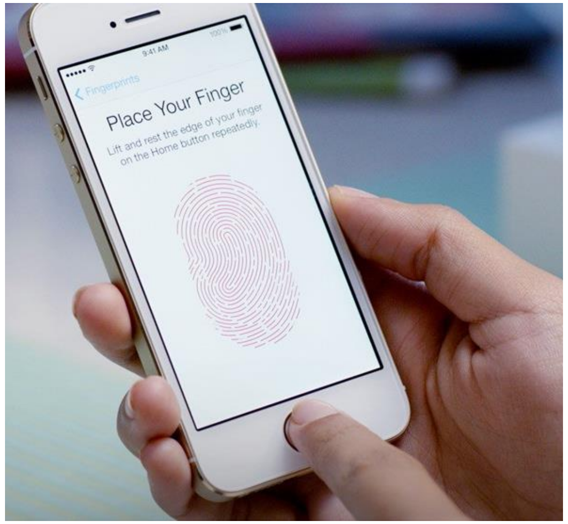
Biometric modalities

- **Biological analysis**:
  EEG signal, DNA…

- **Behavioural analysis**:
  Keystroke dynamics, voice, gait, signature dynamics…

- **Morphological analysis**:
  Fingerprint, iris, palmprint, finger veins, face, ear…

ILLUSTRATIONS



APPLICATIONS

Applications

- Physical access control (buildings),
- Logical access control (computer, information..),
- Identity control (police, frontiers…),
- E-Government,
- Equipment,
- Machines…

DEFINITIONS

Biometric sample: analog or digital representation of biometric characteristics prior to biometric feature extraction

Biometric reference: one or more stored biometric samples, biometric templates or biometric models attributed to a biometric data subject and used as the object of biometric comparison

Biometric sample

Biometric reference

$$T = \{m_1, \dots, m_n\}$$

With $m_i = (x_i, y_i, \theta_i, T_i)$

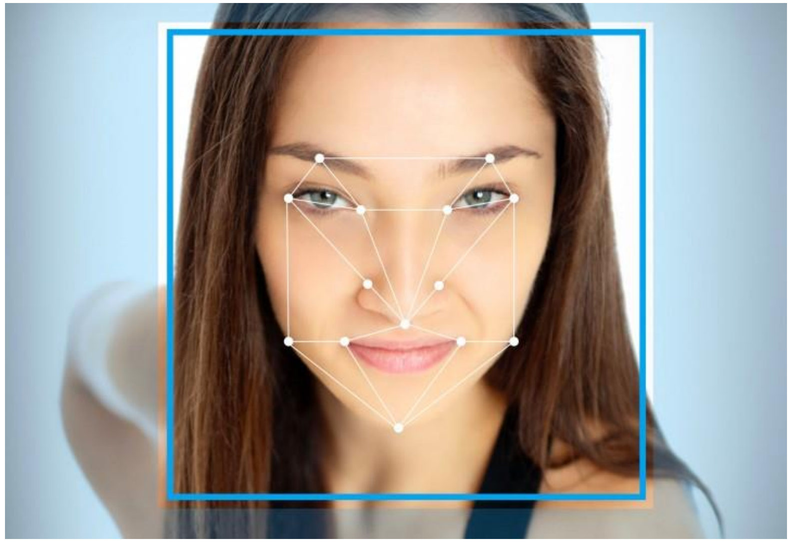
(x_i, y_i): minutiae location
$\theta_i: minutiae\ orientation$
$T_i: minutiae\ type$

DEFINITIONS

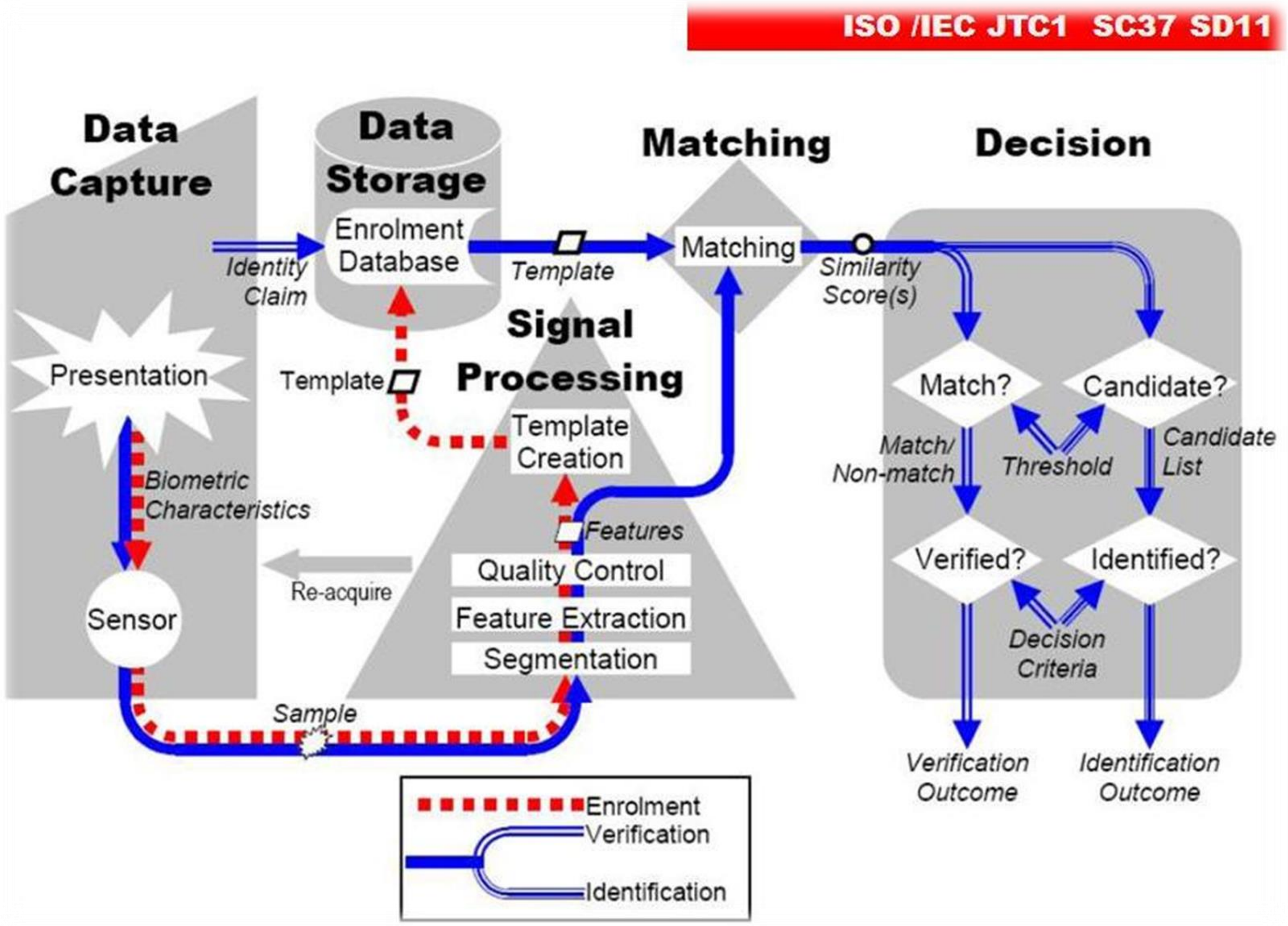
Enrollment: act of creating and storing a biometric reference data record

Verification: process of confirming a biometric claim through a biometric comparison

Identification: process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual



BIOMETRIC SYSTEM



PERFORMANCE

AR database

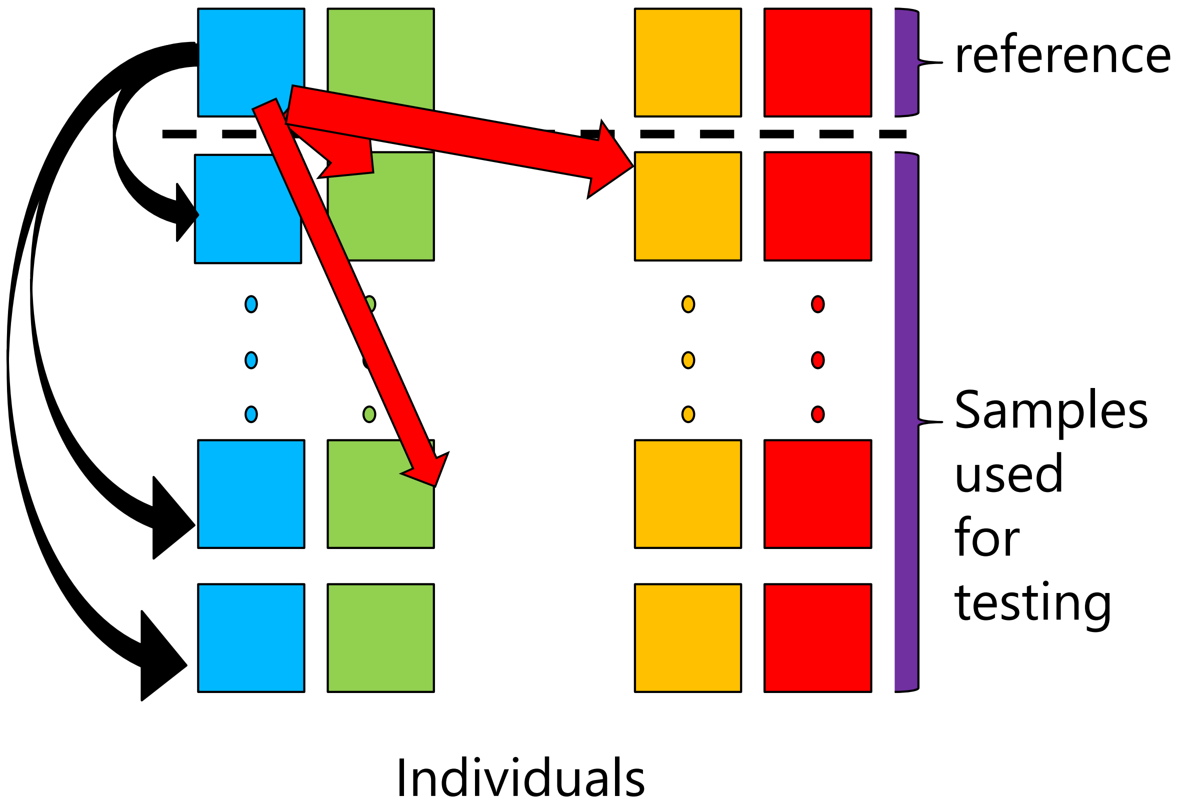
A.M. Martinez and R. Benavente, “The AR face database”, CVC Tech. Report, 24, 1998.

- 120 individuals: 65 men and 55 women,
- 26 images per individual,
- 2 sessions spaced of 2 weeks

Reference

Samples

PERFORMANCE



Distribution of legitimate and impostor scores

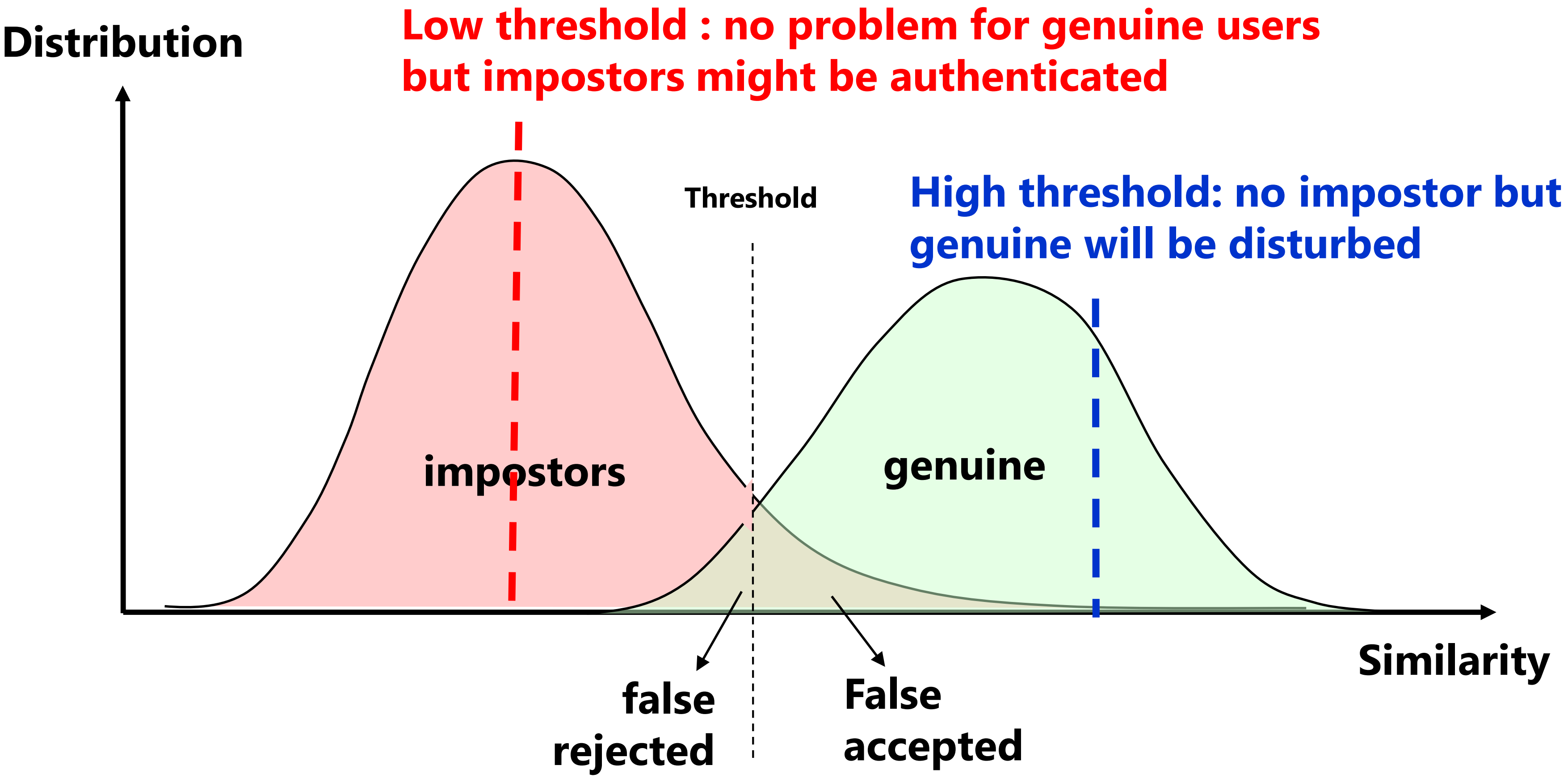
1. Computation of scores
2. Plotting the frequency of each value

Legitimate scores: comparison between a sample and the reference of the same user

Impostor scores: comparison between a sample and the reference of a different user

PERFORMANCE

Distribution of legitimate and impostor scores:



PERFORMANCE

Acquisition metrics

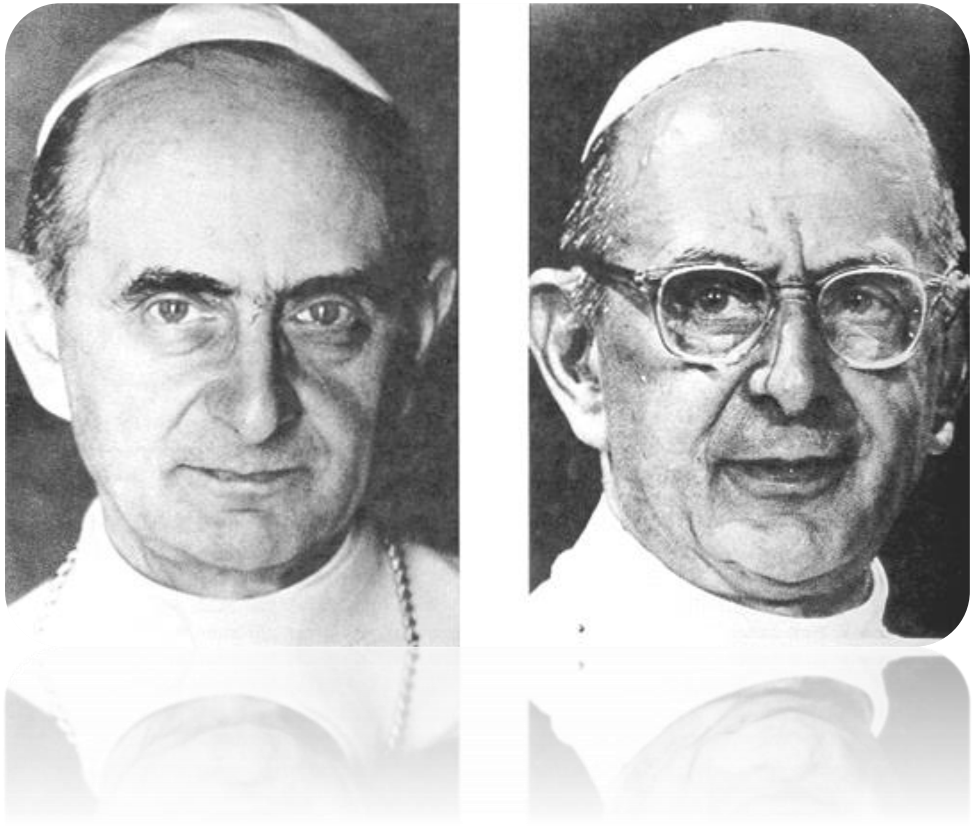
- **Failure To Acquire Rate**
  - ✓ FTAR
  - ✓ Problem during capture
  - ✓ Physical incapacity
  - ✓ Sensor does not work

- **Failure To Enroll Rate**
  - ✓ FTER
  - ✓ Insufficient biometric quality
  - ✓ User does not want to enroll himself

PERFORMANCE

Authentication metrics (algorithm)

- **False Match Rate**
  - ✓ FMR
  - ✓ Ratio of impostors accepted
- **False Non Match Rate**
  - ✓ FNMR
  - ✓ Ratio of genuine users refused

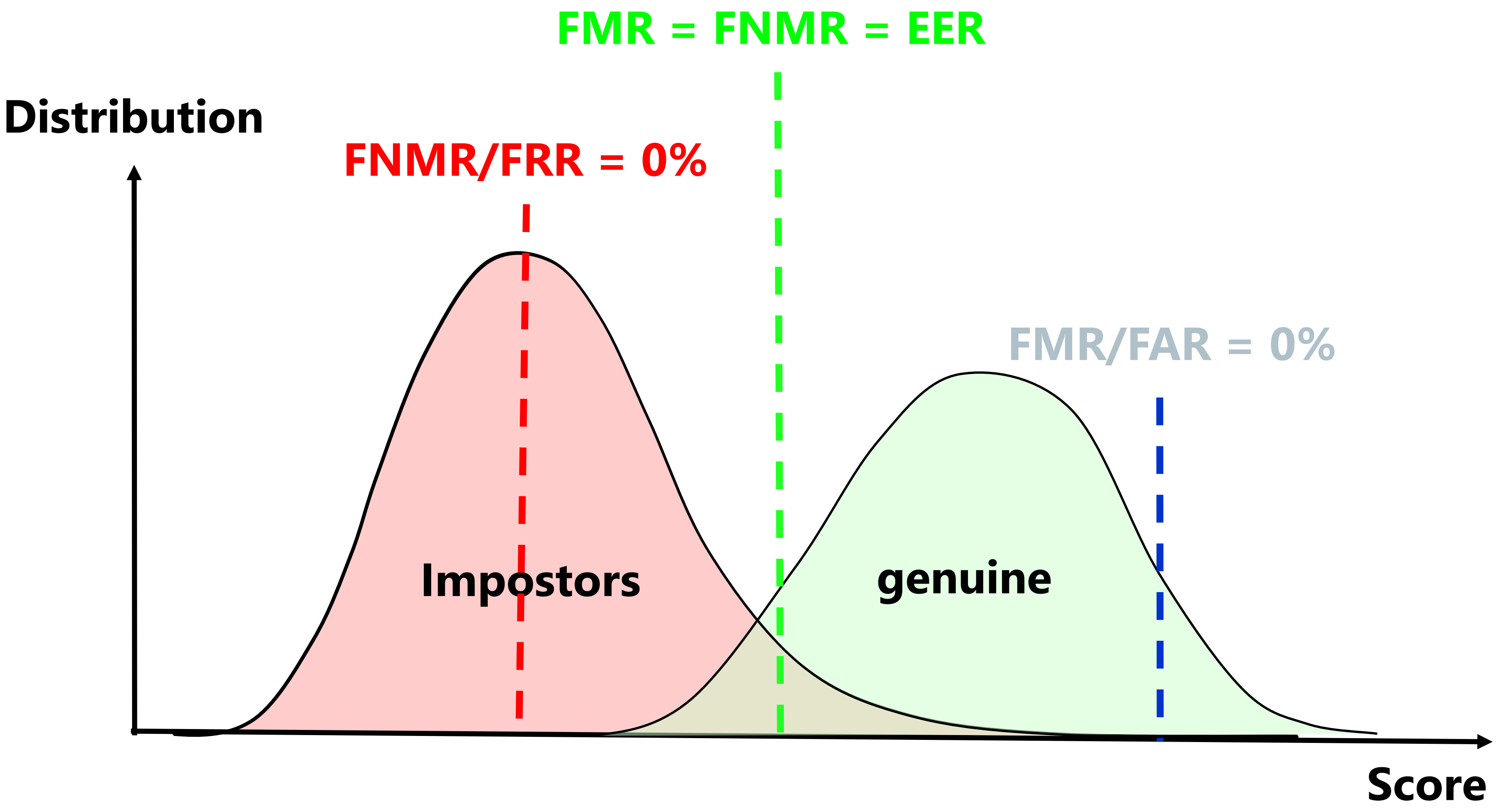


PERFORMANCE

Authentication metrics (system)

- **False Acceptation Rate**
  - ✓ FAR
  - ✓ $FAR(\theta) = (1 - FTAR).FMR(\theta)$
- **False Rejection Rate**
  - ✓ FRR
  - ✓ $FRR(\theta) = (1 - FTAR).FNMR(\theta) + FTAR$
- **Equal Error rate**
  - ✓ EER
  - ✓ $EER=FAR(\theta^*)=FRR(\theta^*)$

PERFORMANCE

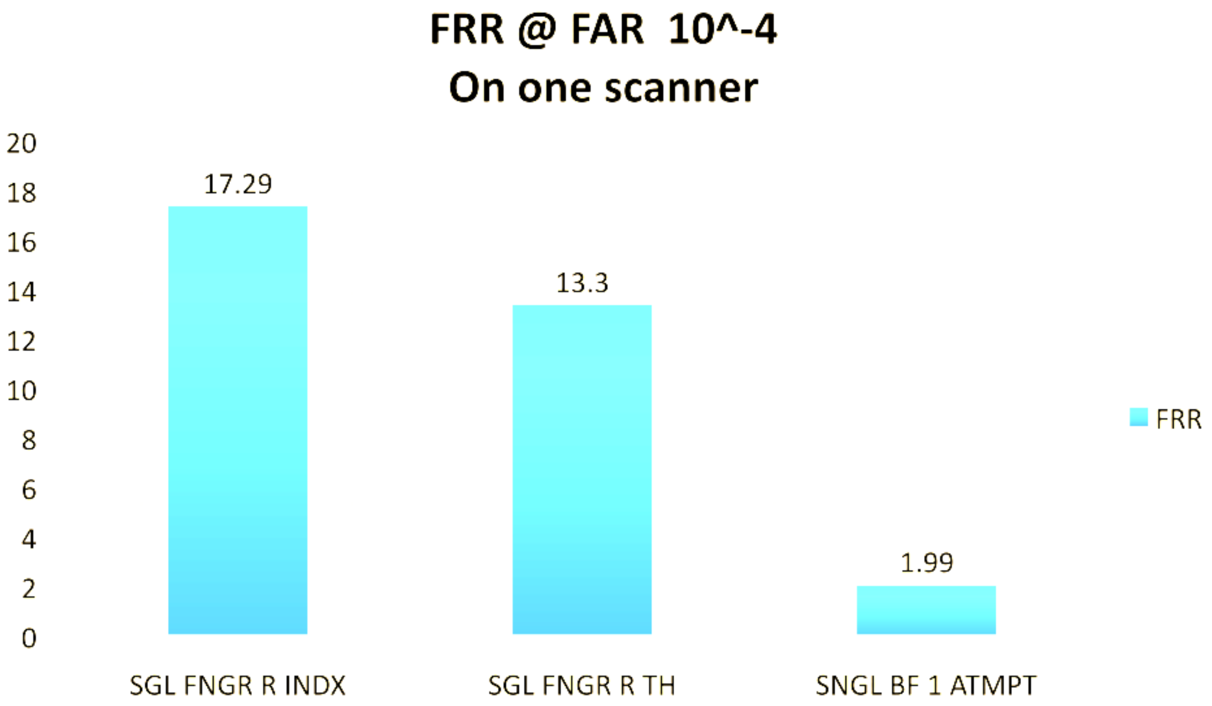


PERFORMANCE

- Enrollment (multi-modal biometric)
  - 36,000 enrollment stations, 87K certified operators
  - 11 models of certified devices
  - 200 Million enrolled
  - 400 Million planned for FY '13
  - 1M/day enrollment rate
  - *100 trillion person matches/day*
- Biometric Verification
  - 8 PoC
  - Two pilot programs underway

Source: Raj Mashruwala, "Scenario Testing of Mobile Fingerprint Verification System", NIST International Biometric Performance Conference 2012.

PERFORMANCE



Source: Raj Mashruwala, "Scenario Testing of Mobile Fingerprint Verification System", NIST International Biometric Performance Conference 2012.

FINGERPRINT

History

cquisition

Representations

Reduction

Comparison

Conclusion

HISTORY

Use of the fingerprint thumb for commercial exchanges (Babylon -3000 before JC)

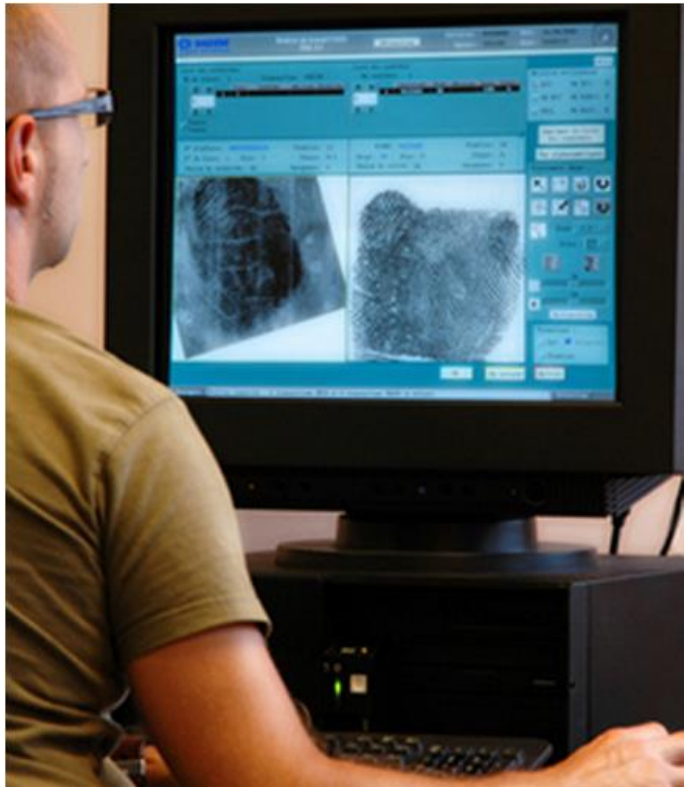
1902: first use of fingerprint to solve a crime

Alphonse Bertillon

HISTORY

1970-1980: first automatic fingerprint recognition systems

1982: starting to have a digital fingerprint database in France



ACQUISITION

- Off-line acquisition
  - Ink technique
  - Latent fingerprints

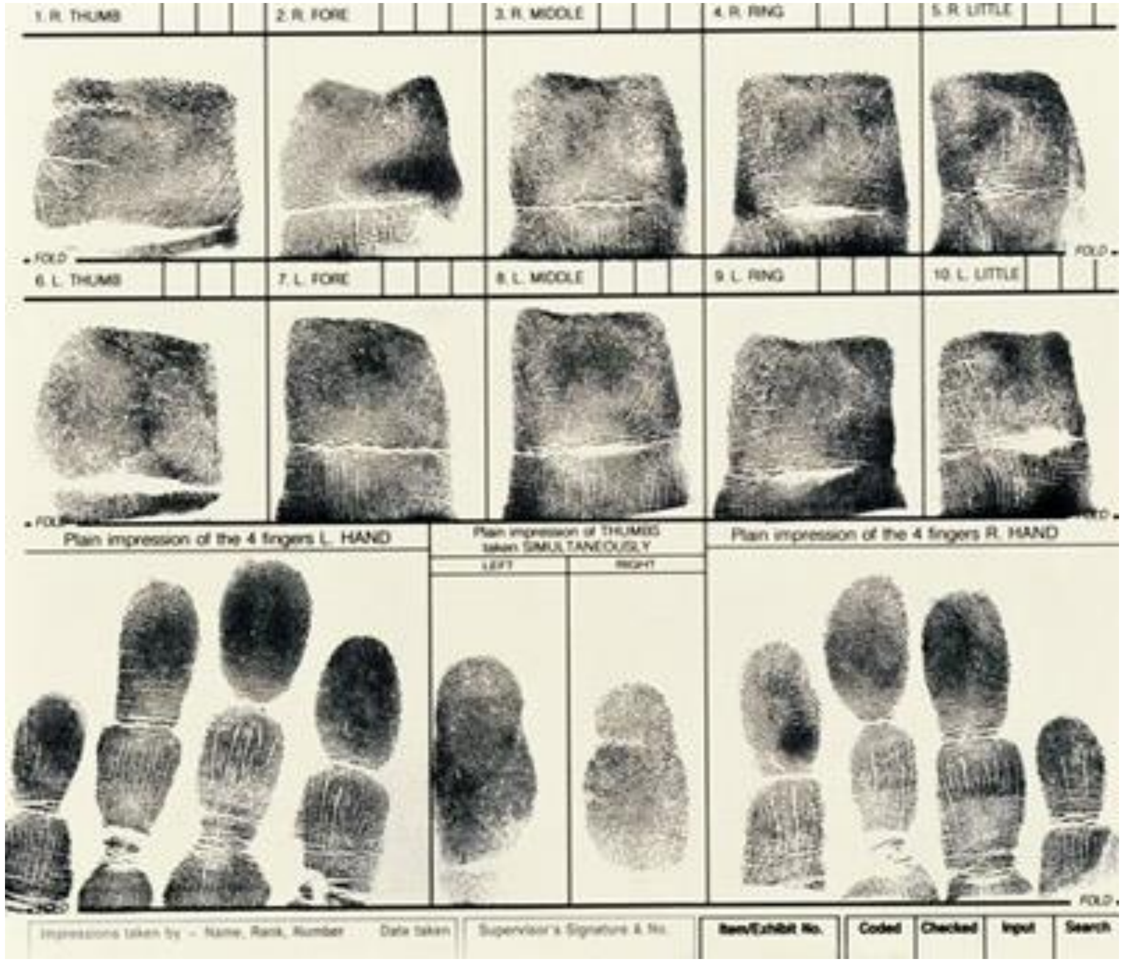
Latent fingerprint

On-line acquisition
- Optical sensors
- Silicon-based sensors
- ...

Plain fingerprint

ACQUISITION

Illustration

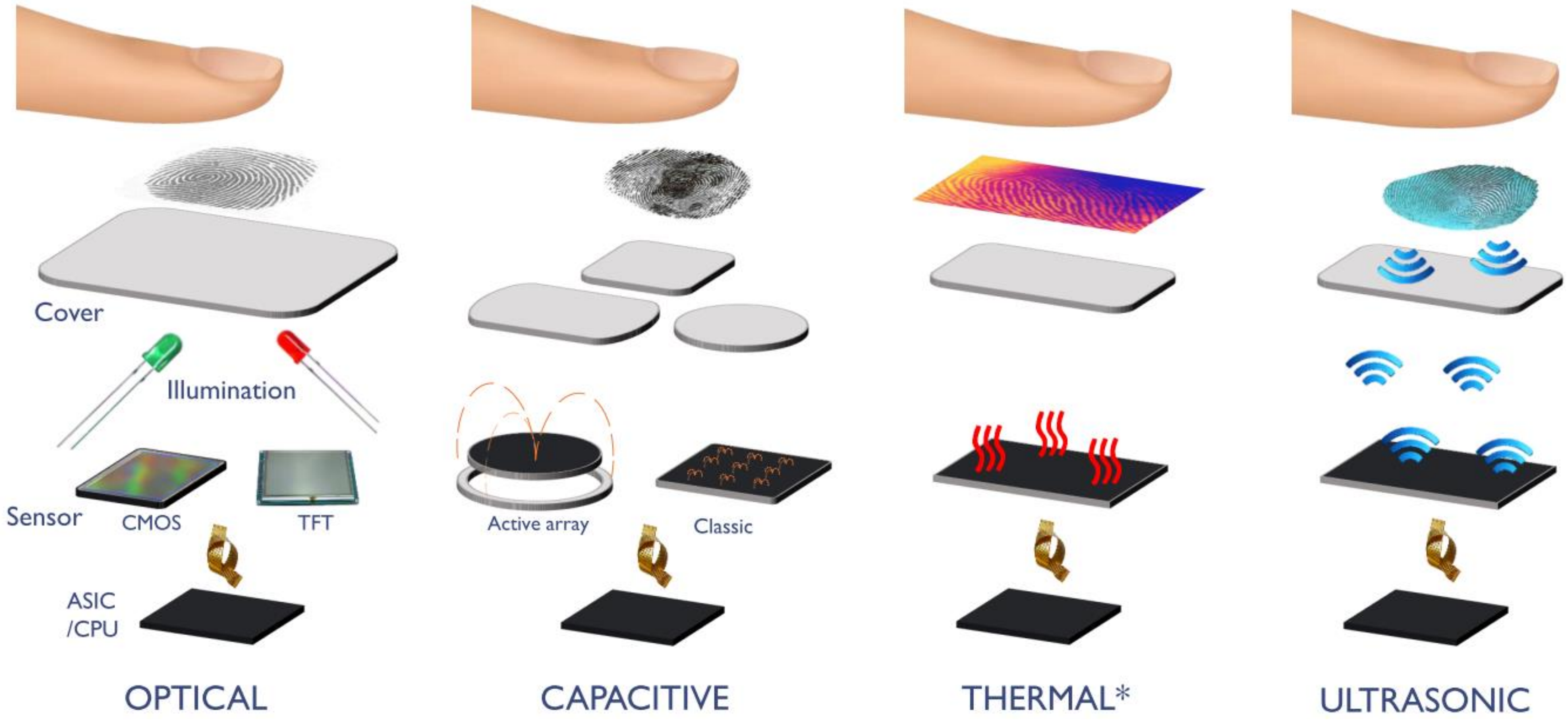


ACQUISITION

Sensors

Sensor technologies

- Capacitive
- Thermal
- Optical
- Ultrasonic



REPRESENTATION

Henry classification

Arch
~5%

Loops
~ 60%

1 spiral

2 spirals

~ 30%

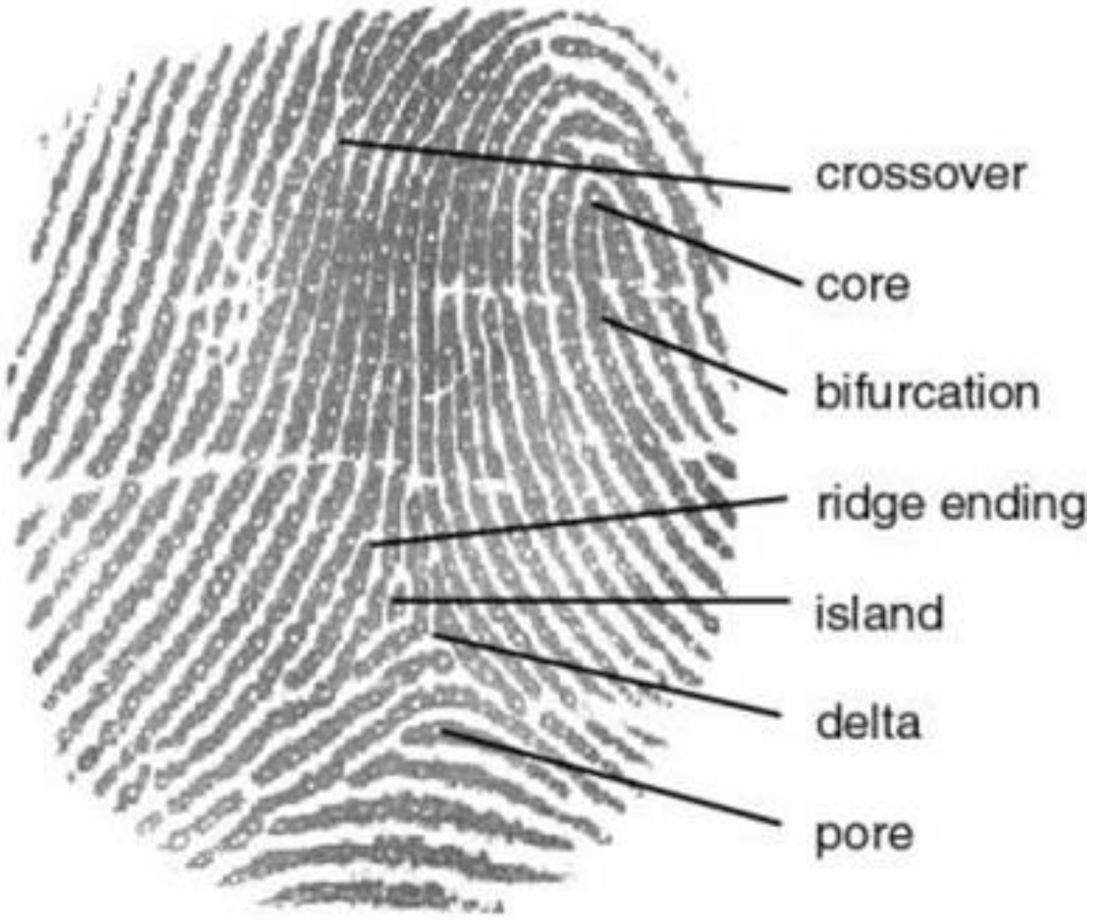
REPRESENTATION

Description

Level 1: ridges

Level 2: minutiae (crossover, delta, bifurcation, ridge ending, core)

Level 3: pores



REPRESENTATION

Minutiae extraction

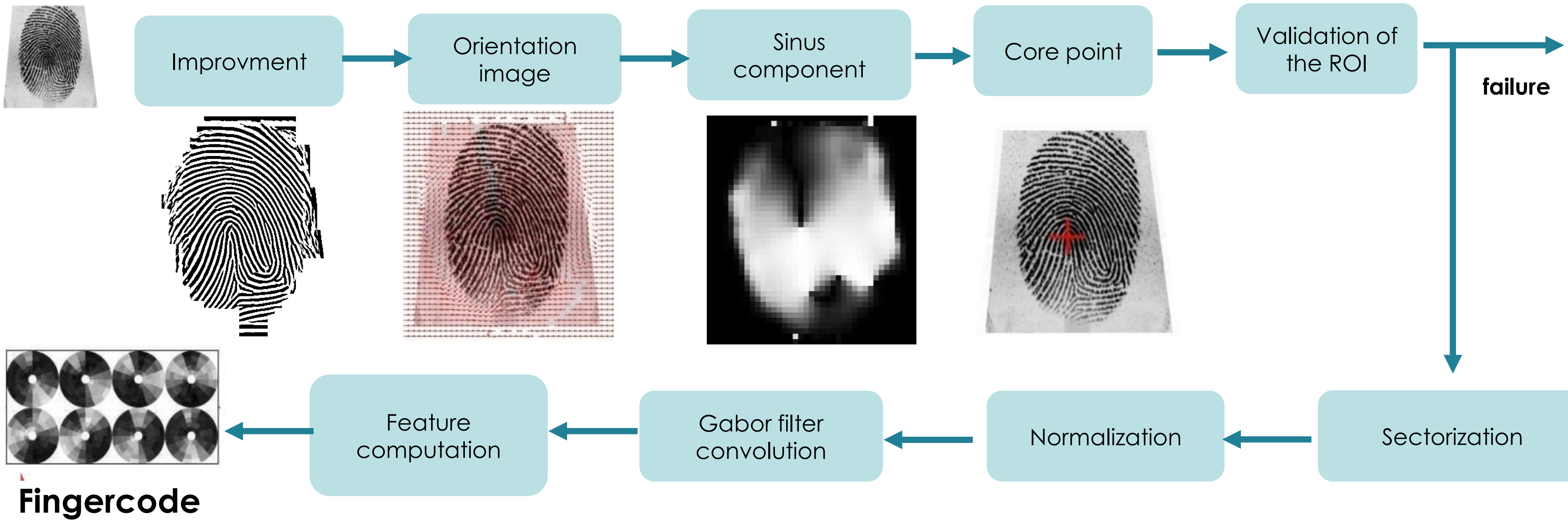
Orginal image

Binarised image

Minutiae extraction

REPRESENTATION

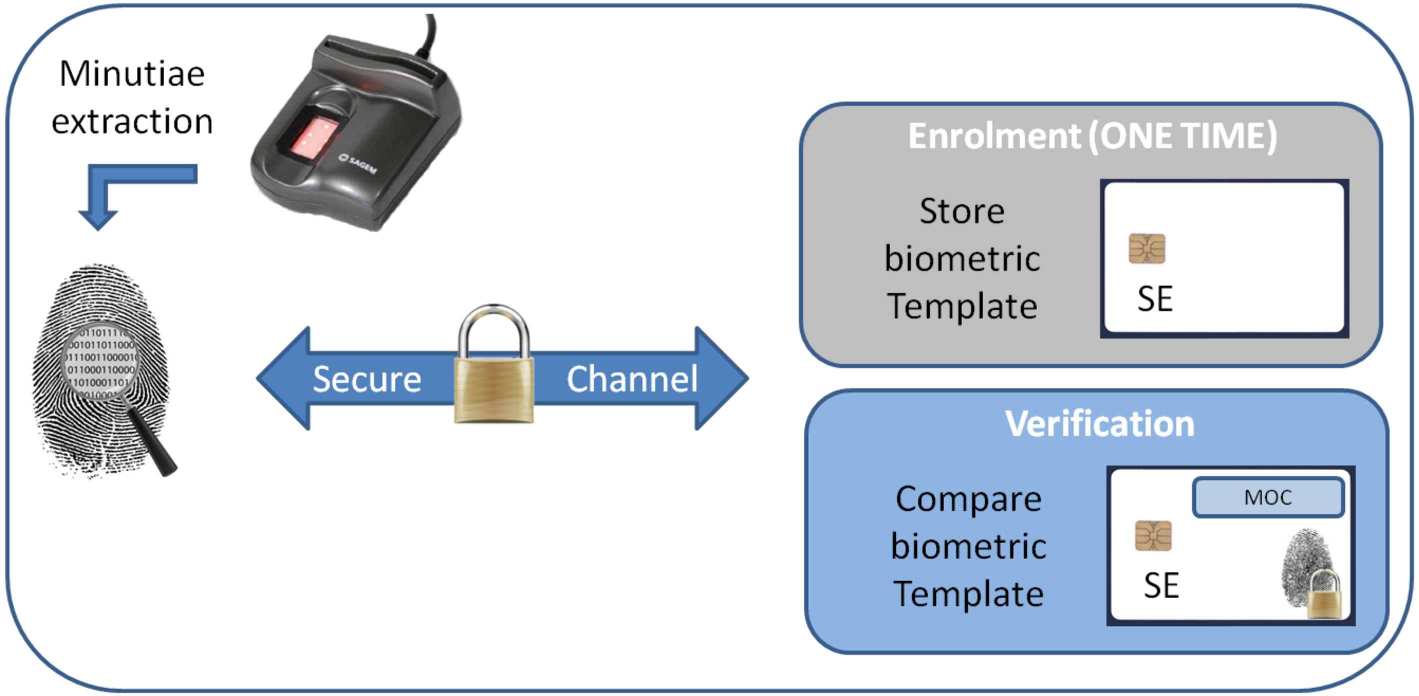
Texture: A fingerprint can be represented by texture features



REDUCTION

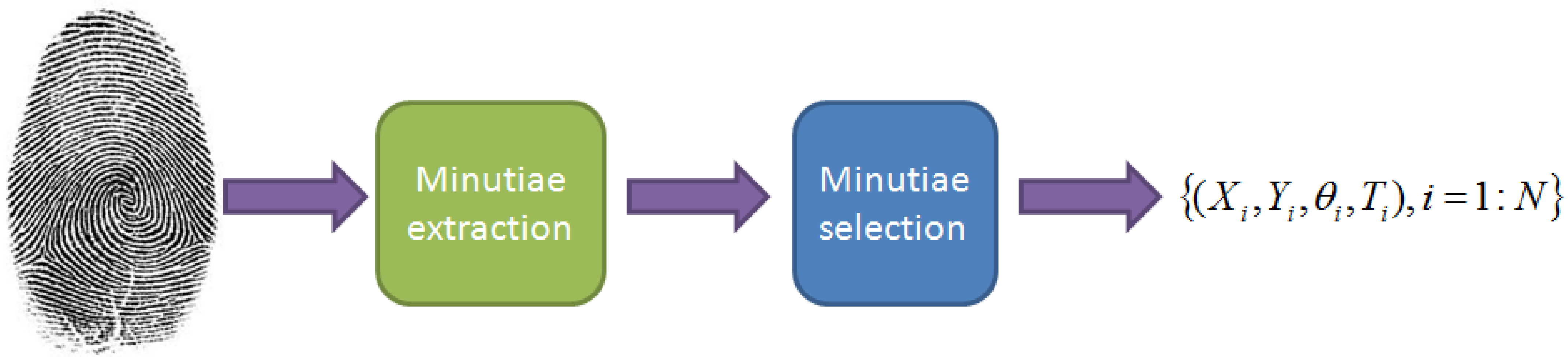
Secure element: used to store the reference template and for the on-card-comparison

Enrolment & Verification



REDUCTION

Secure element: necessary to select minutiae (memory and computation limitations)



Fingerprint
Image representation

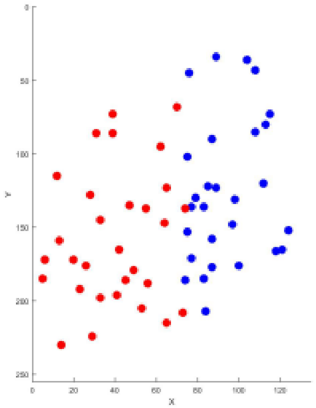
REDUCTION

Methods in the literature:

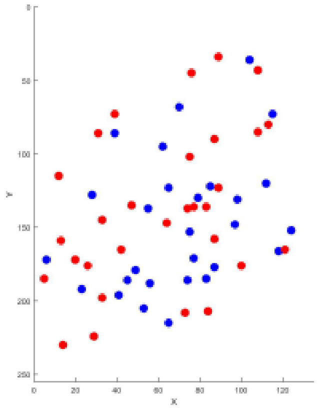
- Random selection,
- Truncation: keep only the first minutiae in the template (ISO/IEC 19794-2),
- Barycenter: keep only the minutiae closest to the CORE point (Grother and Salomon 2007),
- Evolutive barycenter: iterative version of the barycenter approach (Vibert et al. 2015),
- K-means: sub-sampling of minutiae (Vibert et al. 2015),
- Minutiae Reduction by Genetic Algorithm (MRGA) (Vibert et al. 2018).

REDUCTION

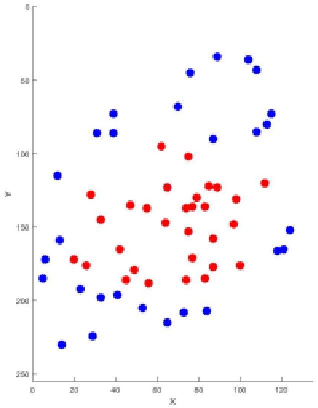
Illustrations:



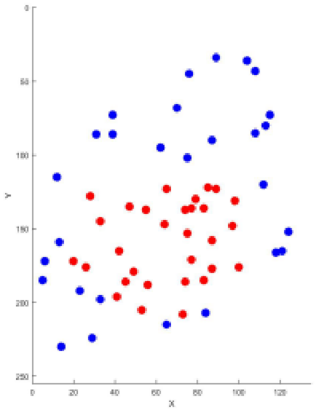
(a) Truncation



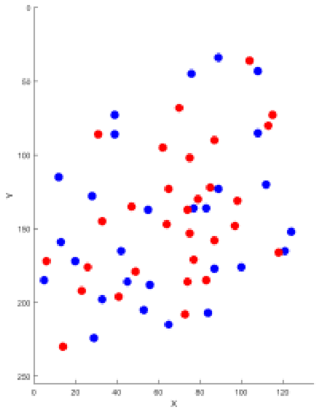
(b) Random



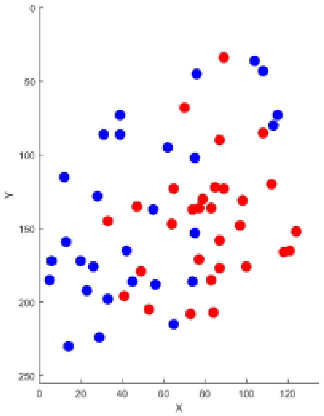
(c) Barycenter



(d) Evolutive



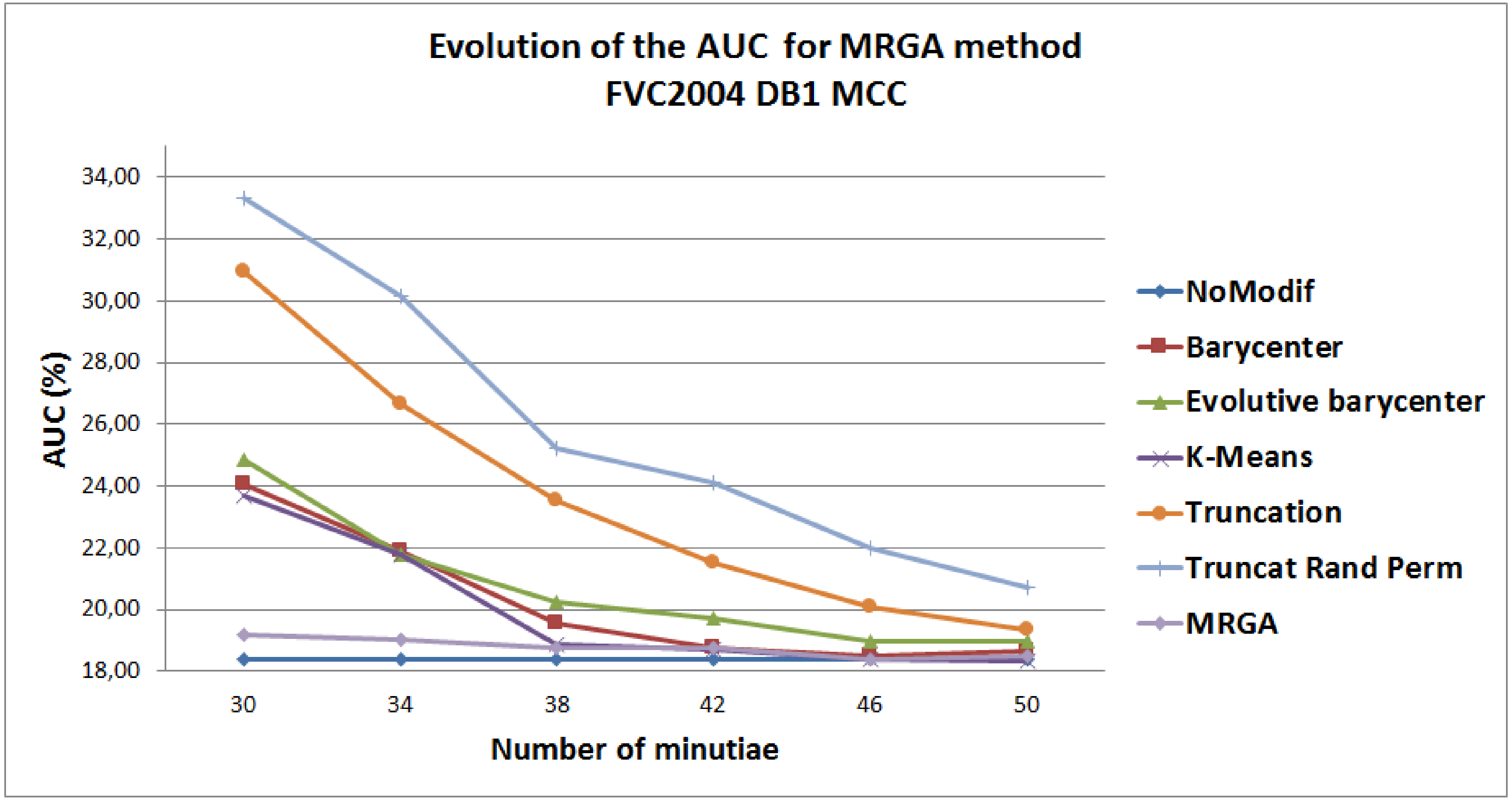
(e) K-Means



(f) MRGA

REDUCTION

Comparative study:

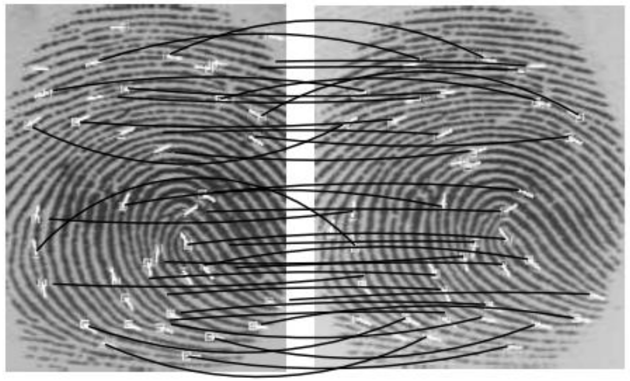


Vibert, C. Charrier, J.-M. Le Bars, C. Rosenberger, "Towards an Optimal Template Reduction for Securing Embedded Fingerprint Devices", International Conference on Information Systems Security and Privacy (ICISSP), 2018.

COMPARISON

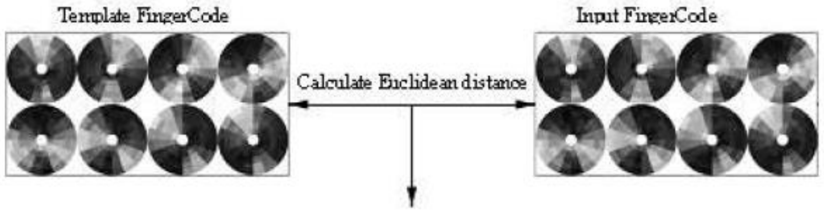
Algorithms

- 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*.



COMPARISON

Minutiae matching

COMPARISON

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

Minutiae matching: baseline algorithm

$$\mathbf{T} = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_m\} \quad \mathbf{m}_i = \{x_i, y_i, \theta_i\} \quad i = 1..m$$
$$\mathbf{I} = \{\mathbf{m}'_1, \mathbf{m}'_2, \ldots, \mathbf{m}'_n\} \quad \mathbf{m}'_j = \{x'_j, y'_j, \theta'_j\} \quad j = 1..n,$$

the two sets of minutiae corresponding to the Template and the Input

$$\underset{\Delta x, \Delta y, \theta, P}{\text{maximize}} \sum_{i=1}^{m} mm\left(map_{\Delta x, \Delta y, \theta}\left(\mathbf{m}'_{P(i)}\right), \mathbf{m}_i\right)$$

maximize the number of minutiae mates between template and "aligned" Input

$$mm\left(\mathbf{m}''_j, \mathbf{m}_i\right) = \begin{cases} 1 & sd\left(\mathbf{m}''_j, \mathbf{m}_i\right) \le r_0 \quad \text{and} \quad dd\left(\mathbf{m}''_j, \mathbf{m}_i\right) \le \theta_0 \\ 0 & \text{otherwise.} \end{cases}$$

$$dd\left(\mathbf{m}'_j, \mathbf{m}_i\right) = \min\left(\left|\theta'_j - \theta_i\right|, 360° - \left|\theta'_j - \theta_i\right|\right)$$
$$sd\left(\mathbf{m}'_j, \mathbf{m}_i\right) = \sqrt{\left(x'_j - x_i\right)^2 + \left(y'_j - y_i\right)^2}$$

the two minutiae can be paired

$P(i)$ is an unknown function that determines the pairing between **I** and **T** minutiae:

1. $P(i) = j$ indicates that the mate of the $\mathbf{m}_i$ in **T** is the minutia $\mathbf{m}'_j$ in **I**;
2. $P(i) =$ null indicates that minutia $\mathbf{m}_i$ in **T** has no mate in **I**;
3. a minutia $\mathbf{m}'_j$ in **I**, such that $\forall\ i = 1..m,\ P(i) \ne j$ has no mate in **T**;
4. $i = 1..m,\ k = 1..m,\ i \ne k \Rightarrow P(i) \ne P(k)$ or $P(i) = P(k) =$ null (each minutia in **I** is associated with a maximum of one minutia in **T**).

$$map_{\Delta x, \Delta y, \theta}\left(\mathbf{m}'_j = \{x'_j, y'_j, \theta'_j\}\right) = \mathbf{m}''_j = \{x''_j, y''_j, \theta'_j + \theta\}$$

$$\begin{bmatrix} x''_j \\ y''_j \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x'_j \\ y'_j \end{bmatrix} + \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix}$$

COMPARISON

Minutiae matching: baseline algorithm

The space of transformations consists of quadruples (Δx, Δy, θ, s), where each parameter is discretized (denoted by the symbol $^+$) into a finite set of values:

$$\Delta x^+ \in \{\Delta x_1^+, \Delta x_2^+, \ldots, \Delta x_a^+\} \quad \Delta y^+ \in \{\Delta y_1^+, \Delta y_2^+, \ldots, \Delta y_b^+\},$$
$$\theta^+ \in \{\theta_1^+, \theta_2^+, \ldots, \theta_c^+\} \quad s^+ \in \{s_1^+, s_2^+, \ldots, s_d^+\}.$$

At the end of the accumulation process, the best alignment transformation (Δx^*, Δy^*, θ^*, s^*) is then obtained as

$$(\Delta x^*, \Delta y^*, \theta^*, s^*) = arg \max_{\Delta x^+, \Delta y^+, \theta^+, s^+} \mathbf{A}[\Delta x^+, \Delta y^+, \theta^+, s^+]$$

Computational complexity: $O(m \times n \times c \times d)$

for each $\mathbf{m}_i$, $i = 1..m$
  for each $\mathbf{m}'_j$, $j = 1..n$
    for each $\theta^+ \in \{\theta_1^+, \theta_2^+, \ldots, \theta_c^+\}$
      if $dd(\theta'_j + \theta^+, \theta_i) < \theta_0$
        for each $s^+ \in \{s_1^+, s_2^+, \ldots, s_d^+\}$

$$\left\{ \begin{bmatrix} \Delta x \\ \Delta y \end{bmatrix} = \begin{bmatrix} x_i \\ y_i \end{bmatrix} - s^+ \cdot \begin{bmatrix} \cos\theta^+ & -\sin\theta^+ \\ \sin\theta^+ & \cos\theta^+ \end{bmatrix} \begin{bmatrix} x'_j \\ y'_j \end{bmatrix} \right.$$

Δx^+, Δy^+ = quantization of Δx, Δy to the nearest bin
$\mathbf{A}[\Delta x^+, \Delta y^+, \theta^+, s^+] = \mathbf{A}[\Delta x^+, \Delta y^+, \theta^+, s^+] + 1$
}

COMPARISON

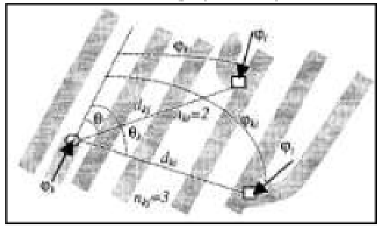
Minutiae matching: algorithms in the literature

Local minutiae matching *consists of comparing two fingerprints according to local minutiae structures.*

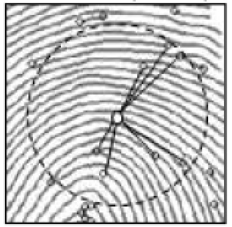
Local structures *are characterized by attributes that are invariant with respect to global transformations (e.g., translation, rotation, etc.) and therefore are suitable for matching without any a priori global alignment.*

Matching local minutiae structures *is usually* ***faster*** *and* ***more robust*** *to distortion, but* ***less distinctive****.*

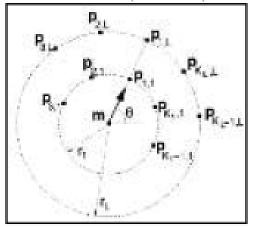
Jiang (2000)



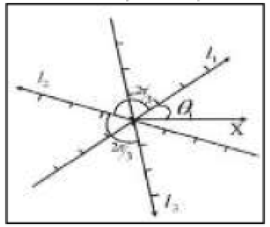
Ratha (2000)



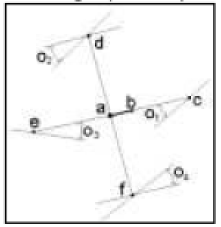
Tico (2003)



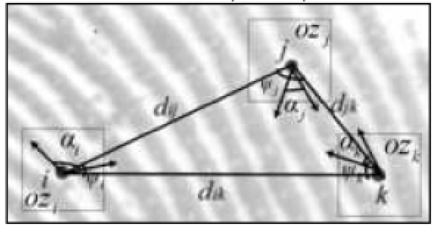
Qi (2004)



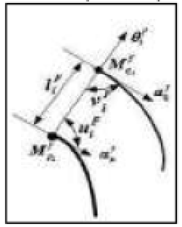
Ng (2004)



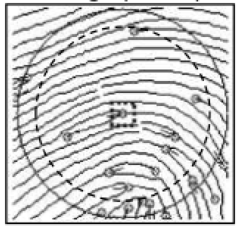
Chen (2005)



He (2006)



Feng (2008)



ILLUSTRATIONS

Minutiae matching: performance on datasets (FVC ONGOING platform)

Benchmark FMISO-STD-1.0:

Published on	Benchmark	Participant	Type	Algorithm	Version	EER ▲	FMR1000	FMR10000
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%
15/12/2010	FMISO-STD-1.0	Suprema, Inc.	Company	SFCore	1.0	0,258%	0,346%	0,639%
12/10/2009	FMISO-STD-1.0	Tiger IT Bangladesh	Company	Tiger ISO	0.1	0,317%	0,447%	0,866%
14/05/2011	FMISO-STD-1.0	Institute of Automation, Chinese Academy of Sciences	Academic Research Group	MntModel	1.0	0,380%	0,505%	0,819%
02/04/2010	FMISO-STD-1.0	id3 Semiconductors	Company	Fingerprint Matcher ISO	1.0	0,559%	0,783%	1,147%
22/07/2010	FMISO-STD-1.0	Biometric System Laboratory	Academic Research Group	MCC (Baseline)	1.1	0,570%	0,884%	1,331%
26/09/2009	FMISO-STD-1.0	APRO TECHNOLOGY (BANGKOK) CO., LTD.	Company	APF_FMISO	1.1	0,582%	0,801%	1,057%
20/07/2009	FMISO-STD-1.0	Neurotechnology	Company	MM_FMISO	3.0	0,598%	0,801%	1,234%
30/11/2010	FMISO-STD-1.0	Communik8 Ltd	Company	Authentik8	1.0	1,017%	2,475%	10,473%
15/09/2010	FMISO-STD-1.0	Robert Vanak	Independent Developer	SourceAFIS	1.3	1,334%	2,002%	2,900%

ILLUSTRATIONS

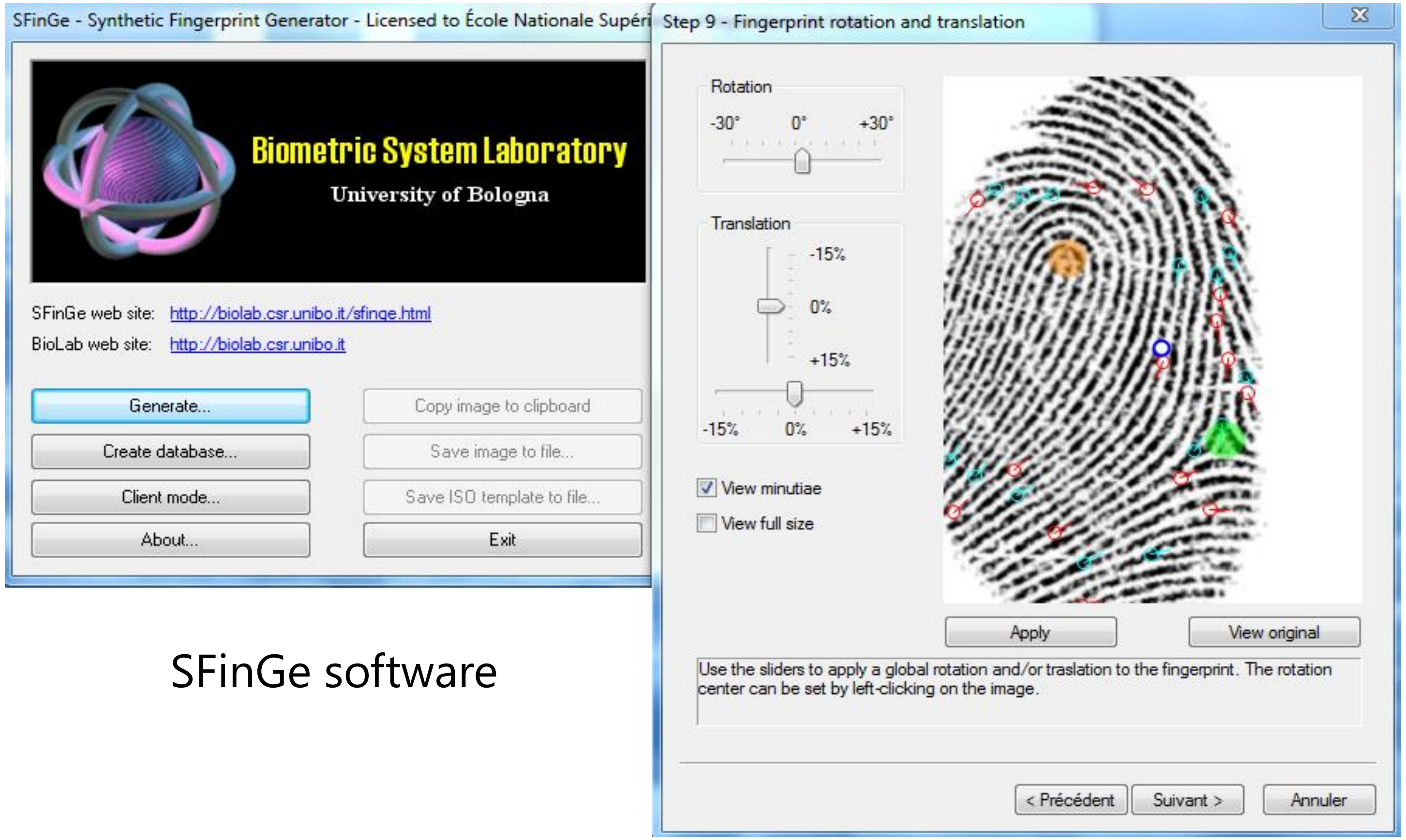
Minutiae matching: performance on datasets (FVC ONGOING platform)

Benchmark FMISO-HARD-1.0:

Published on	Benchmark	Participant	Type	Algorithm	Version	EER ▲	FMR1000	FMR10000
24/03/2011	FMISO-HARD-1.0	UnionCommunity	Company	Triple_M_ISO	1.2	1,103%	3,157%	7,878%
15/05/2011	FMISO-HARD-1.0	AA Technology Ltd.	Company	EMB9200	2.41	1,113%	2,076%	3,282%
15/12/2010	FMISO-HARD-1.0	Suprema, Inc.	Company	SFCore	1.0	1,407%	2,697%	4,570%
14/05/2011	FMISO-HARD-1.0	Institute of Automation, Chinese Academy of Sciences	Academic Research Group	MntModel	1.0	1,588%	2,821%	3,965%
22/07/2010	FMISO-HARD-1.0	Biometric System Laboratory	Academic Research Group	MCC (Baseline)	1.1	2,315%	4,876%	6,206%
09/03/2010	FMISO-HARD-1.0	id3 Semiconductors	Company	Fingerprint Matcher ISO	1.0	2,400%	4,260%	6,605%
20/07/2009	FMISO-HARD-1.0	Neurotechnology	Company	MM_FMISO	3.0	2,430%	4,607%	6,139%
26/09/2009	FMISO-HARD-1.0	APRO TECHNOLOGY (BANGKOK) CO., LTD.	Company	APF_FMISO	1.1	2,552%	4,581%	5,963%

ILLUSTRATIONS

Is it possible to generate a fingerprint given a minutiae set ?



SFinGe software

GREYC

FINGERPRINT QUALITY ASSESSMENT

Motivations

State of the art

Validation of FQA metrics

cnrs dépasser les frontières

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

UNICAEN

QUALITY

Reference template:

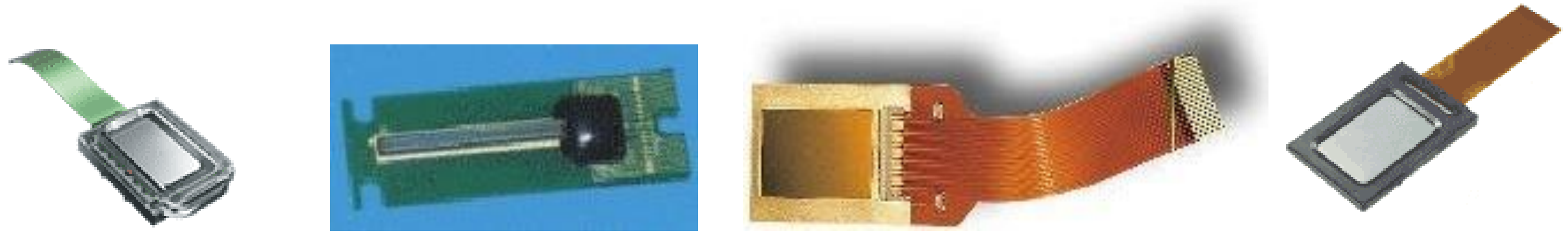
Need of the optimal quality of the reference template, problems can occur such as:

- Intrinsic low quality of the biometric sample
- Bad capture (positioning, pressure, blur...)
- Environmental conditions (humidity, frog, coldness...)

QUALITY

Benefits of evaluating the quality of biometric data

- Improving performance with a better enrollment
- New capture during verification if quality is insufficient
- Quality can be used as a soft biometric information
- Comparison of biometric sensors



Different types of fingerprint sensors

QUALITY

A first illustration on fingerprint recognition

Selection without quality checking

FAR = 0.41%

FRR = 17.36%

NFIQ template selection

FAR = 0.05%

FRR = 14.36%

QMF template selection

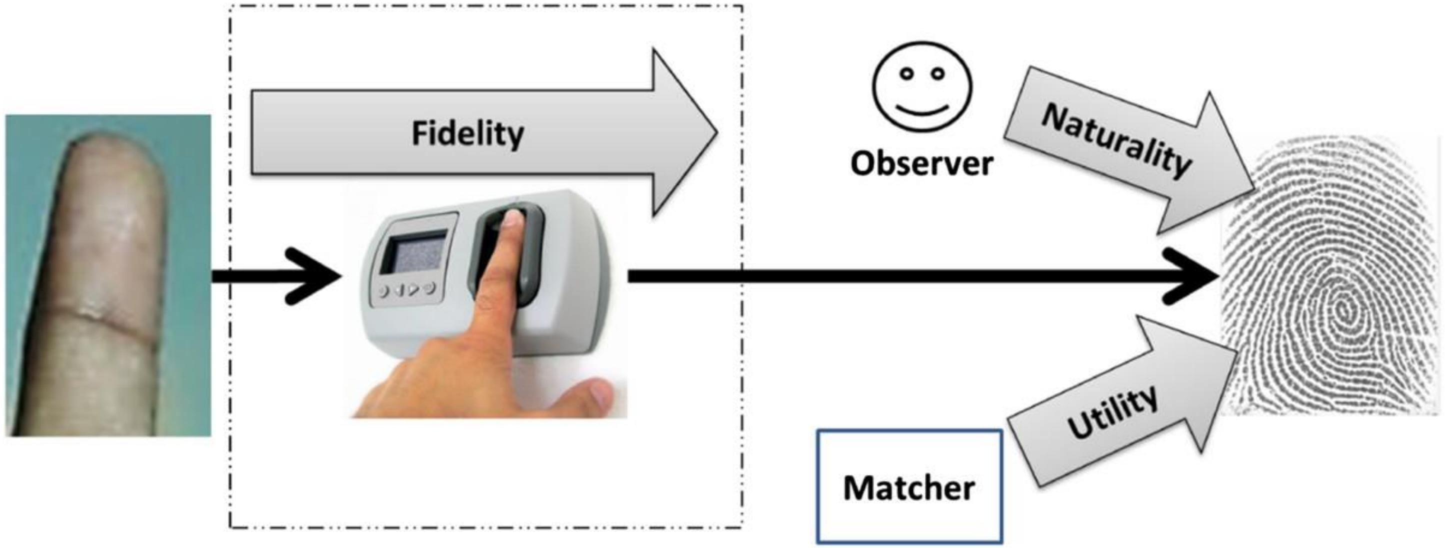
FAR = 0.003%

FRR = 4.75%

QUALITY

Aspects of quality assessment

- Naturality: Does it look like a fingerprint?
- Fidelity: How the sample represents the acquired fingerprint?
- Utility: Which performance can I expect with this sample?



Samarth Bharadwaj, Mayank Vatsa, Richa Singh, "Biometric quality: a review of fingerprint, iris, and face", EURASIP Journal on Image and Video Processing:34, 2014

QUALITY

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

Quality assessment of biometric data

Table 1

Different interpretations of quality in biometrics from literature

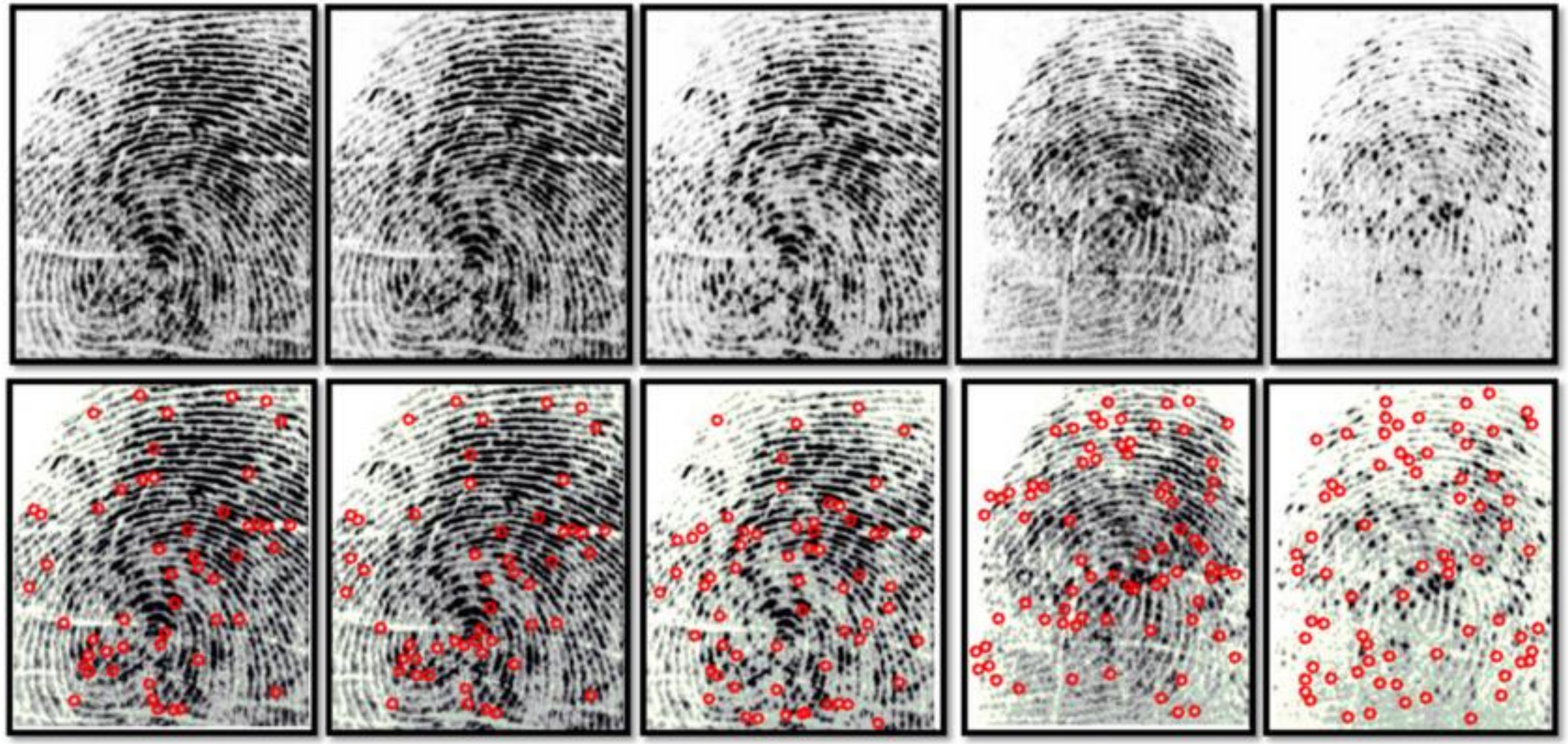
Reference	Modality	Interpretation of quality in biometrics
Chen et al.[3]	Fingerprint	A global measure of the strength of ridges
Grother and Tabassi[4]	Fingerprint	Suitability for automatic matching
Youmaran and Adler[5]	Face	The decrease in uncertainty of identity due to a given sample
Kryszczuk et al.[6]	Face	Conditionally relevant class predictors
Beveridge et al.[7]	Face	A measurable and actionable predictor of performance
ISO/IEC standards[13]	Face	Biometric data that adheres to best capture practices
Kalka et al.[8]	Iris	The measurement of various degradations known to affect iris recognition
Kumar and Zhang[9]	Knuckles	Confidence of generating reliable matching scores from the user templates
Poh and Kittler[10]	General framework	Degree of *extractability* of recognition features
BioAPI[14]	General framework	Biometric data that provides good performance for the intended purpose

Samarth Bharadwaj, Mayank Vatsa and Richa Singh, "Biometric quality: a review of fingerprint, iris, and face", EURASIP Journal on Image and Video Processing:34, DOI: 10.1186/1687-5281-2014-34, Springer, 2014.

QUALITY

Fingerprint Quality Assessment (FQA)

Poor quality fingerprint images lead to spurious minutiae



QUALITY

Fingerprint Quality Assessment (FQA)

- Lim et al. 2002: OCL metric weighted combination of local and global quality scores,
- Tabassi et al. 2005: **NFIQ** metric with Amplitude, frequency, and variance of sinusoid to model valid ridges,
- Ko 2007: NBIS metric considering minutiae quality,
- Vatsa et al. 2008: Combined response from RDWT for dominant edge information,
- El Abed et al. 2013: QMF metric based on texture features, no-reference image quality,
- Yao et al. 2015: MSEG metric based on gradient uniformity,
- Yao et al. 2015: QMF metric computed on minutiae templates,
- Tabassi 2015: **NFIQ 2.0** metric as a combination of various features.

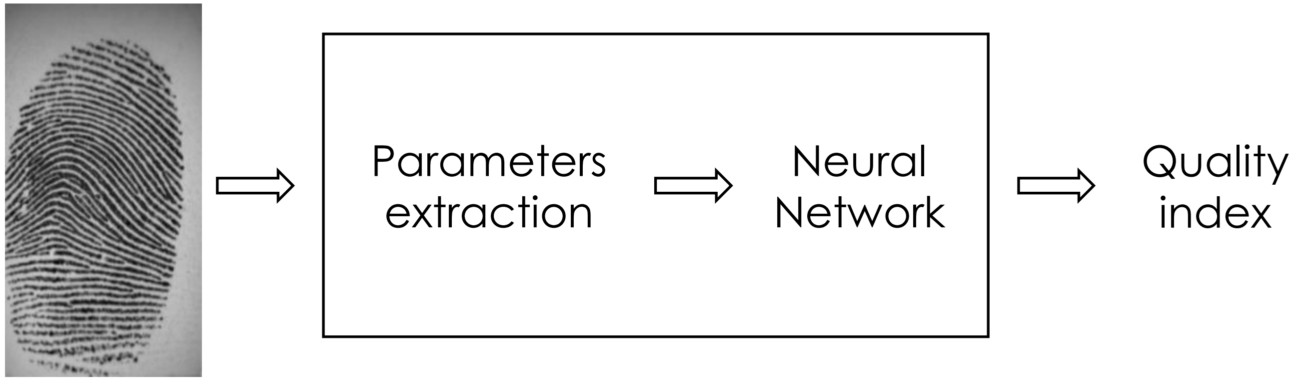
QUALITY

NFIQ 1.0 metric:

Quality metric for fingerprints

Returns a value between 1 and 5

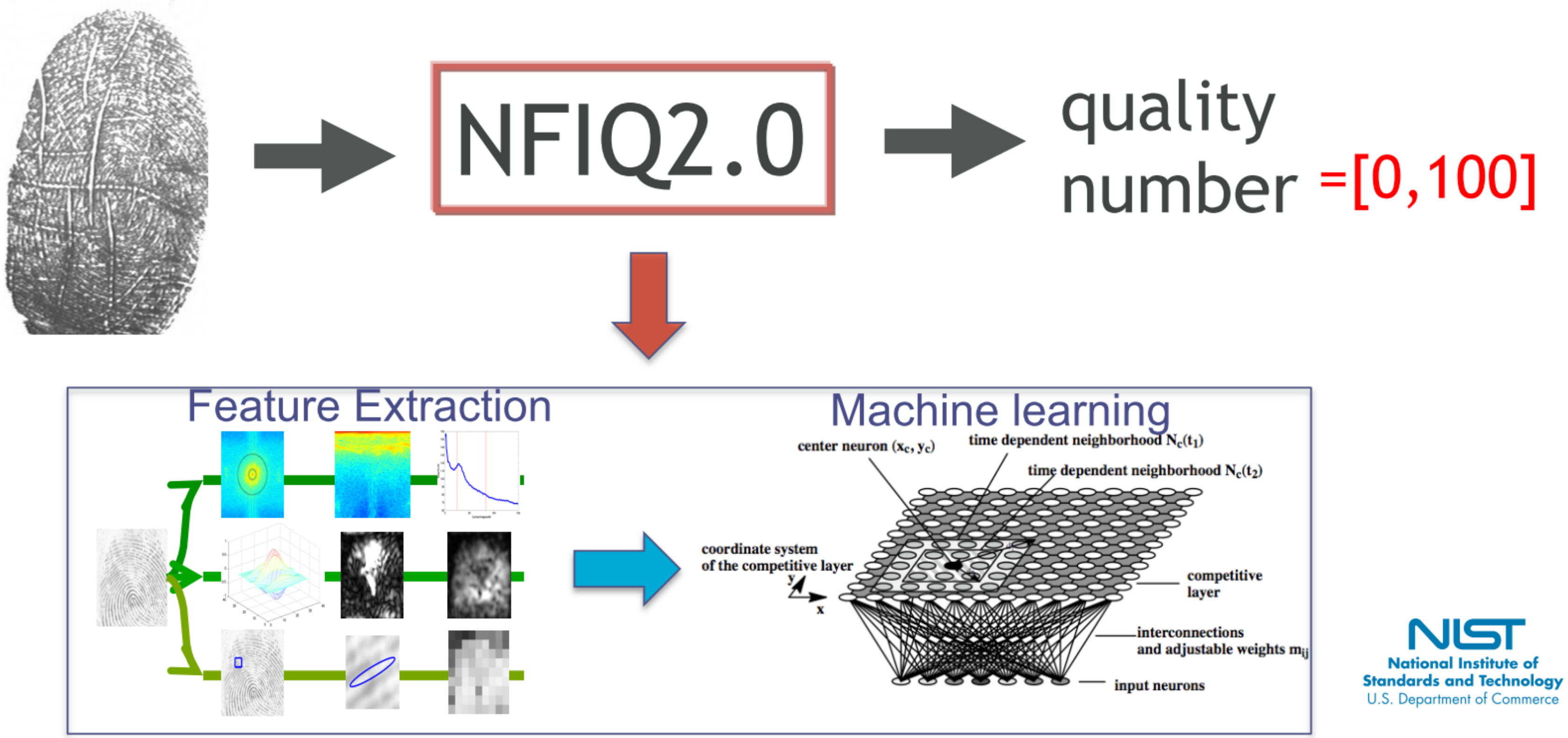
- 1 means a good quality fingerprint
- 5 means a poor quality fingerprint



E. Tabassi and C.L. Wilson. A novel approach to fingerprint image quality. *International Conference on Image Processing (ICIP)*, p. 37-40, 2005.

QUALITY

NFIQ 2.0 metric:



E. Tabassi et al., "The push towards zero error biometrics", NIST International conference of Biometric Performance, 2016

QUALITY

NFIQ 1.0

- 5 levels.
  - 1(highest) to 5(lowest)
- 11 features
- Comparison scores of 3 algorithms used for training
- 3400 training images
- Neural network
- ~300 msec per image

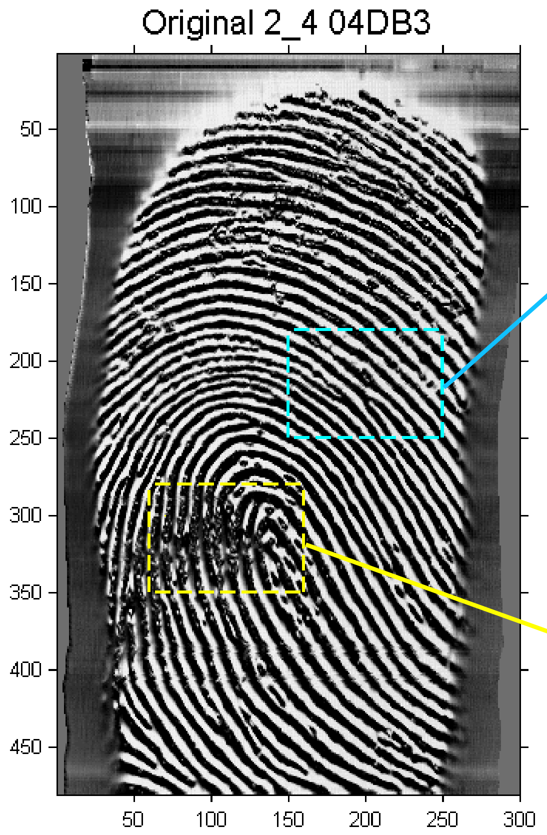
NFIQ 2.0

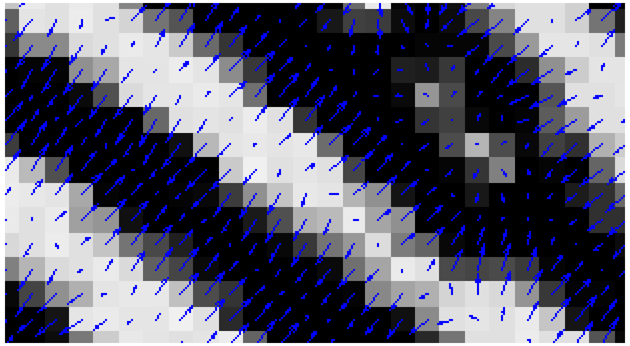
- 100 levels
  - 0(lowest) to 100(highest)
- 14 (69) features
- Comparison scores of 7 algorithms used for training
- ~5000 training images
- Random forest
- ~ 120 msec per image
- Actionable quality
  - Flags for blank image, low contrast
- Design for NFIQ Mobile

E. Tabassi et al., "The push towards zero error biometrics", NIST International conference of Biometric Performance, 2016

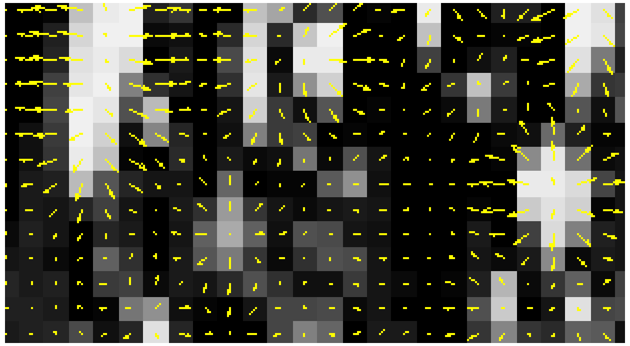
QUALITY

GREYC MSEG metric:





Gradients descent against ridge.

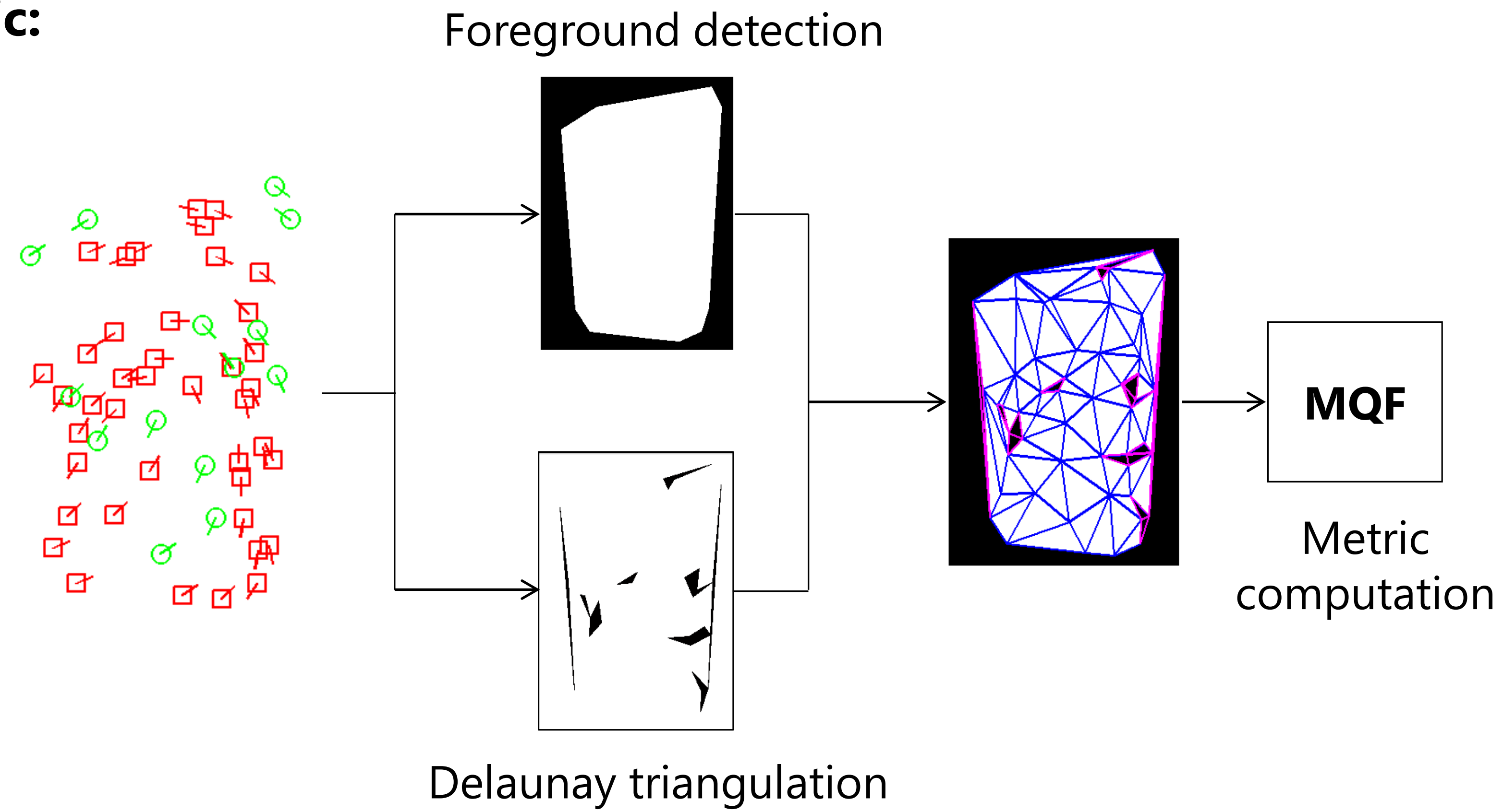


no uniform gradients

Z. Yao, J-M Le Bars, C. Charrier, C. Rosenberger. Fingerprint Quality Assessment With Multiple Segmentation. In 2015 International Conference on Cyberworlds (CW) IEEE. Scotland, Sweden. Oct. 7, 2015.

QUALITY

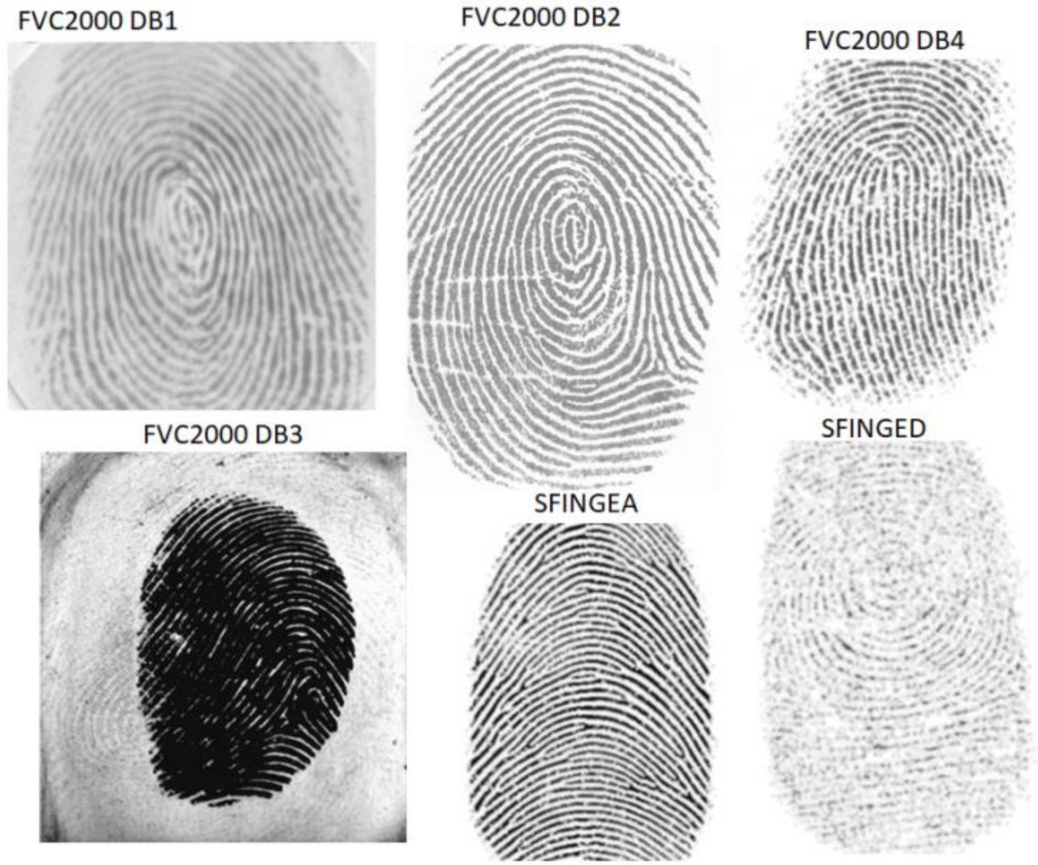
GREYC MQF metric:



Z. Yao, J.-M. LeBars, C. Charrier, and C. Rosenberger. Quality assessment of fingerprints with minutiae delaunay triangulation. In ICISSP - 1st International Conference on Information Systems Security and Privacy. INSTICC, Feb. 2015.

QUALITY

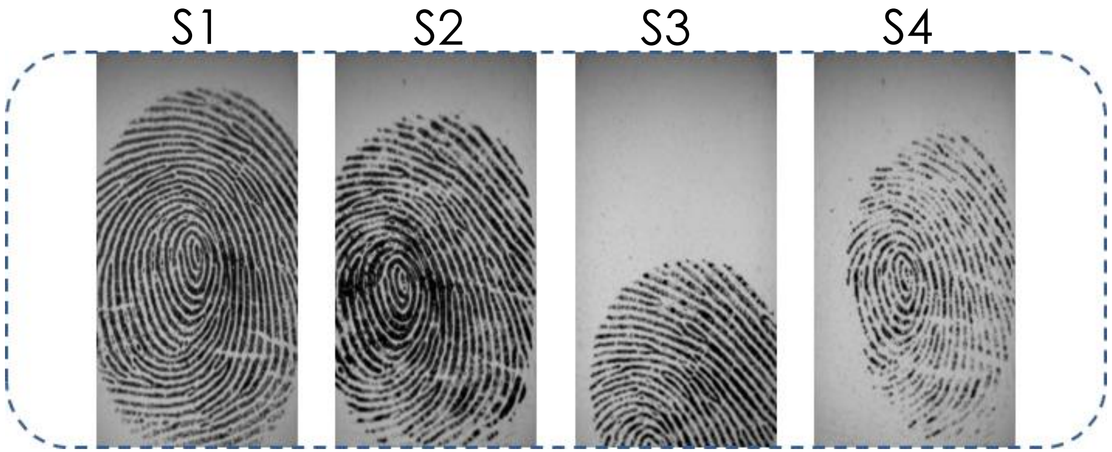
Comparison of quality metrics: an illustration



Dataset	NFIQ	NFIQ2	OCL	QMF	NBIS	MSEG	MQF
FVC2000DB1	2	65	0.73	83.81	14.16	0.44	59802
FVC2000DB3	4	40	0.71	28.06	15.11	0.18	29804
SFINGEA	1	69	0.90	76.09	57.46	0.83	55720
SFINGED	3	28	0.47	91.19	10	0.006	43546

QUALITY

Which metric is the most reliable?



Sample	S1	S2	S3	S4
Metric 1	66	63	41	40
Metric 2	1	2	2	2

How to validate a metric ?

QUALITY

Which properties for a validation framework ?

- **Generality:** can be used for any biometric modality;
- **Biometric test:** overall error rate to be considered;
- **Reliability:** computation of statistical measures;
- **Usability**: should be objective, reliable and reproducible.

QUALITY

Related works

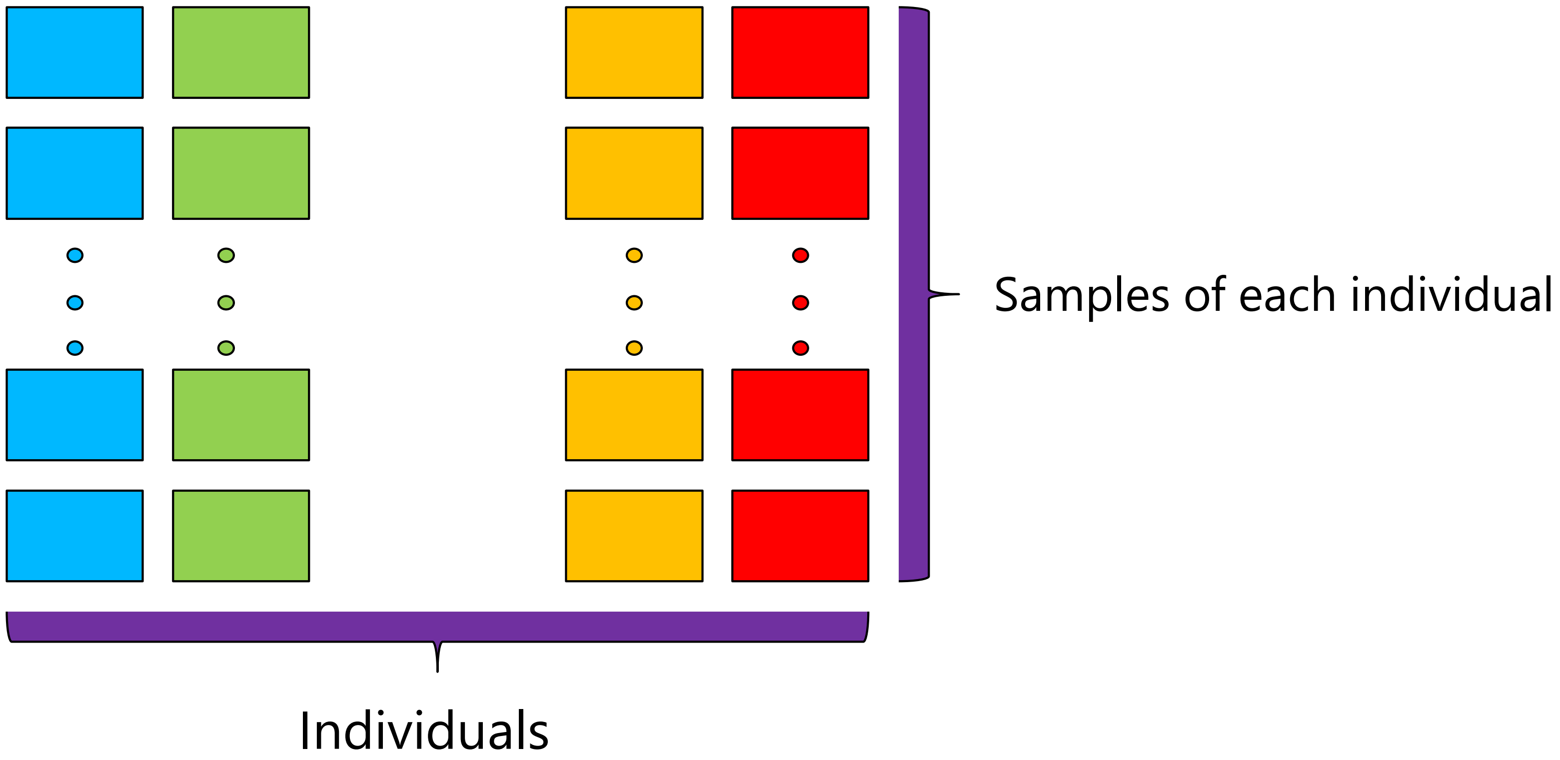
- Fitting of a reference or subjective results (Bolle 1999)
  Problem: Not completely reliable, objective and not repeatable.

- Genuine matching error (Grother 2007)
  Shortage: only genuine matching is considered.

- Overall error rate based on sorting samples (Chen 2005)
  Shortage: it is complex to deal with the matching scores of samples.

QUALITY

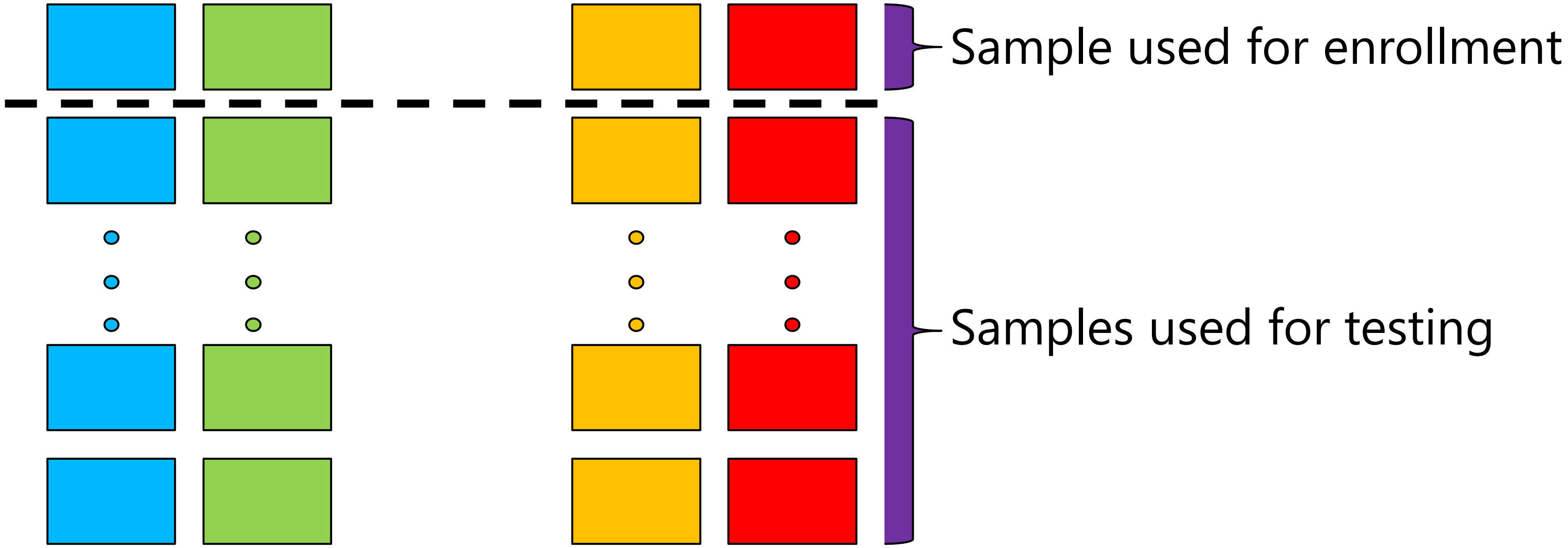
Enrollment selection approach (1/3)



Z. Yao, C. Charrier, C. Rosenberger, "Utility validation of a new fingerprint quality metric". In International Biometric Performance Testing Conference (IBPC), Gaithersburg, USA, Apr. 2014.

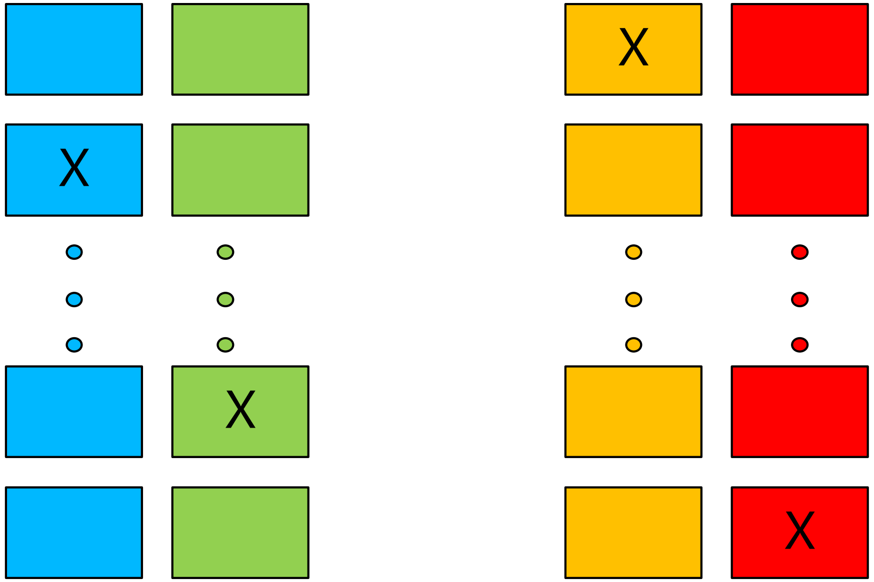
QUALITY

Enrollment selection approach (2/3)



Enrollment without quality checking

Enrollment selection approach (3/3)



X Sample used for enrollment

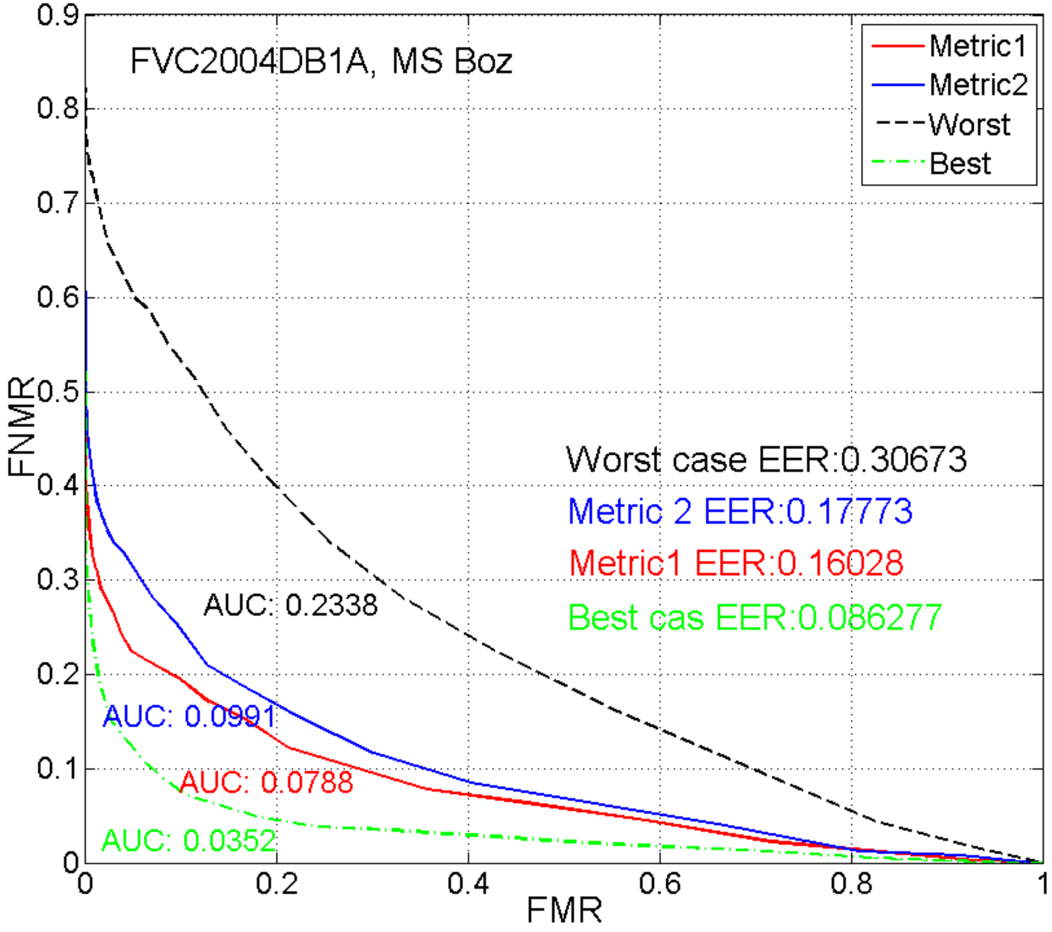
Other samples used for testing

Enrollment with quality checking
Best: choosing the sample minimizing errors
Worst: choosing the sample maximizing errors
Quality metric: choice driven by quality value

Comparison of quality metrics

Performance of quality metric:

$$P = 1 - \frac{(AUC_{metric} - AUC_{best})}{(AUC_{worst} - AUC_{best})}$$



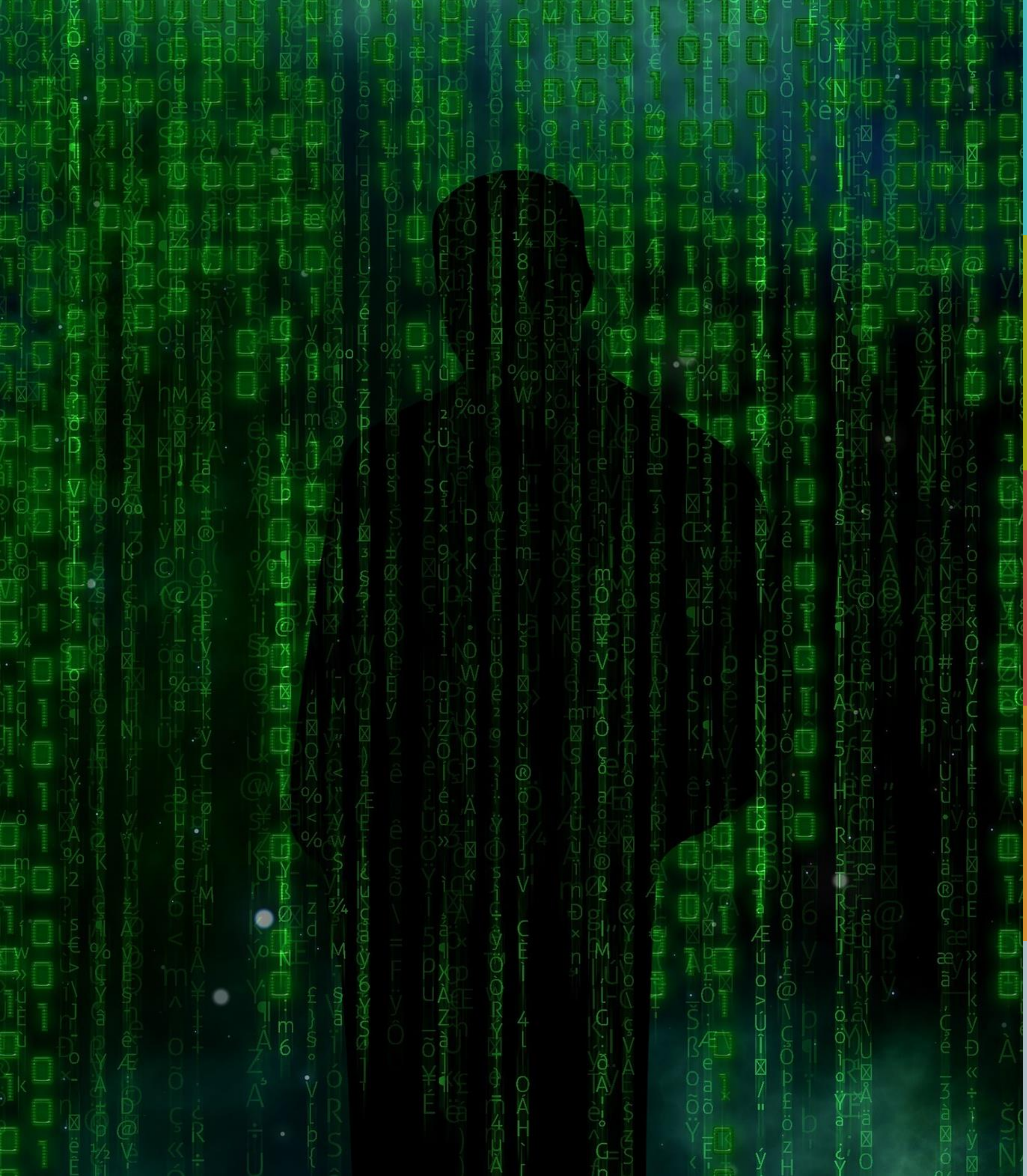
A graphical illustration

QUALITY

Comparison of quality metrics: reliability for different datasets (values of P)

Dataset	NFIQ	NFIQ2	OCL	QMF	NBIS	MSEG	MQF	EER
FVC2000DB1	71.7%	70.4%	**79.4%**	72.8%	73.7%	76.5%	71.5%	2.1%
FVC2000DB2	74.8%	**82.9%**	63.3%	69.4%	80.0%	79.5%	68.9%	1.9%
FVC2000DB3	74.5%	**82.8%**	72.1 %	61.3%	78.6%	71.4%	77.0%	11.7%
FVC2000DB4	63.7%	69.1%	68.8%	61.5%	56.4%	**69.3%**	69.0%	8.1%
SFINGE0	64.0%	**80.0%**	66.8%	68.0%	66.1%	74.7%	77.0%	10.9%
SFINGEA	81.1%	14.5%	67.4%	63.1%	78.1%	24.0%	**89.4%**	0.4%
SFINGEB	**90.9%**	57.7%	64.6%	44.8%	63.4%	55.1%	80.3%	0.5%
SFINGEC	87.1%	92.7%	95.7%	**100%**	76.3%	92.2%	87.7%	0.8%
SFINGED	70.3%	75.3%	**90.8%**	71.4%	71.3%	61.2%	70.8%	11%
MEAN FVC2000	71.2%	**76.3%**	70.9%	66.2%	72.2%	74.2%	71.6%	-
MEAN TOTAL	75.3%	69.7%	74.3%	68.0%	71.5%	67.1%	**76.8%**	-

Z. Yao, J.M. Le Bars, C. Charrier, C. Rosenberger, "Comparative study of digital fingerprint quality assessment metrics". In International Conference on Biometrics (ICB), Australia, February 2018.



PROTECTION OF FINGERPRINT

Motivations

State of the art

Validation of FQA metrics

SECURITY

Why is it necessary ?

- ❑ Personal data
- ❑ Difficult to revoke a biometric data
- ❑ Can be captured without any consent
- ❑ Its encryption is not sufficient

ATTACKS

HOME » FEATURED ARTICLES » Hackers Have Stolen Almost Six Million US Government...

Hackers Have Stolen Almost Six Million US Government Fingerprints

GRAHAM CLULEY
SEP 24, 2015 | IT SECURITY AND DATA PROTECTION

78 195 129 33

The Office of Personnel Management (OPM) has revealed in a statement that when hackers breached its systems earlier this year they made away with approximately 5.6 million fingerprints – a significant increase from the 1.1 million previously reported.

As is now well known, in addition to fingerprint data being stolen the Social Security numbers, addresses, employment history, and financial records of some 21.5 million current and former US government employees was also stolen.

The good news is that they believe the opportunities for criminals to exploit the fingerprint data is currently limited.

But the bad news is that chances are that won't continue to be the case.

FAA Managers Association > Aviation News > OPM says 5.6 million fingerprints stolen in cyberattack, five tim as many as previously thought

OPM says 5.6 million fingerprints stolen in cyberattack, five times as many as previously thought

Posted on September 23, 2015

By Andrea Peterson

One of the scariest parts of the massive cybersecurity breaches at the Office of Personnel Management just got worse: The agency now says 5.6 million people's fingerprints were stolen as part of the hacks.

That's more than five times the 1.1 million government officials estimated when the cyberattacks were initially disclosed over the summer. The total number of those believed to be caught up in the breaches, which included the theft of the Social Security numbers and addresses of more than 21 million former and current government employees, remains the same.

OPM and the Department of Defense were reviewing the theft of background investigation records when they identified additional fingerprint data that had been exposed, OPM said in a statement.

Read More...

ATTACKS


Login Register Subscribe Rewards Video

The Telegraph HOME NEWS

Technology

News | Reviews | Opinion | Internet security | Social media | Apple | Google

Technology

Peace sign selfies could let hackers copy your fingerprints

share

5 Comments

Savvy fraudsters could recreate fingerprints from photos CREDIT: REX

ATTACKS

Attacks on a biometric system: spoofing a fingerprint

LivDet-Finger 2017

Fingerprint Systems Liveness Detection Competition 2017

http://fingerprint2017.livdet.org/

PET TECHNOLOGIES

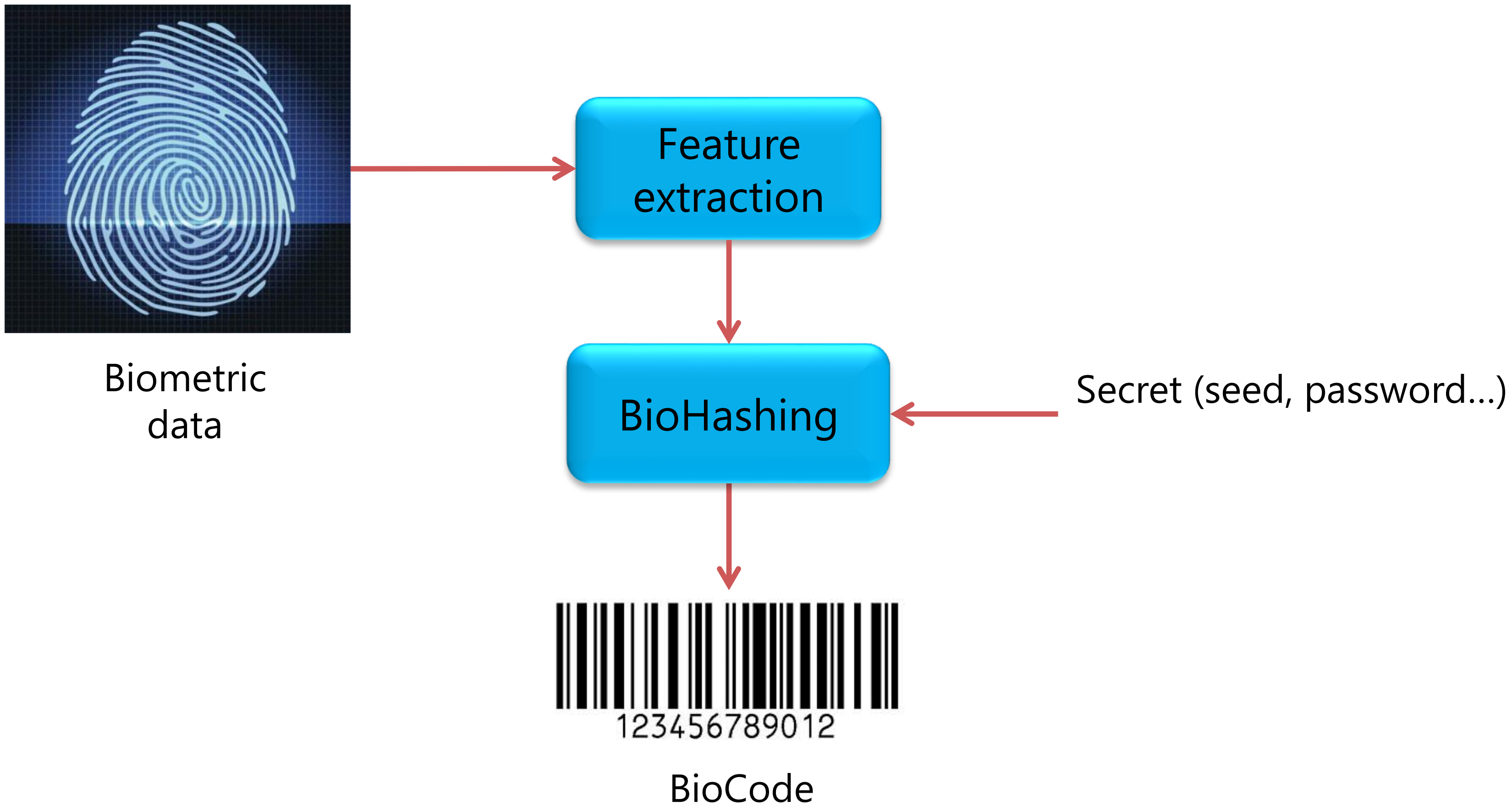
PET (Privacy Enabling Technologies) schemes:

- ✓ Secure computing: matching in the encrypted domain
  [Bringer et al. 2012], [Chabanne et al. 2013]

- ✓ Crypto-biometrics: Fuzzy vault, Secure Sketches
  [Rathgeb and Uhl 2011]

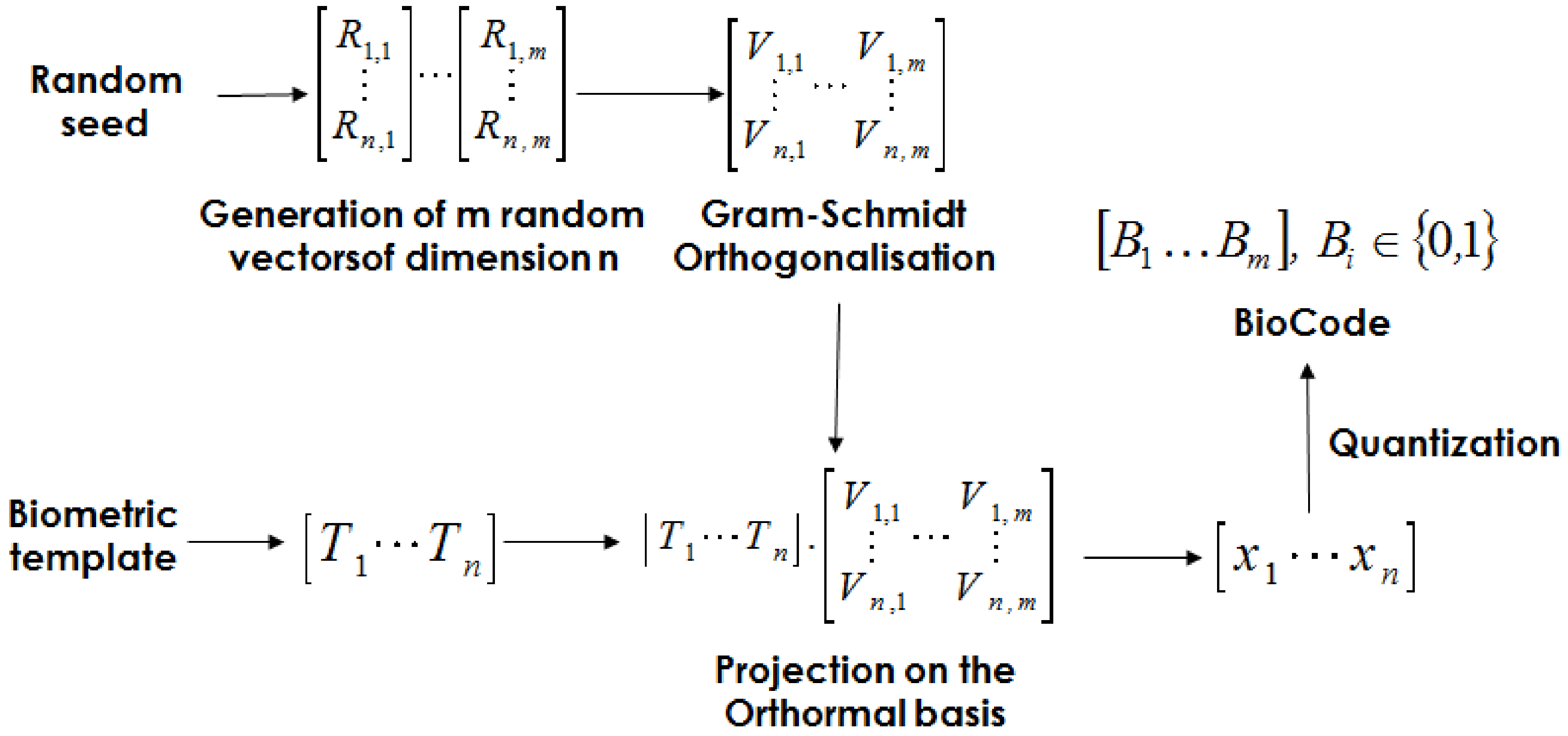
- ✓ Transformation: BioHashing
  [Teoh et al. 2004]

BIOHASHING



Jin, Andrew Teoh Beng, David Ngo Chek Ling, and Alwyn Goh. "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." *Pattern recognition* 37.11 (2004): 2245-2255.

BIOHASHING



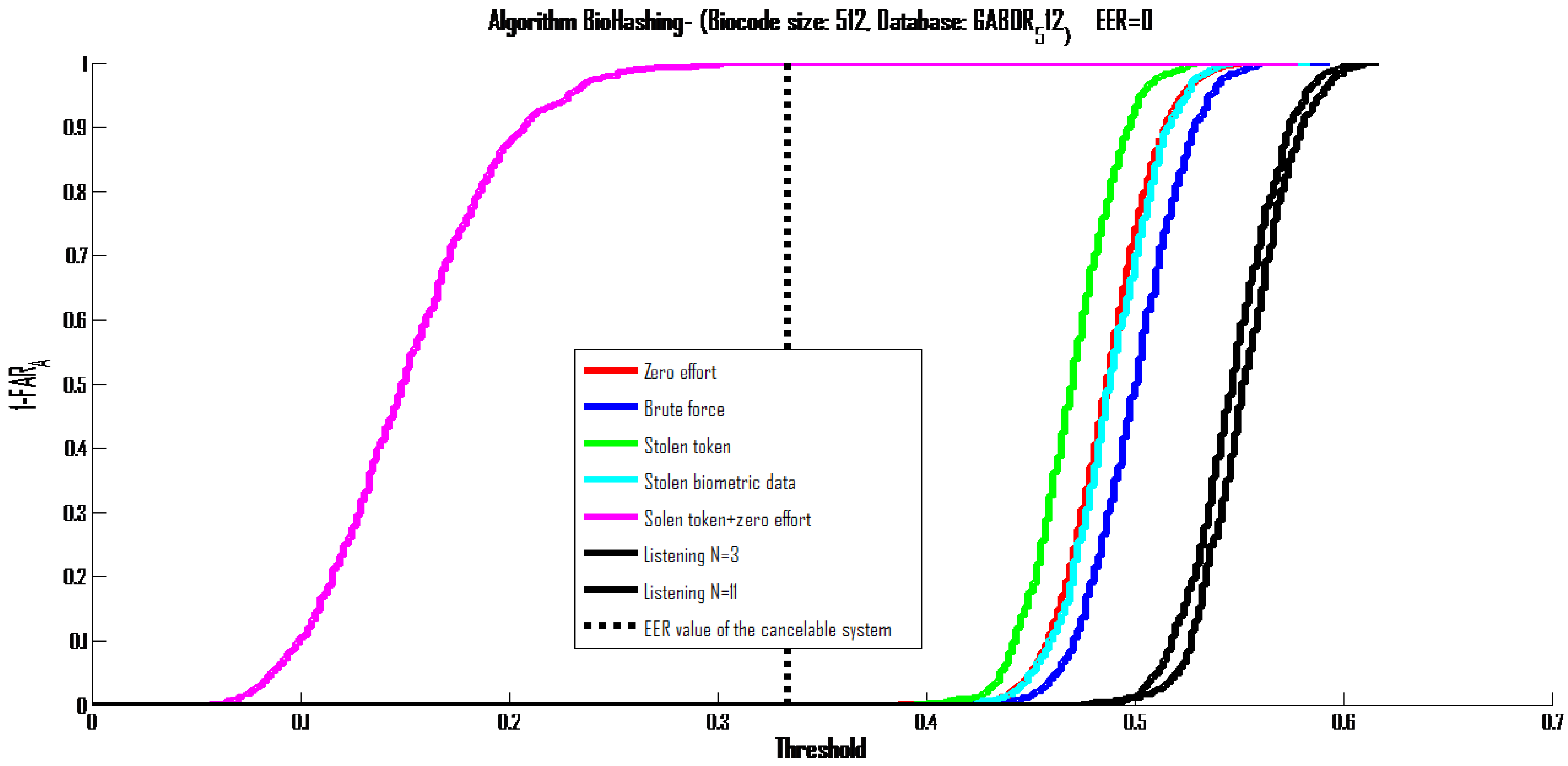
Jin, Andrew Teoh Beng, David Ngo Chek Ling, and Alwyn Goh. "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." *Pattern recognition* 37.11 (2004): 2245-2255.

BIOHASHING

Combining biometrics and passwords:

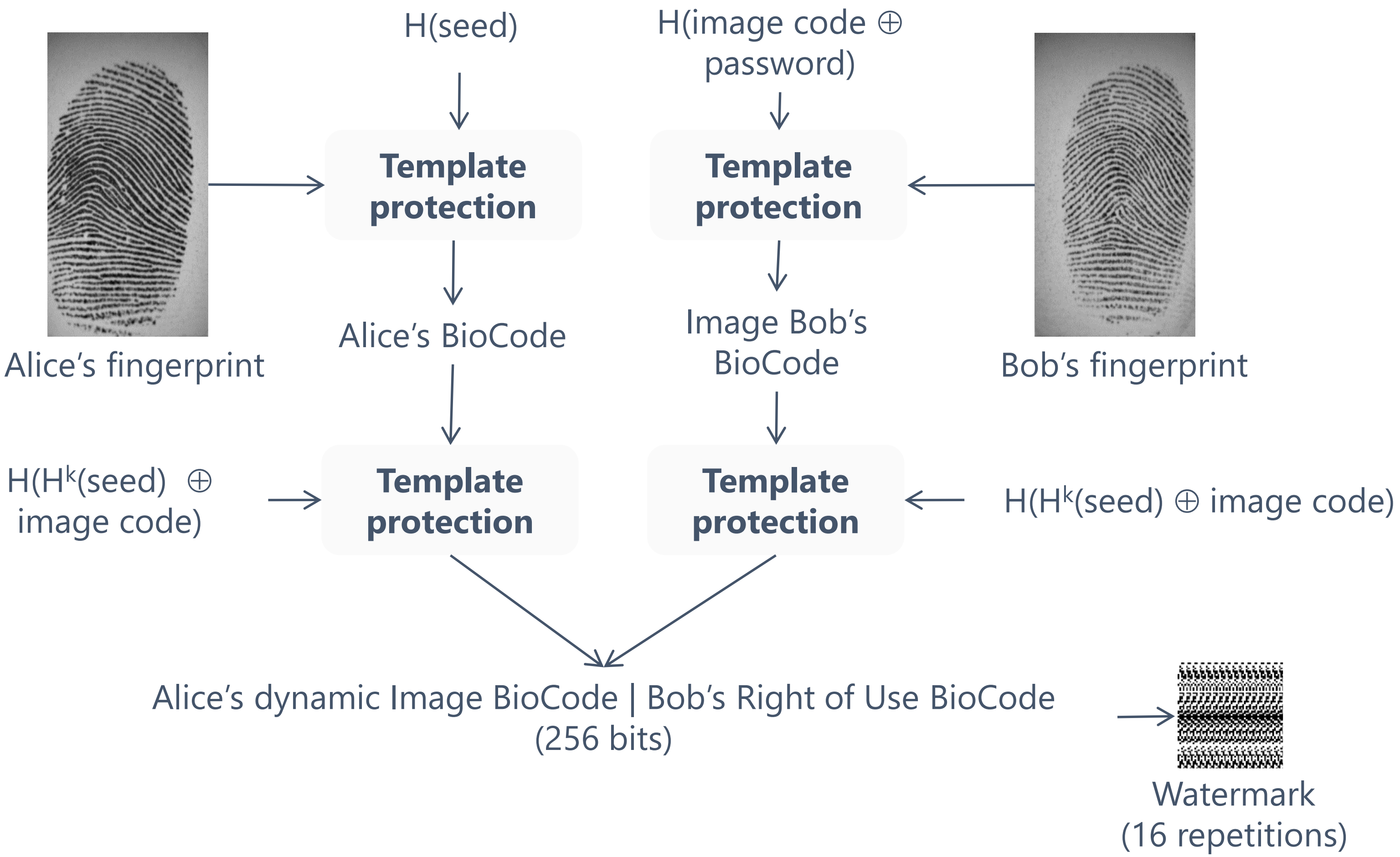
R. Belguechi, E. Cherrier, C. Rosenberger, S. Ait-Aoudia, "Operational Bio-Hash to Preserve Privacy of Fingerprint Minutiae Templates", IET journal on Biometrics, 2013

SECURITY ANALYSIS



R. Belguechi, E. Cherrier, C. Rosenberger, "How to Evaluate Transformation Based Cancelable Biometric Systems?", NIST International Biometric Performance Testing Conference (IBPC), 2012.

COPYRIGHT PROTECTION



Seed: Alice's master secret key
H: Hashing function
Password: provided by Alice to Bob

M. Barbier, J.-M. Le Bars, C. Rosenberger, "Image Watermarking With Biometric Data For Copyright Protection", International Conference on Availability, Reliability and Security (ARES), International Workshop MFSEC, August, Toulouse, France, 2015.

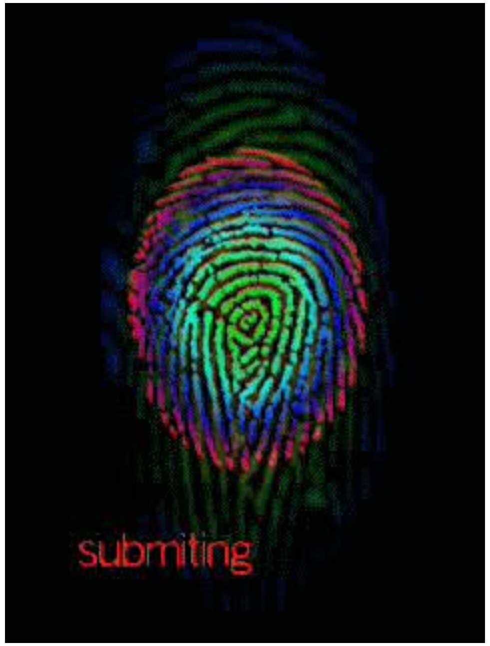
CONCLUSION

CONCLUSION

ENSI CAEN
ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

Biometrics

- ✓ Very interesting topic related to multiple research areas (cryptography, image processing, deep learning, embedded systems...)
- ✓ Many societal and scientific issues to solve
- ✓ Hot topic for industry and research



THANKS

Christophe ROSENBERGER

Full Professor

christophe.rosenberger@ensicaen.fr

ENSI CAEN

ÉCOLE PUBLIQUE D'INGÉNIEURS
CENTRE DE RECHERCHE

L'École des INGÉNIEURS Scientifiques