GREYC
MONÉTIQUE & BIOMÉTRIE

An Overview of Biometrics

Christophe Rosenberger
GREYC Research Lab - France

Plan

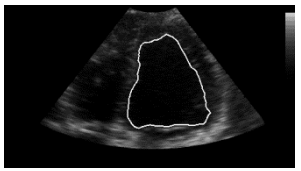
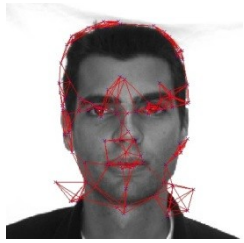
- GREYC research lab
- Introduction to biometrics
- Trends in biometrics
- Emerging techniques
- Conclusions

GREYC research lab

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

Laboratory staff:
- 7 CNRS researchers
- 25 Full professors
- 9 Associate professors
- 59 Assistant professors
- 79 PhD students
- 15 Administrative and technical staff

Research topics:
- Electronics
- Image processing
- Algorithmic
- Document analysis
- Multi-agents
- Robotics navigation
- Automatics
- Computer security
- Natural language processing
- Cryptography
- E-payment
- Biometrics

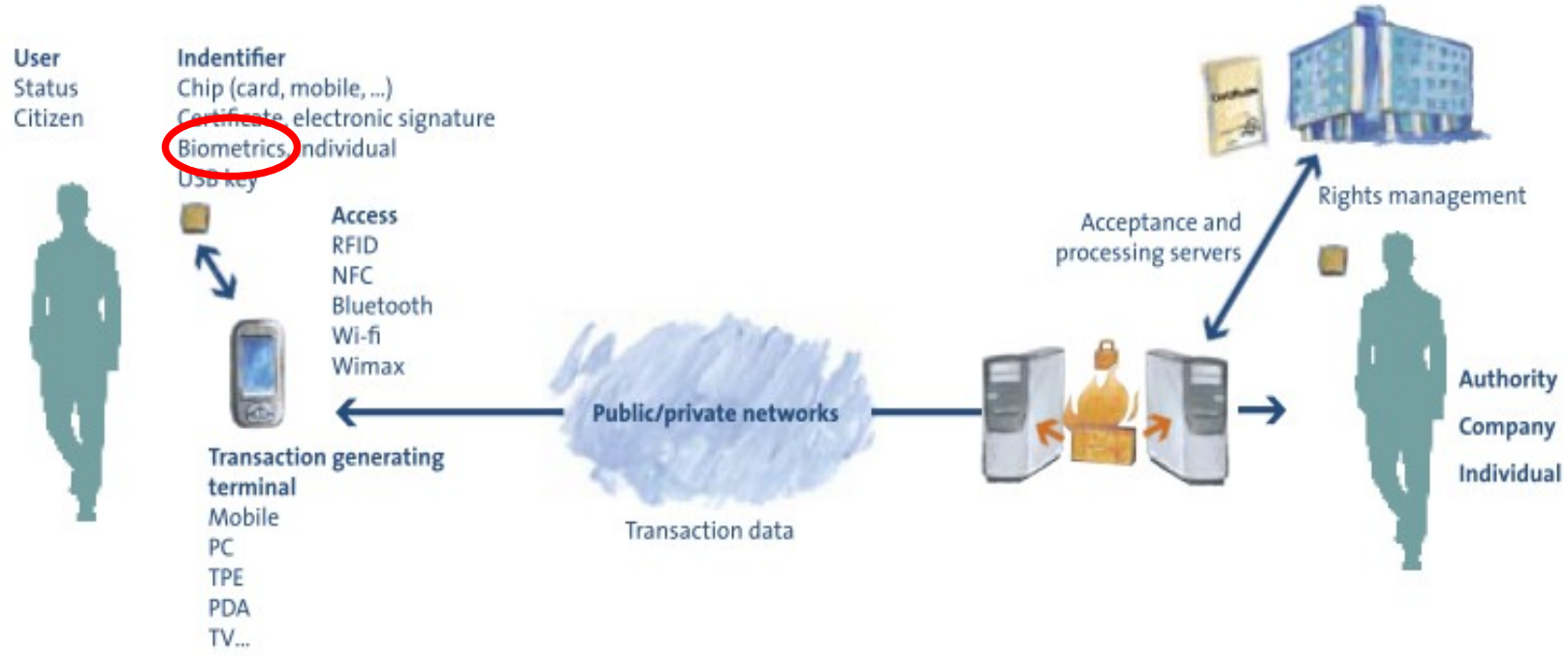





GREYC research lab

E-payment & biometrics research unit

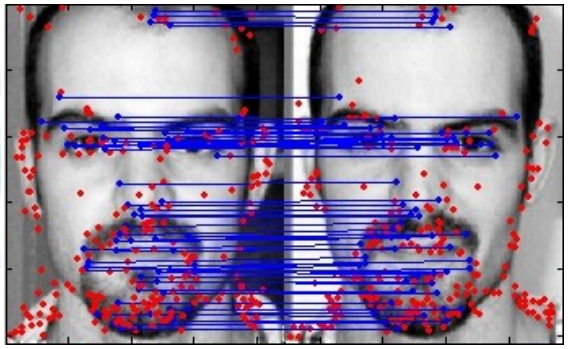
Biometrics: C2M authentication



E-transactions (© E-secure Transactions Cluster)

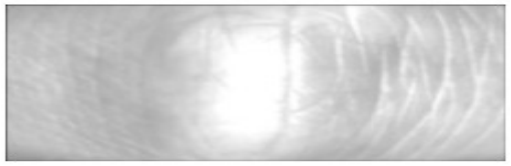
GREYC research lab

Biometric systems



Face

Iris

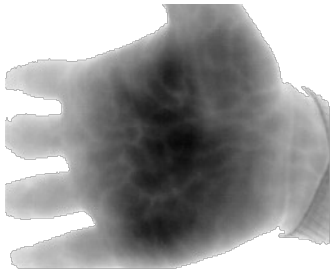


Finger Knuckle Print

Keystroke dynamics

Signature dynamics

Touch screen interaction



Hand shape, palm vein

Fingerprint

Plan

- GREYC research lab
- Introduction to biometrics
- Trends in biometrics
- Emerging techniques
- Conclusions

Introduction

GREYC

Definition: Authentication

Process whose objective is to guarantee the identity of a user or a service given a set level of confidence.

➡ **User Authentication**

Definition: Authentication factors

An authentication factor is an authenticator element:

- what we know (password),
- what we own (smartcard),
- What we are or how we behave (biometrics).

Introduction

GREYC

Biometric modalities:

- **Biological analysis**:

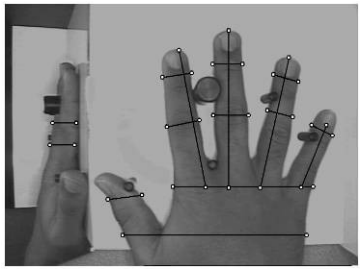
  EEG signal, blood, DNA…

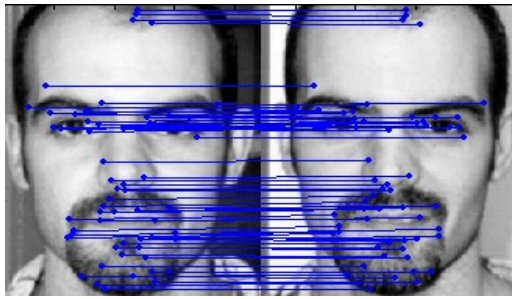
- **Behavioural analysis**:

  Keystroke dynamics, voice, gait, signature dynamics...

- **Morphological analysis**:

  Fingerprint, iris, palmprint, finger veins, face, ear…

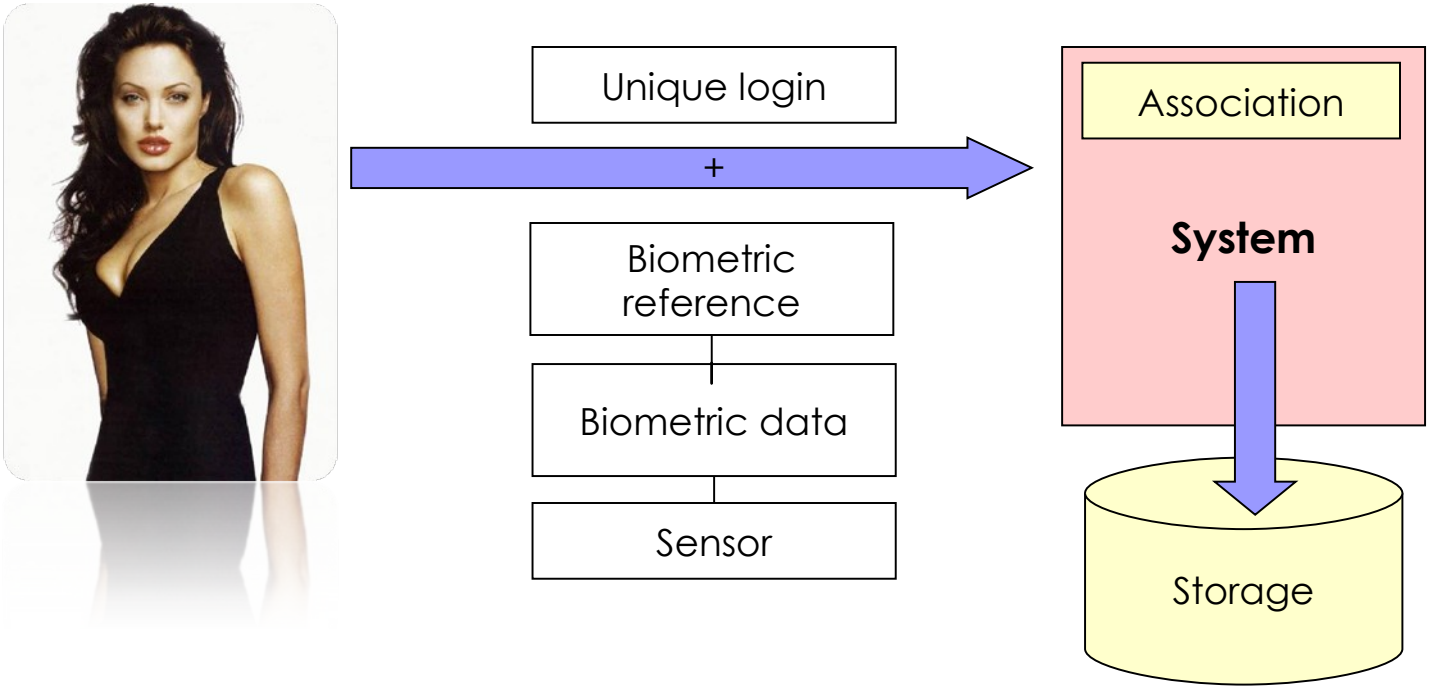




Introduction

Enrolment

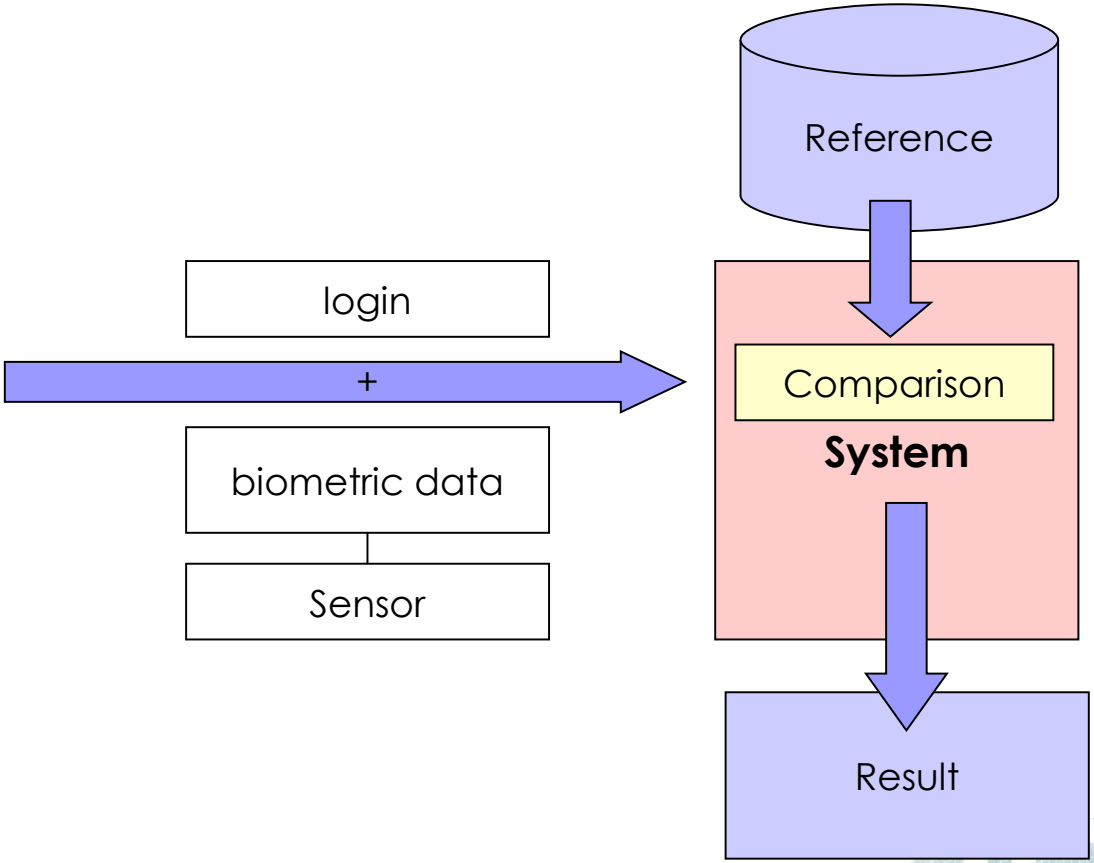
Individual's **registration** in the biometric system



Introduction

Verification

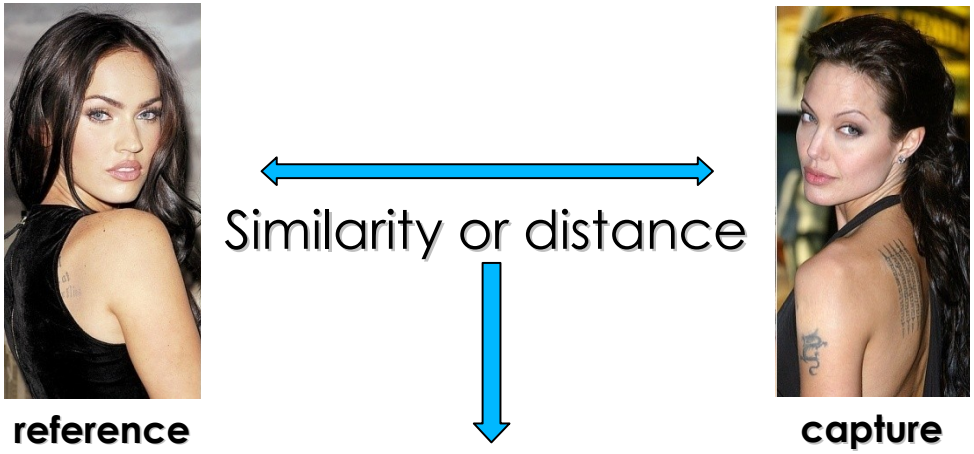
Comparison between the capture and **the reference**



Introduction

Matching result

Given the biometric reference and the capture, we have to decide if it is the same person.

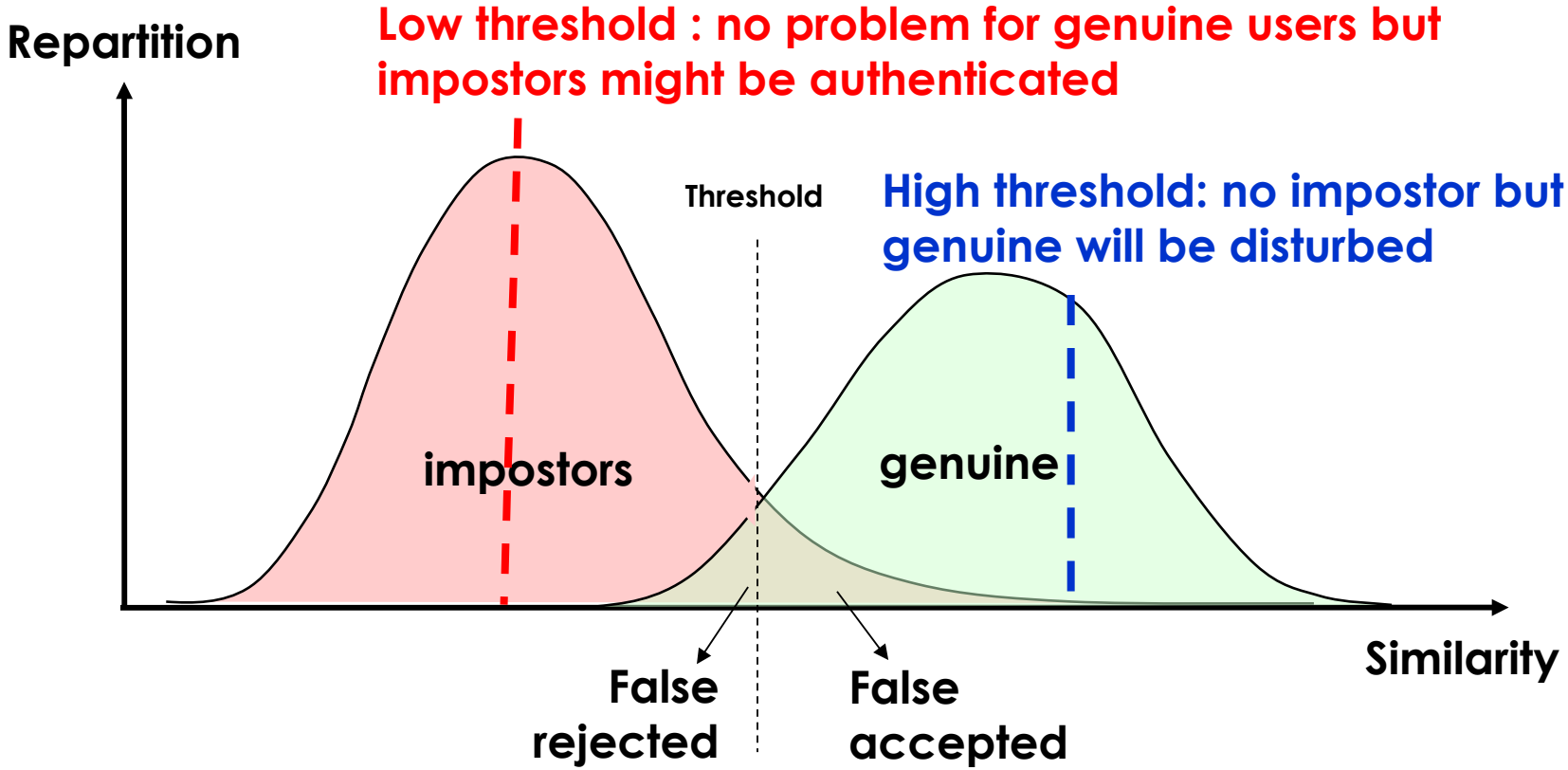


Use of a threshold for the decision

Threshold set by the administrator (in function of the application).

Introduction

Decision criterion



Introduction

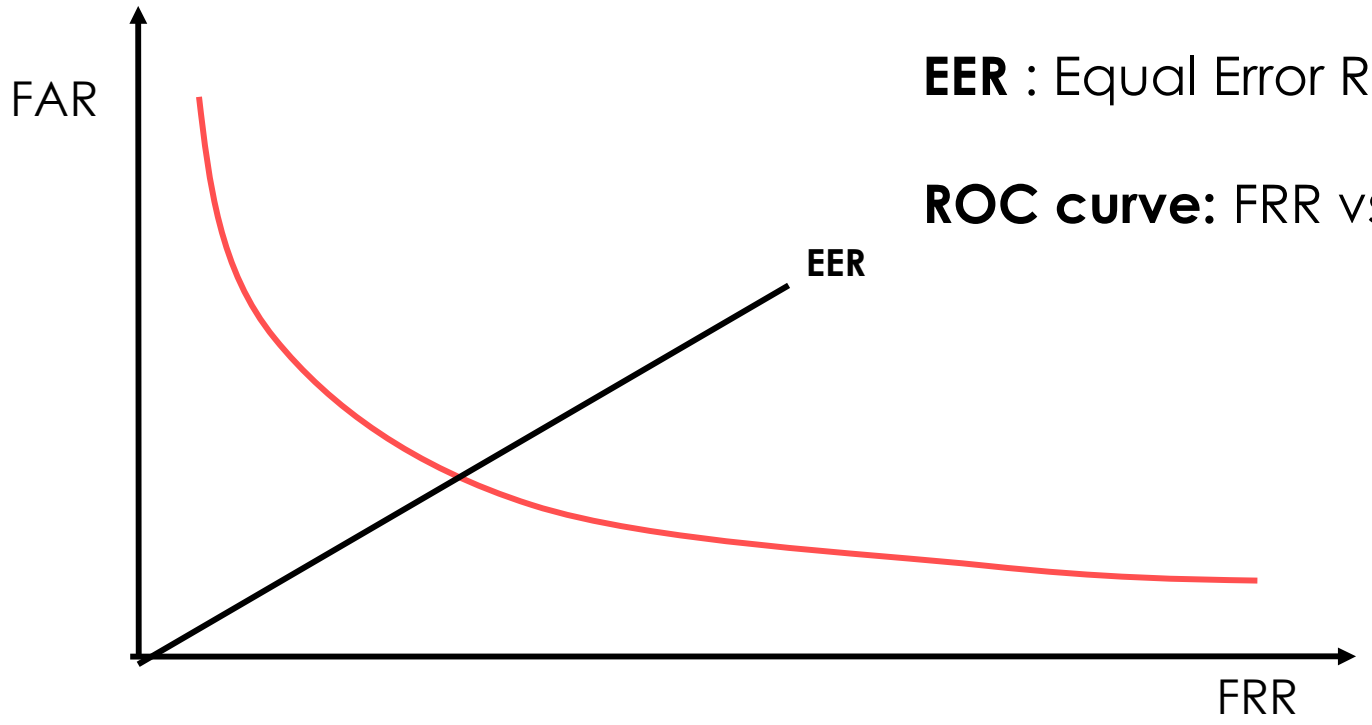
Performance evaluation

FAR : False Acceptance Rate

FRR : False Rejection Rate

EER : Equal Error Rate

ROC curve: FRR vs FAR



Plan

- GREYC research lab
- Introduction to biometrics
- **Trends in biometrics**
- **Emerging techniques**
- **Conclusions**

Trends

Performance and evaluation

Possible error for an authenthication result

Authentication for mobile devices

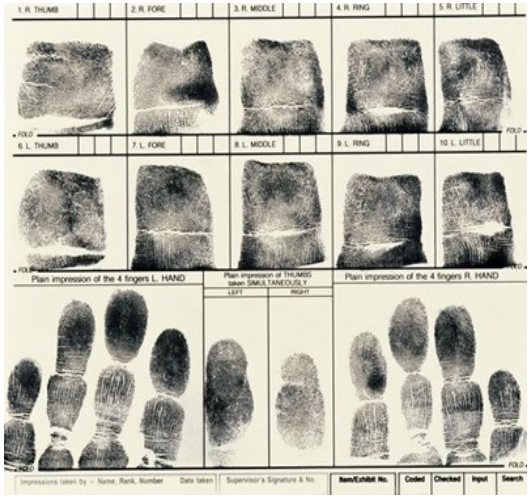
Bad capture of the biometric information

- Misuse

- Environment

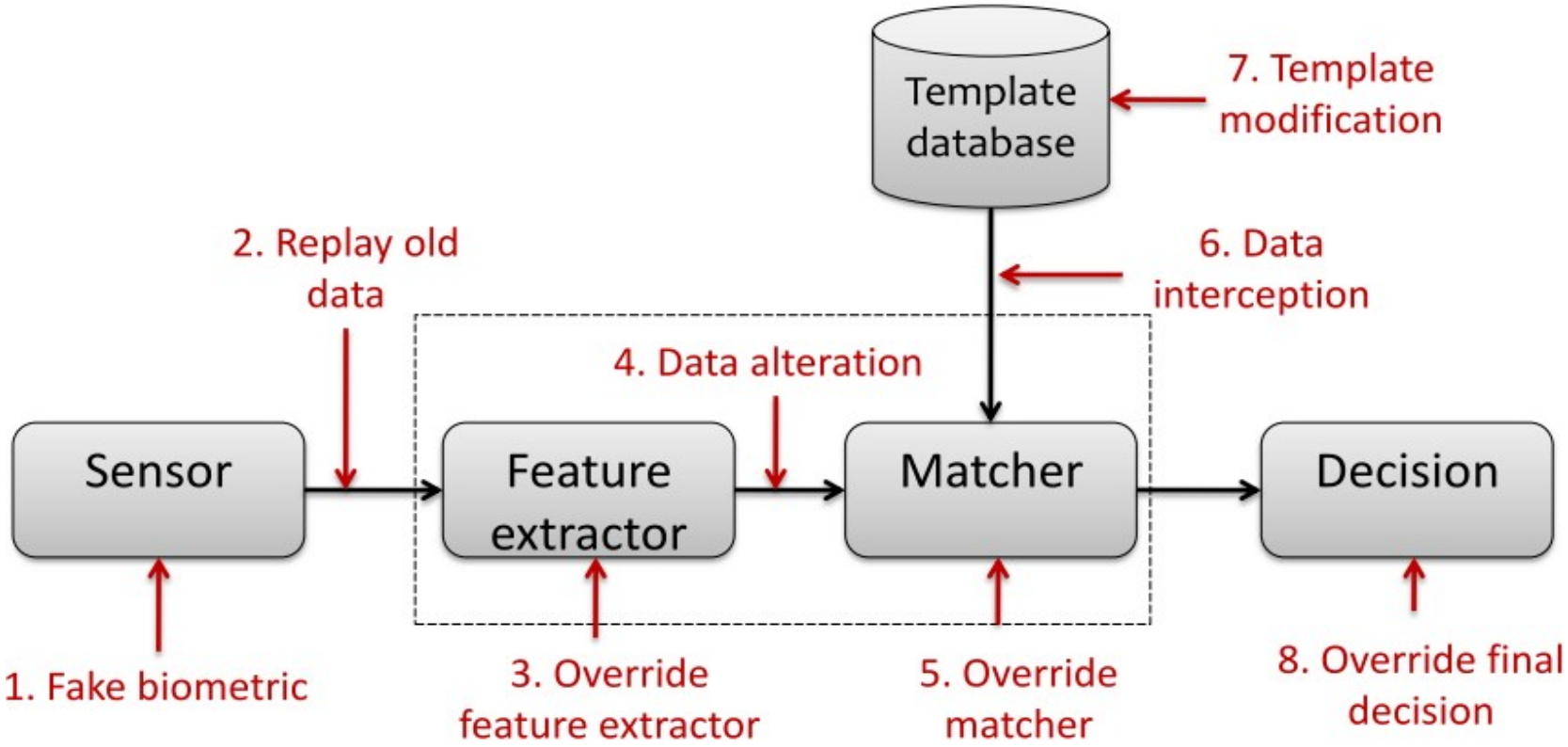
How to evaluate a biometric system ?

- Performance
- Security
- Usability



Trends

Security and privacy



Trends

Security and privacy

Liveness detection biometric sensor

Secure storage of the biometric template

Diversity of biometric templates

How to cancel a biometric information ?

Plan

- GREYC research lab
- Introduction to biometrics
- Trends in biometrics
- **Emerging techniques**
- **Conclusions**

Emerging technologies

A) Multibiometrics

B) Soft biometrics

C) Adaptive systems

D) Quality of biometric data

E) Cancelable systems

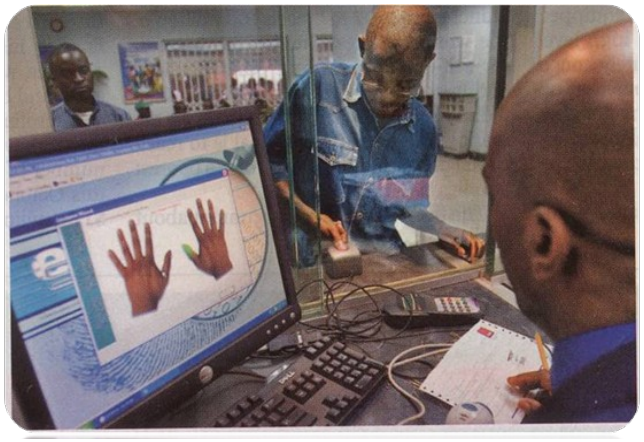
F) Secure storage

Multibiometrics

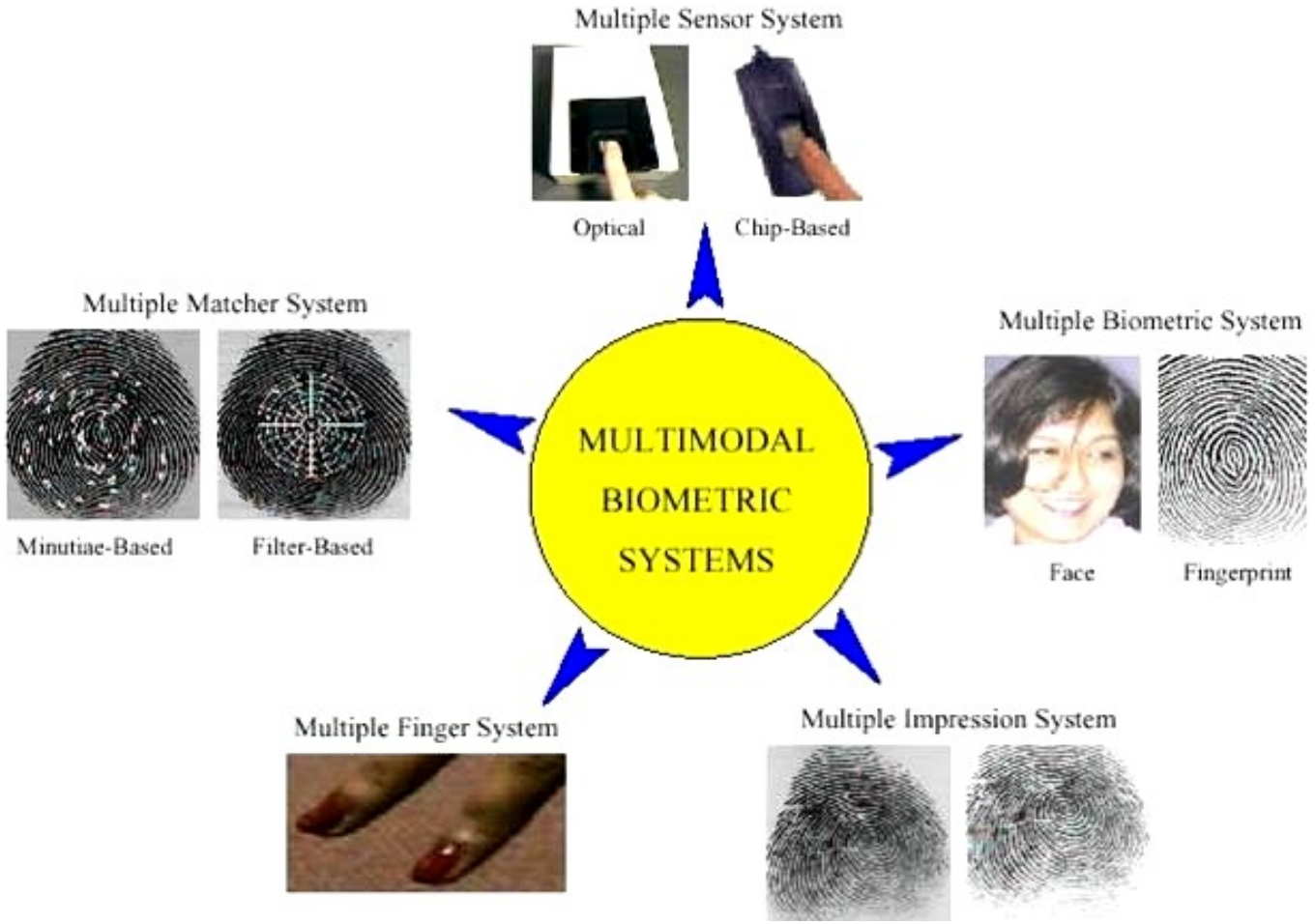
GREYC

Objectives:

- Combine different biometric systems to decrease errors,
- Have some alternatives in case of impossibility to use a biometric information (no sensor available, physical reasons…),
- Use as information as possible for the biometric system.

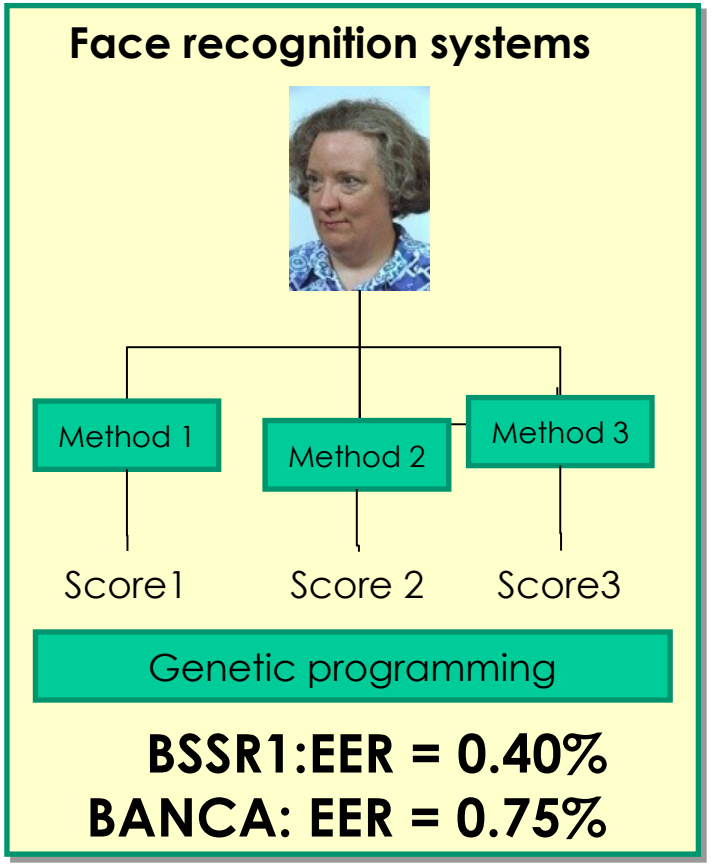


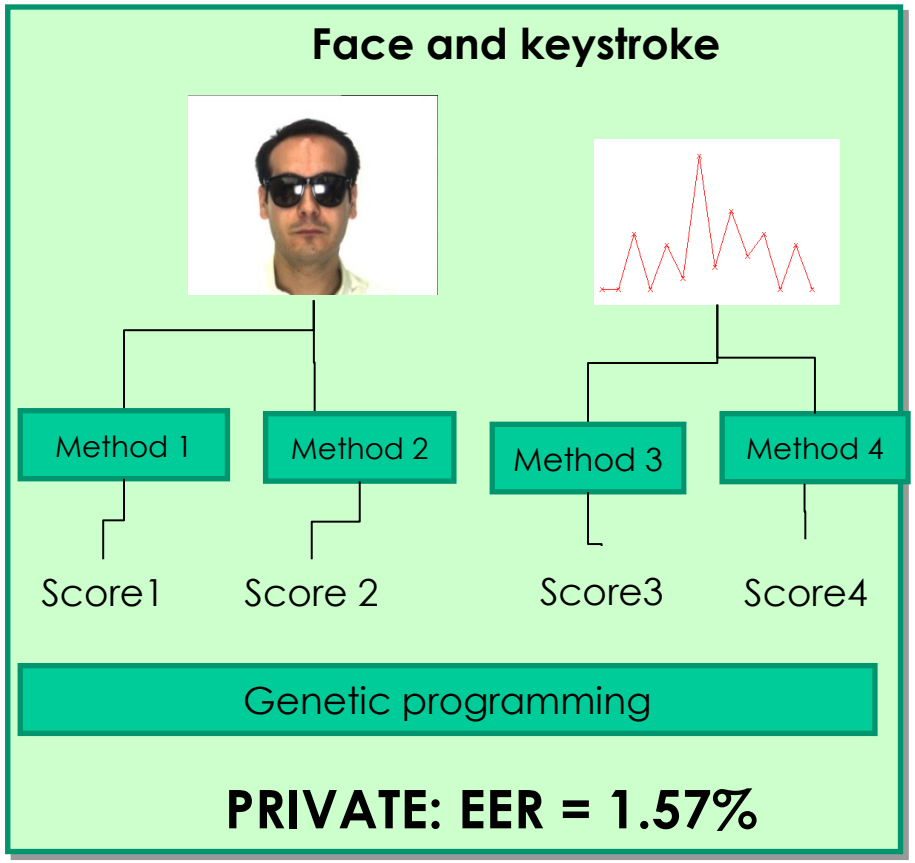
Multibiometrics



Jain et al. 2004

Multibiometrics





R. Giot, B. Hemery, C. Rosenberger, "Low Cost and Usable Multimodal Biometric System Based on Keystroke Dynamics and 2D Face Recognition", International Conference on Pattern Recognition (ICPR), 2010.

Soft biometrics

GREYC

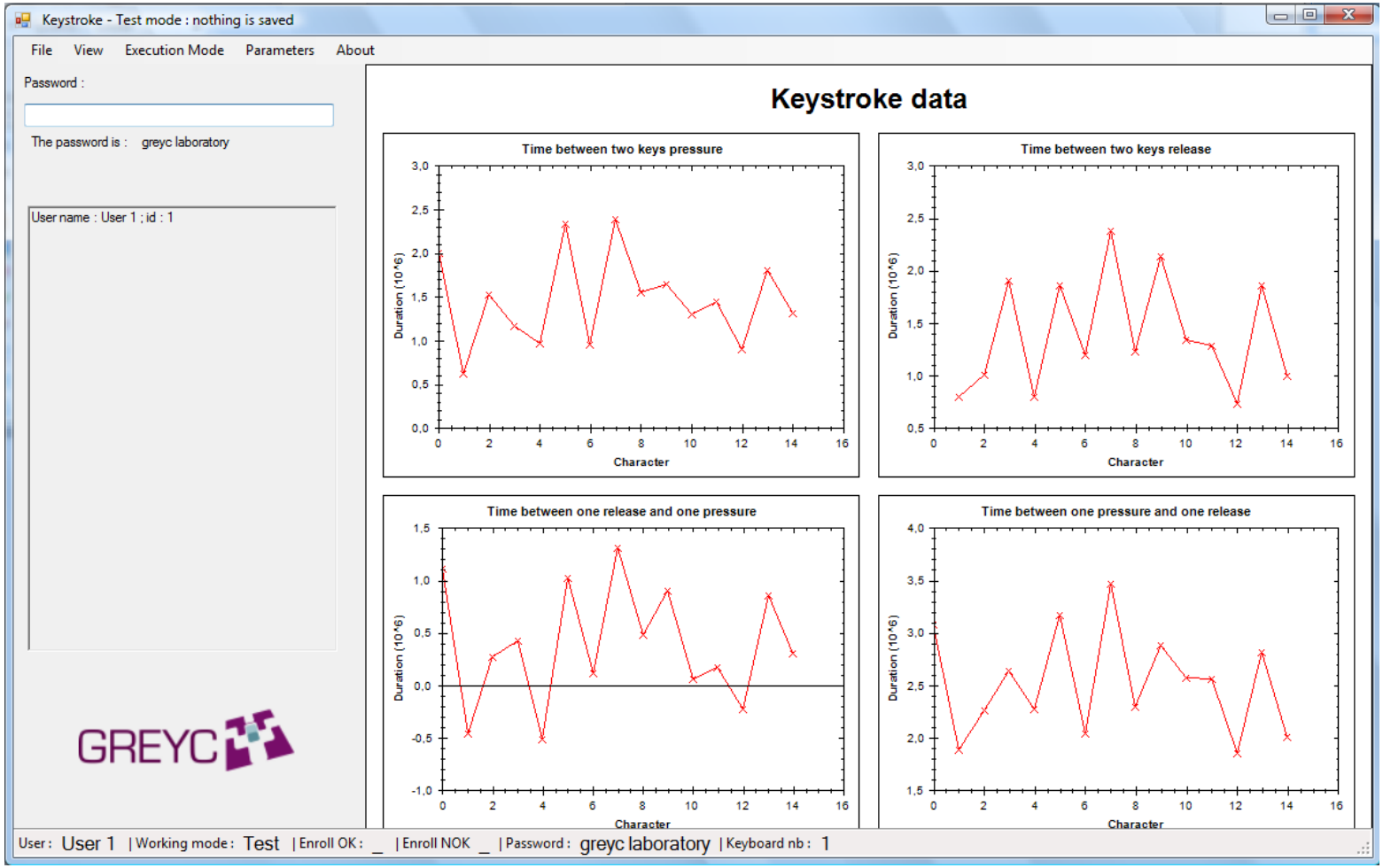
Objective

Use of a priori knowledge to make a better identity verification:

- Known information : i.e. Period between the capture and the date of capture of the reference (electronic passport)

- Extracted information : gender, non semantic category...

Soft biometrics



GREYC Keystroke software

Soft biometrics

Gender recognition with keystroke dynamics:

Experiments on a dataset composed of 133 users

Use of a passphrase « Greyc laboratory »

Gender recognition: 91% (based on SVM learning)

Classical keystroke recognition: EER = 10.6%

Keystroke recognition (gender recognition): EER = 7.6%

R. Giot, C. Rosenberger, "A New Soft Biometric Approach For Keystroke Dynamics Based On Gender Recognition" International Journal of Information Technology and Management (IJITM) Special Issue on : "Advances and Trends in Biometrics". Dr Lidong Wang, pages 1-16, 2011.

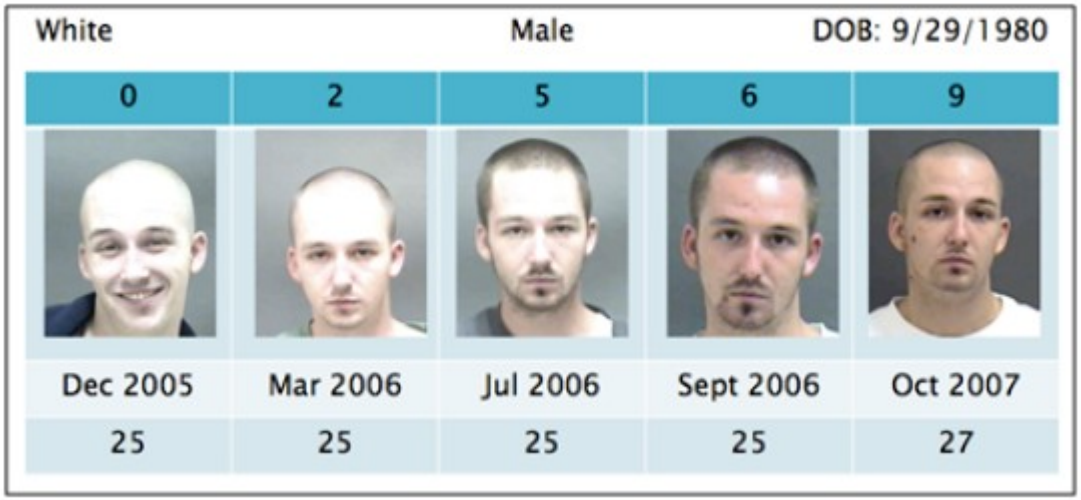
Adaptive systems

Objective

Deal with the intrinsic intraclass variability of the biometric captures following two approaches:

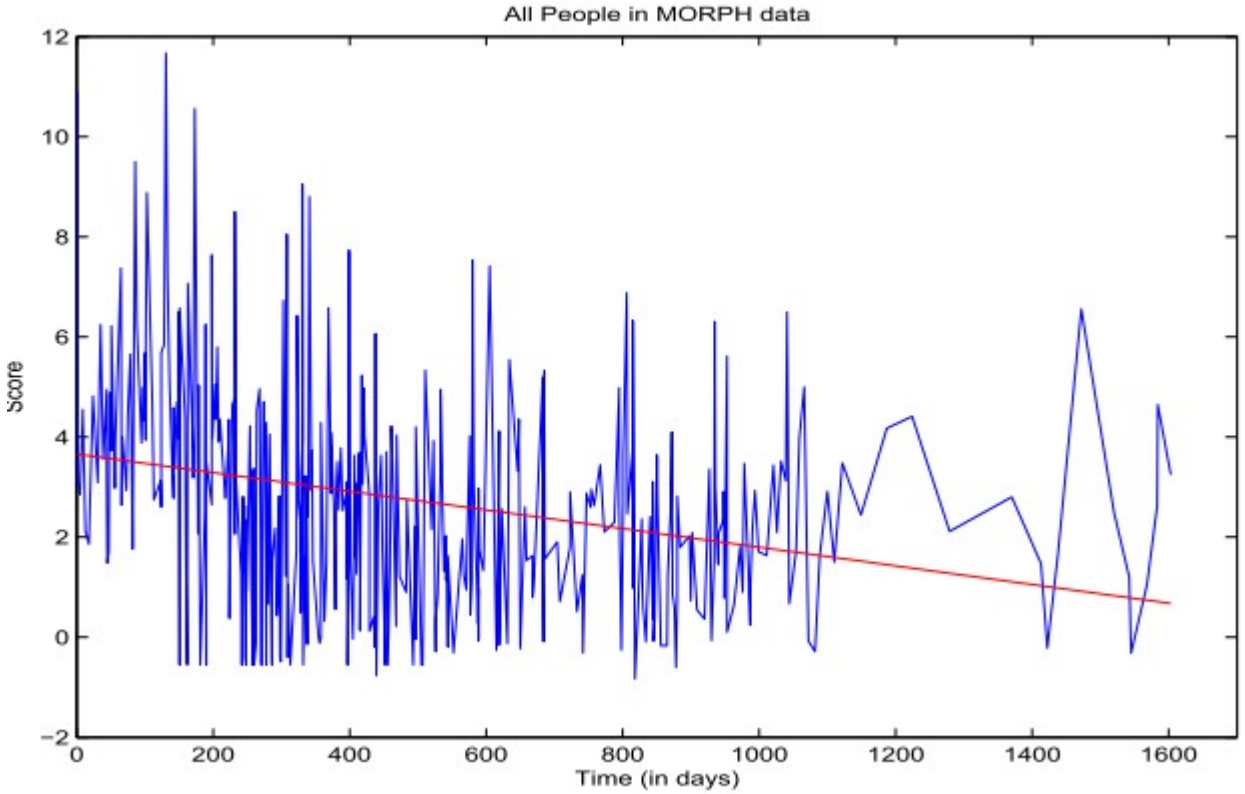
- Adaptive decision threshold setting,

- Template update strategies.



MORPH database

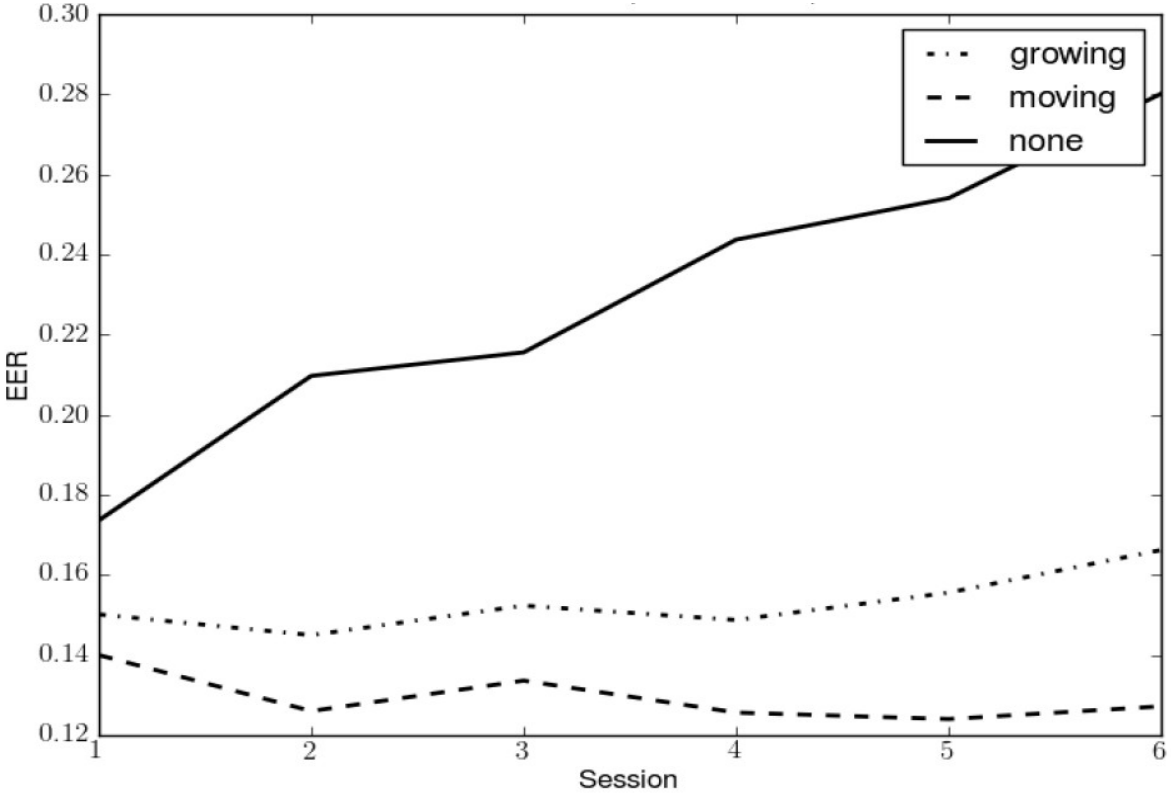
Adaptive systems



Evolution of the intra-score with ageing faces in the MORPH database

W. LI, A. DRYGAJLO and H. QIU: Aging face verification in score-age space using single reference image template. In Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, pages 1–7. IEEE, 2010.

Adaptive systems



Template update for keystroke dynamics

R. Giot, B. Dorizzi, C. Rosenberger, "Analysis of Template Update Strategies for Keystroke Dynamics", SSCI 2011 CIBIM - 2011 IEEE Workshop on Computational Intelligence in Biometrics and Identity Management 2011

Quality of biometric data

Objective

Quantifying the quality of a biometric raw data to optimize the performance of biometric systems

nfiq=5

nfiq=2

Patrick Grother, Elham Tabassi, "Performance of Biometric Quality Measures", IEEE Transactions on Pattern Analysis and Machine Intelligence archive, Volume 29 Issue 4, April 2007

Quality of biometric data

GREYC

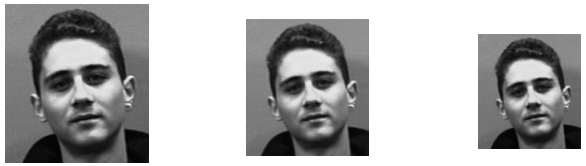
A generic approach for image based biometric captures

1) BLIINDS
2) Keypoints
3) DC coefficient
4) Mean and 5) Standard deviation of scales

10-class SVM

Sample quality

1 2 3 4 5 6 7



8 9 10

Quality of biometric data

Database	Good	Fair	Poor	Very poor
FACES94	0.4744 0.2936	0.6843 0.5131	1.8078 1.661	5.7983 5.044
ENSIB	10.6397 10.413	13.2912 13.4	16.5495 16.53	17.787 17.774
FERET	31.88 26	32.23 30.187	32.52 32.12	34.37 33.757

The predicted EER /real EER values for each quality set

Method	Good	Fair	Poor	Very poor
Contribution	0.869	0.828	0.797	0.626
NFIQ	0.82	0.698	0.632	0.64

Kolmogorov-Smirnov (KS) test of the genuine and impostor scores distribution

M. El Abed, R. Giot, B. Hemery, C. Charrier, C. Rosenberger, "A SVM-Based Model for the evaluation of biometric sample quality" SSCI 2011 CIBIM - 2011 IEEE Workshop on Computational Intelligence in Biometrics and Identity Management 2011.

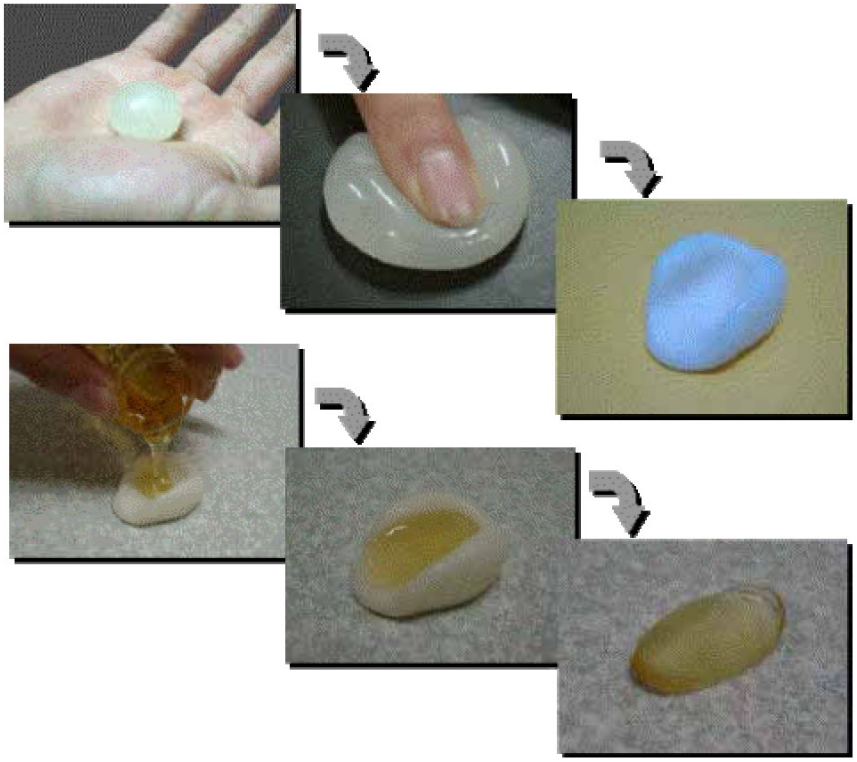
Cancelable systems

GREYC

Motivations

A biometric information:

- can be duplicated,
- can be stolen.



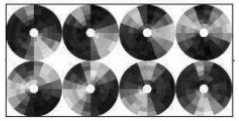
Problem of privacy

➡ Proposal of algorithmic solutions

Cancelable systems

Cancelable biometrics: make the biometric template revocable

Feature



Fingercode

seed

BioHashing

Salting with the seed

$m \leq n$

$b_i \in \{0,1\}$

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

BioCode

- ❑ The original image is not stored
- ❑ The biocode is stored
- ❑ It is not possible to compute the pattern or retrieve the original image given the biocode
- ❑ A biocode can re-generated with another seed
- ❑ The biohashing process improves performance

R. Belguechi, C. Rosenberger, "Study on the Convergence of FingerHashing and a Secured Biometric System", Proceedings of the International conference CIIA, 2009.

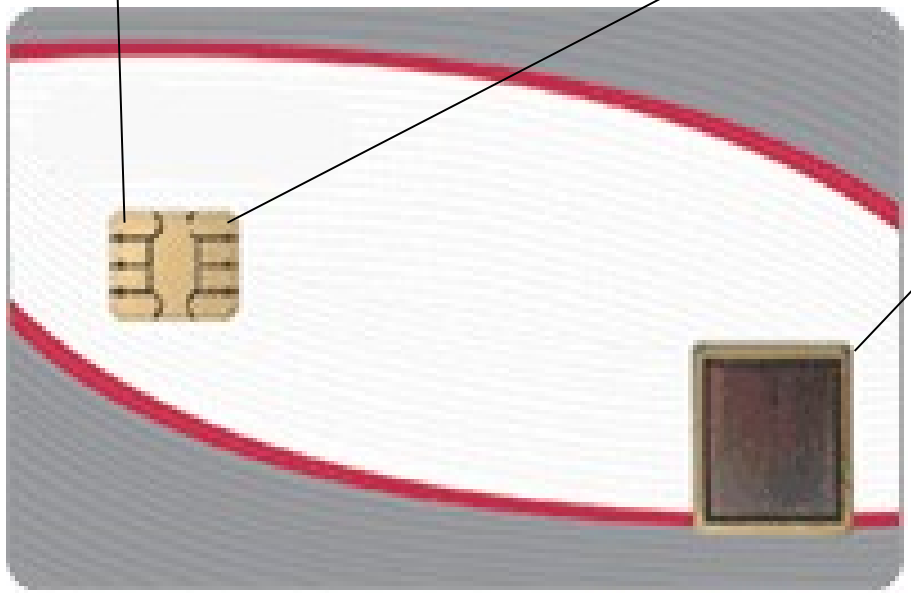
Secure storage

GREYC

Match and capture on card solution

Comparison between the reference and the capture

Storage of the reference fingerprint



Fingerprint sensor

Plan

- GREYC research lab
- Introduction to biometrics
- Trends in biometrics
- Emerging techniques
- **Conclusions**

Conclusion

Many achievements in the state of the art

Improving the performance (multibiometrics, quality, adaptability, soft biometrics)

Protection of the biometric templates (PET, storage in a SE, embedded capture)

Perspectives

Privacy:

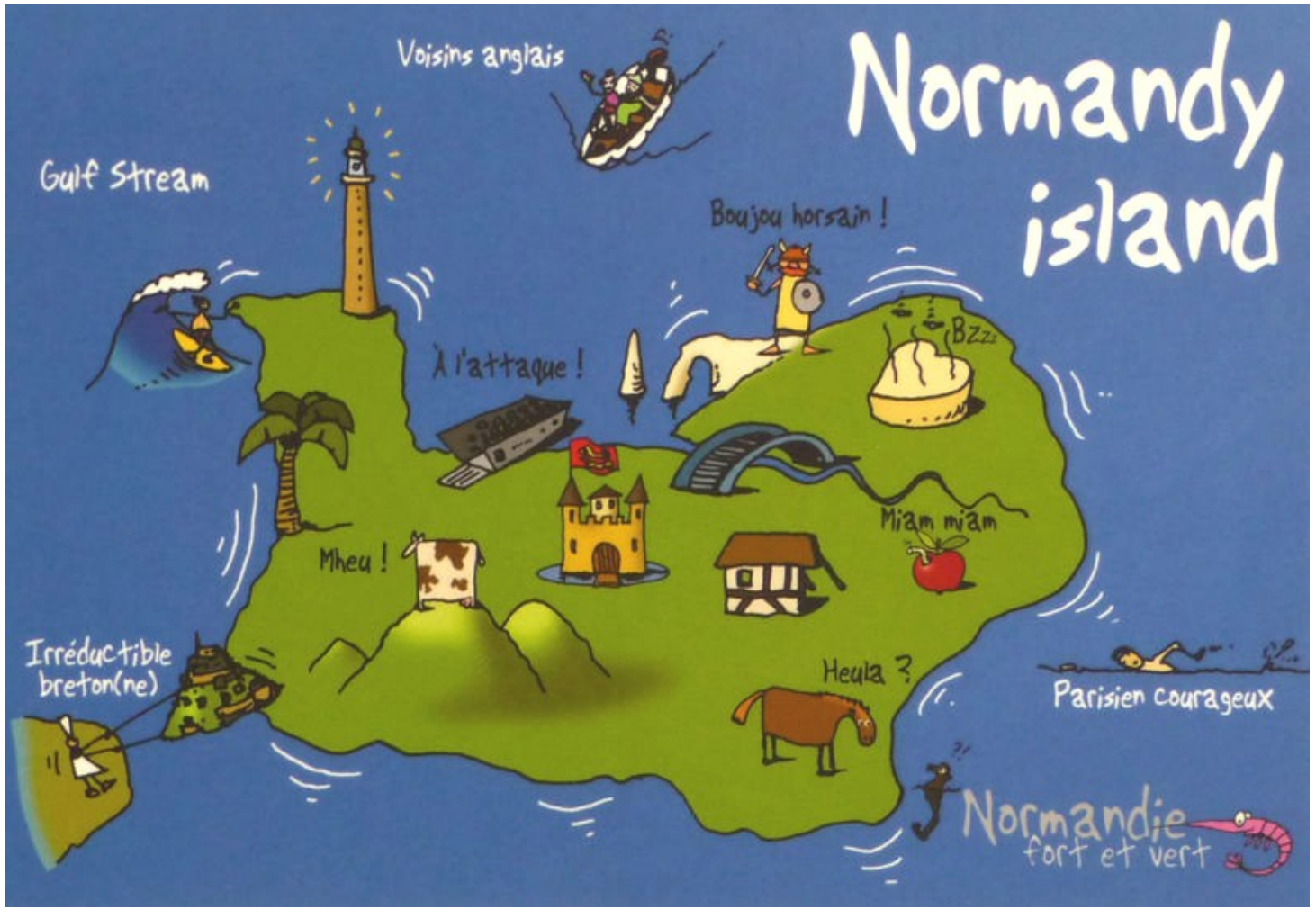
Study the robustness of PET

Security:

End to end

Mobility

Questions



christophe.rosenberger@ensicaen.fr

http://www.epaymentbiometrics.ensicaen.fr

Algorithme génétique

Algorithme génétique :
Méthode d'optimisation s'appuyant sur la théorie de l'évolution de Darwin (1859) et sur les méthodes de combinaison des gènes par Mendel (1976).

Analogie avec la sélection naturelle dans le monde vivant
L'évolution dans le monde vivant a permis l'émergence de d'organismes étonnamment adaptés à leurs environnements.

Propriétés :

- Il n'est pas nécessaire de dériver la fonctionnelle à optimiser,
- technique efficace pour un espace de recherche important,
- pas nécessaire d'avoir une solution initiale.

Algorithme génétique

Principe :

Un algorithme génétique est défini par les étapes suivantes :

1. Définition de la population initiale et calcul de la fonction d'aptitude de chaque individu,
2. Sélection des individus,
3. Mutation et croisement des individus,
4. Évaluation des individus dans la population,
5. Retour à l'étape 2 si le critère d'arrêt non satisfait.

Programmation génétique

Un exemple : approximation polynomiale