Journée thématique Biométrie – 4 juin 2010

La biométrie : principes & enjeux

Christophe Rosenberger
Professeur à l'ENSICAEN
Laboratoire GREYC

GREYC
MONÉTIQUE & BIOMÉTRIE

ENSICAEN
ÉCOLE NATIONALE SUPÉRIEURE D'INGÉNIEURS DE CAEN
& CENTRE DE RECHERCHE

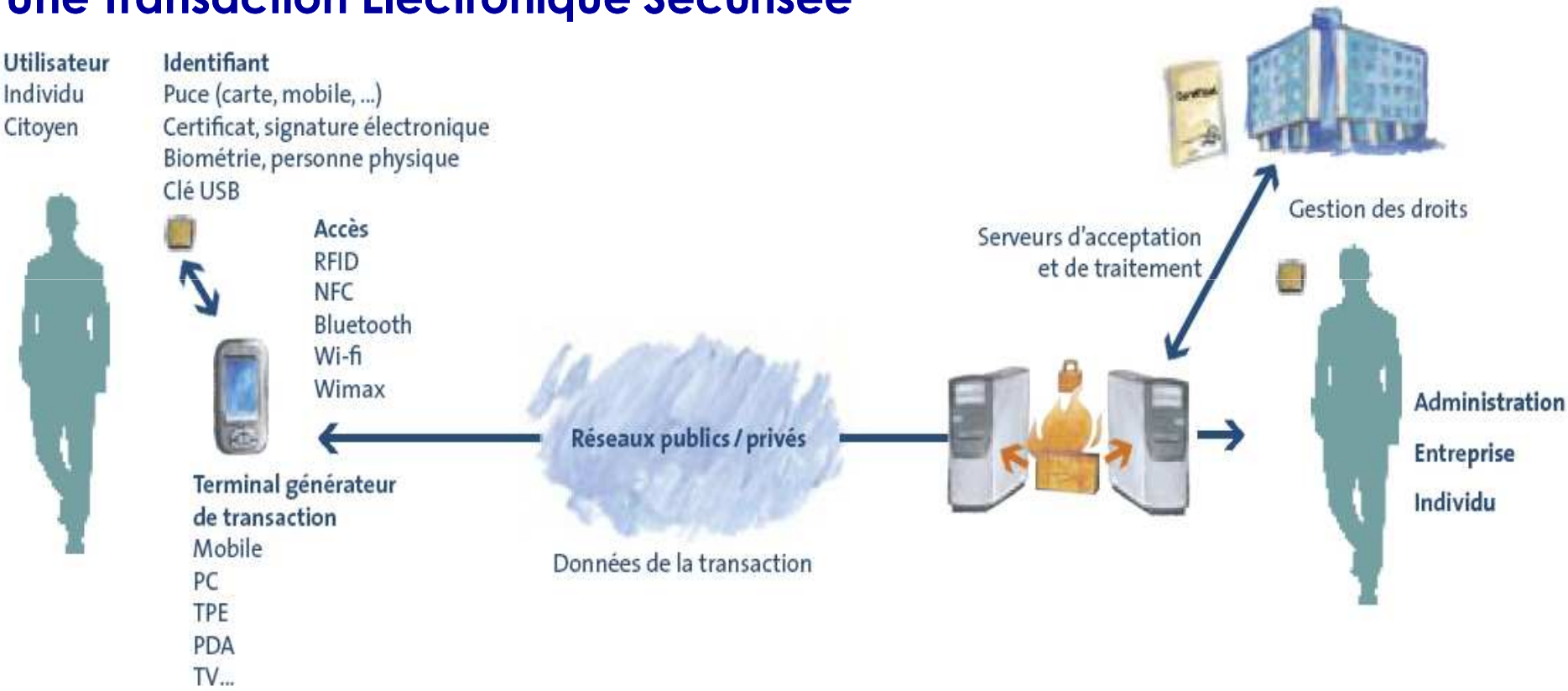
cnrs
dépasser les frontières

Université de Caen
Basse-Normandie

PLAN

- Motivations
- Les principes de la biométrie
- Les enjeux de la biométrie
- Les activités de recherche au GREYC

Une Transaction Electronique Sécurisée



L'authentification d'un individu

Définition : Procédé visant à s'assurer avec un niveau de confiance raisonnable de l'identité d'un utilisateur

Ne pas confondre avec l'identification

Définition : Facteur d'authentification

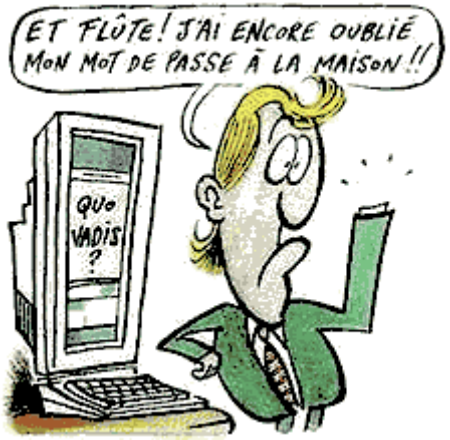
Un facteur d'authentification est un élément :

- que l'on sait (mot de passe),
- que l'on possède (support physique),
- que l'on est ou que l'on sait faire (biométrie).

L'authentification d'un individu

Les enjeux

- Confiance dans l'identité du client
- Difficulté à falsifier ou s'approprier
- Respect de la vie privée du client
- Faciliter l'usage pour le client



PLAN

- Motivations
- Les principes de la biométrie
- Les enjeux de la biométrie
- Les activités de recherche au GREYC

L'authentification biométrique

Catégories de biométrie :

- **Analyse biologique** :

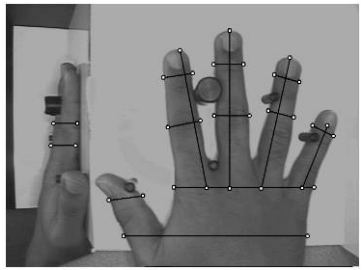
ADN, signal cardiaque…

- **Analyse comportementale** :

dynamique de la signature, la dynamique de frappe au clavier, voix...

- **Analyse morphologique** :

empreinte digitale, forme de la main, traits du visage, réseau veineux de la main…



L'authentification biométrique

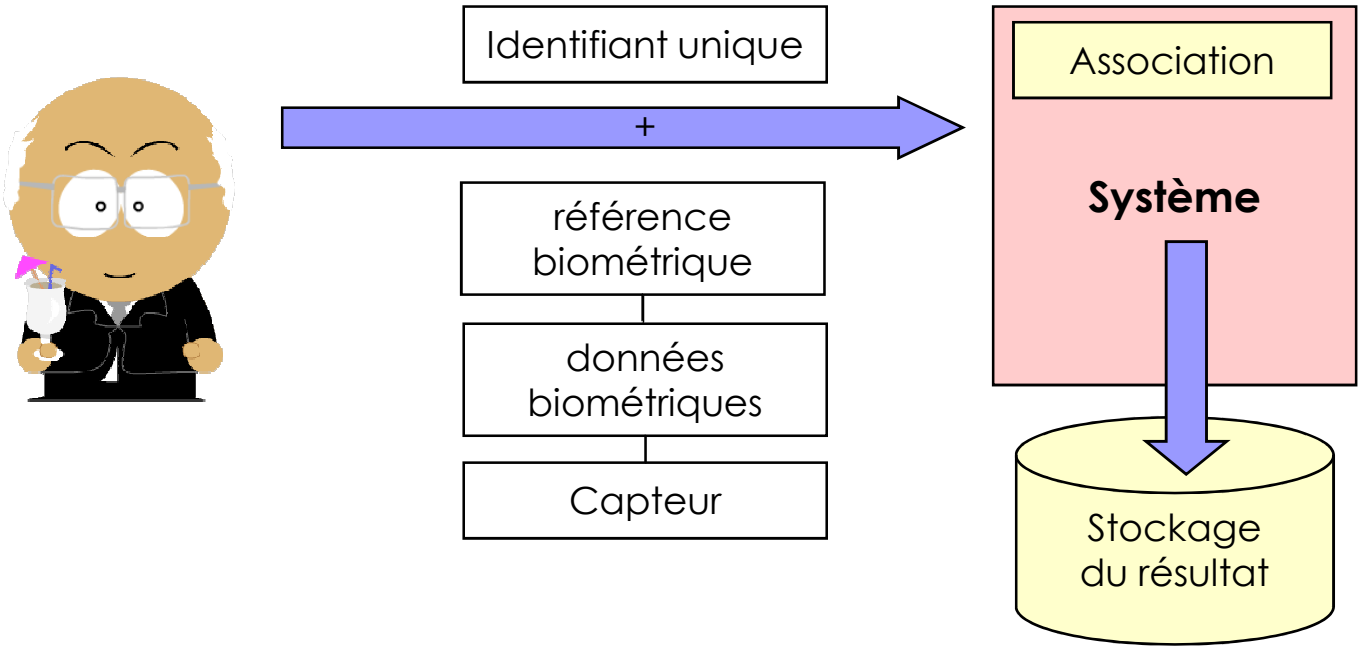
Propriétés

Une information biométrique doit respecter les propriétés suivantes :

- **Universalité** : Tous les individus peuvent être caractérisés par cette information ;
- **Unicité** : Cette information doit être aussi différente que possible pour deux individus différents ;
- **Permanence** : Elle doit subsister durant la vie de l'individu ;
- **Collectabilité** : Elle doit être mesurable facilement ;
- **Acceptabilité** : Les utilisateurs doivent être prêts à donner cette information.

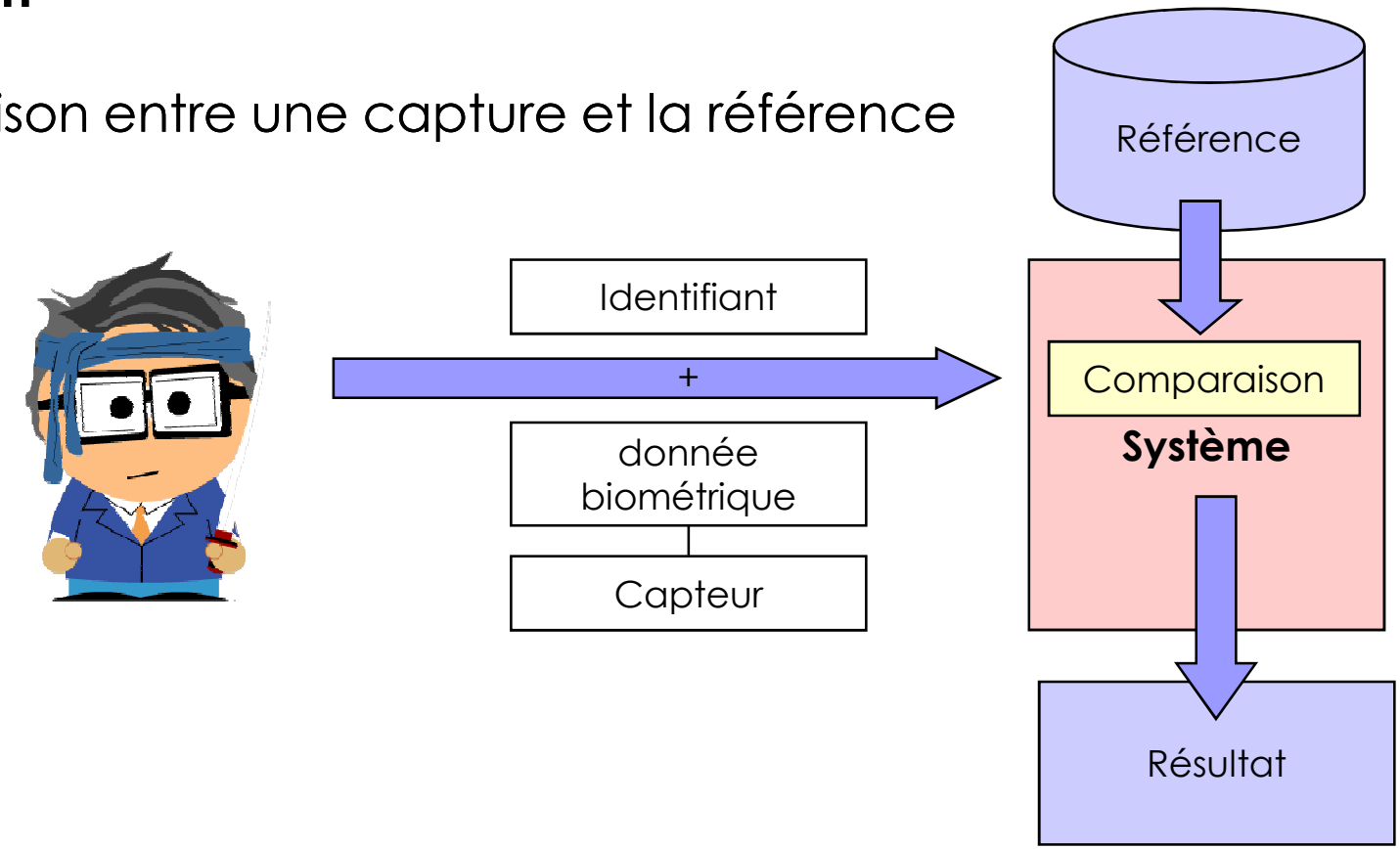
Enrôlement

Enregistrement de l'individu dans le système

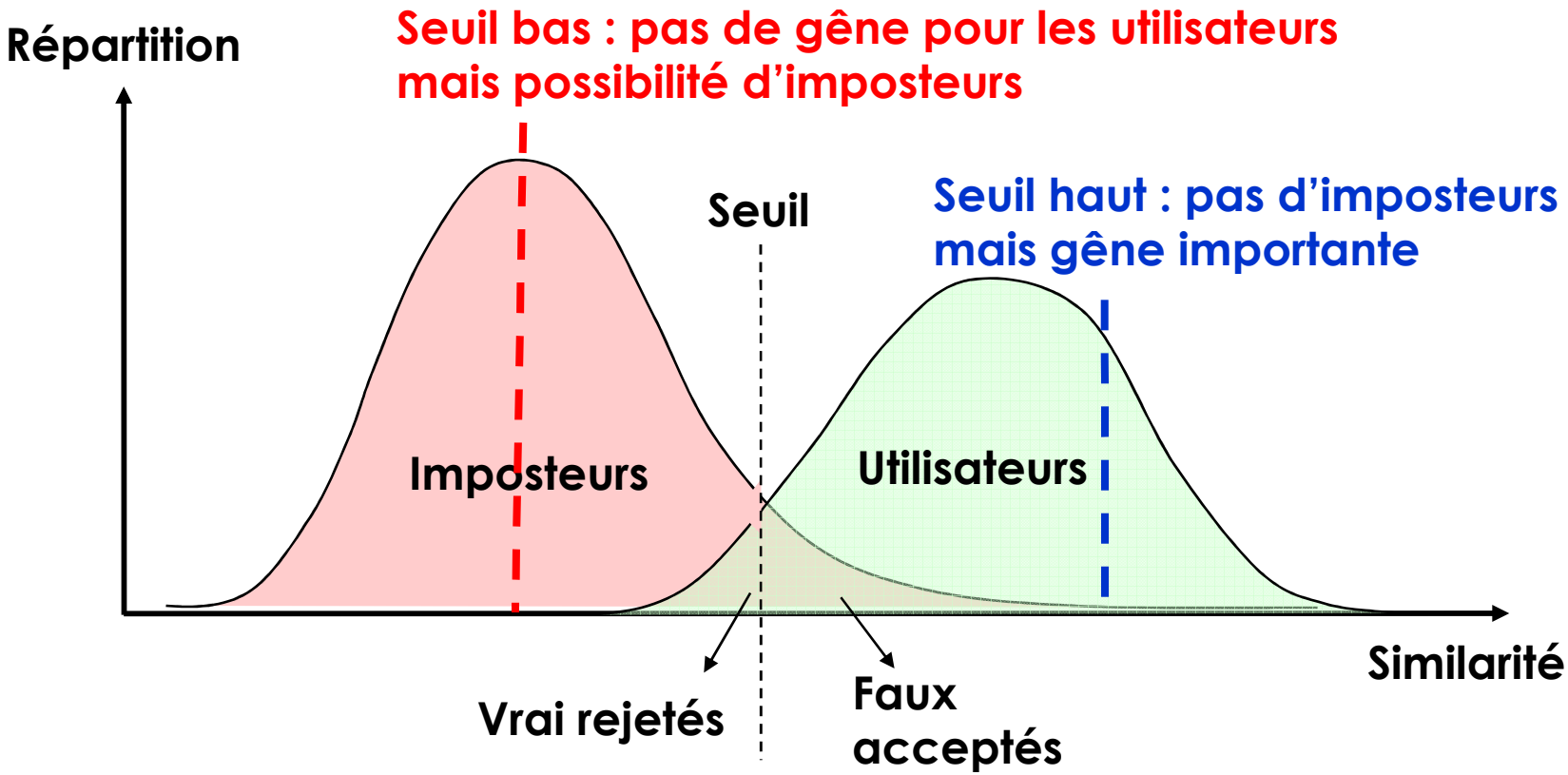


Vérification

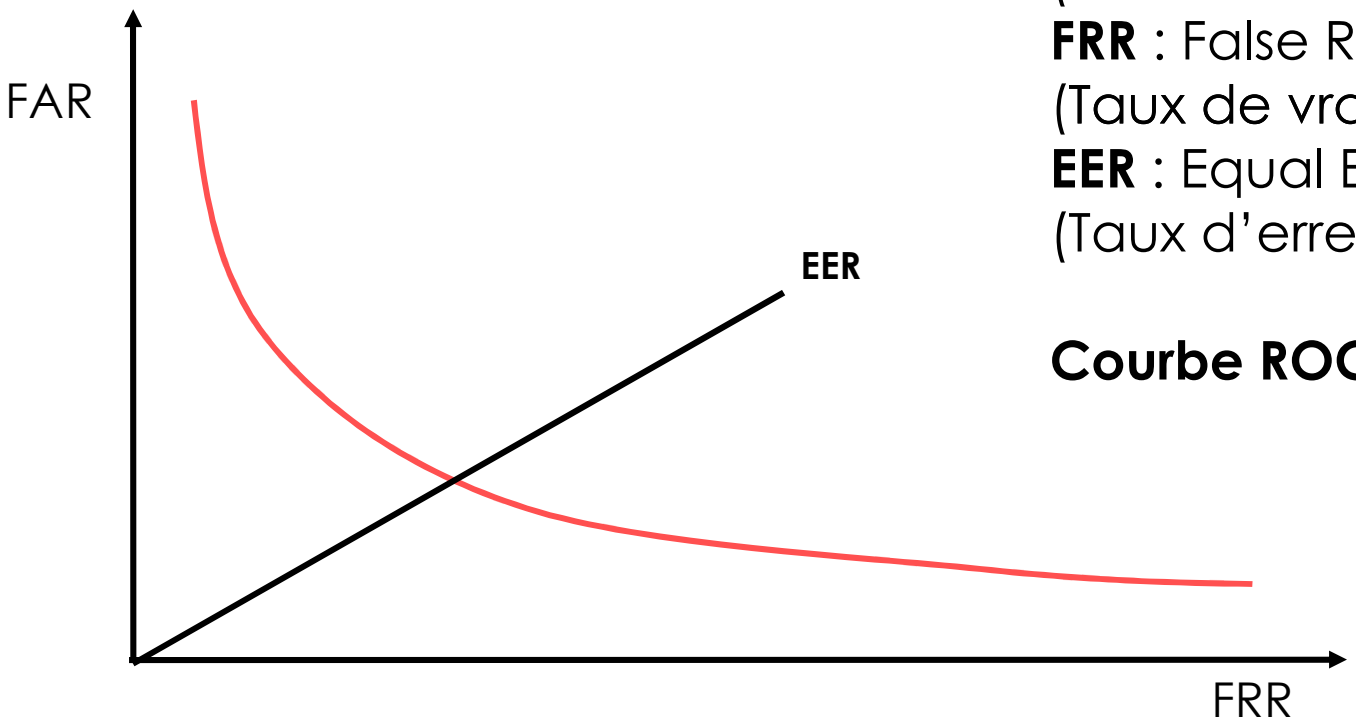
Comparaison entre une capture et la référence



Evaluation de performance



Evaluation de performance



FAR : False Acceptation Rate
(Taux de faux acceptés)
FRR : False Rejection Rate
(Taux de vrais rejetés)
EER : Equal Error Rate
(Taux d'erreur compromis)

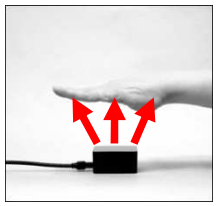
Courbe ROC : FAR vs FRR

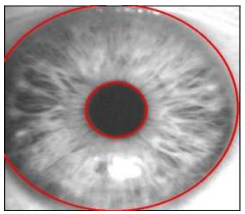
Modalités biométriques

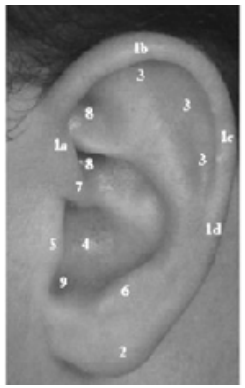
Empreintes digitales, visage, iris, rétine, veines de la main, veines des doigts, plis des doigts, oreille, forme de la main, lignes de la main, thermographie infrarouge du visage...

Dynamique de frappe au clavier, dynamique de signature, démarche, façon de conduire une voiture, dynamique d'interaction avec un écran tactile, façon de jouer au poker sur internet...

Voix, signal cardiaque...







Applications

- Contrôle d'accès physique (locaux)
- Contrôle d'accès logique (PC, SI..)
- Contrôle douanier ou police
- Machine & Équipement divers
- Résolution de crimes
- Système de vote électronique

PLAN

- Motivations
- Les principes de la biométrie
- **Les enjeux de la biométrie**
- **Les activités de recherche au GREYC**

Les enjeux la biométrie (1)

- **Performance** : Rupture technologique de l'authentification ou une erreur est possible intrinsèquement

➡ roposer des systèmes plus performants

- Nouvelles modalités biométriques (veines...)
- Nouveaux algorithmes
- Combinaison de systèmes (multimodalité)

Les enjeux la biométrie (2)

- **Sécurité** : des attaques sont possibles (SI, biométrie…)

➡ Solutions :

- Qualifier la sécurité des systèmes existants
- Utiliser des données biométriques révocables
- Contraindre le stockage et le traitement biométrique dans des enceintes sécurisées

Les enjeux la biométrie (3)

- **Acceptabilité** : l'usage de cette technologie doit être amélioré

➡ Solutions :

- Communication sur la protection des données personnelles
- Limiter le nombre de données pour l'enrôlement
- Favoriser les modalités perçues comme non intrusives

PLAN

- Motivations
- Les principes de la biométrie
- Les enjeux de la biométrie
- **Les activités de recherche au GREYC**

GREYC :
Groupe de Recherche en Informatique, Image, Automatique et Instrumentation de Caen

Unité mixte CNRS 6072

Effectif du Laboratoire :

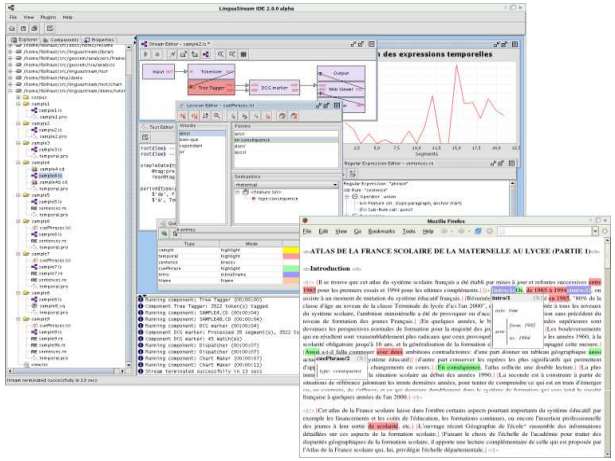
- 7 chercheurs CNRS
- 27 professeurs des universités
- 6 maîtres de conférences HDR
- 59 maîtres de conférences
- 56 doctorants
- 16 post-doctorants
- 15 personnels IATOS

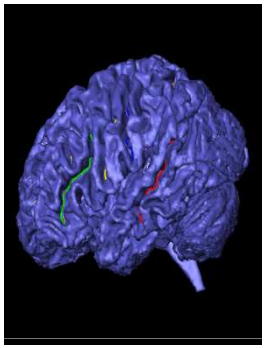
GREYC

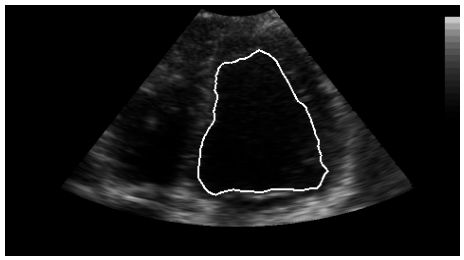
www.GREYC.fr

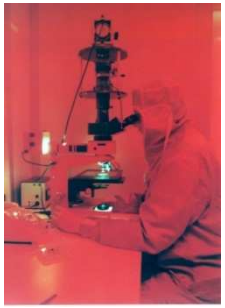
Thèmes de recherche :

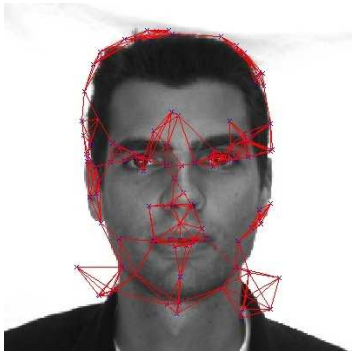
- Electronique
- Traitement d'images
- Transactions électroniques
- Algorithmique
- Analyse de documents
- Multi-agents
- Biométrie
- Automatique
- Sécurité informatique
- Traitement du langage naturel...





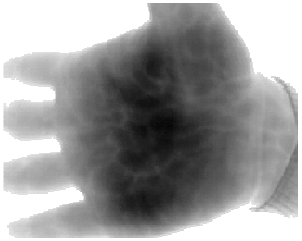






Quelques activités de recherche au GREYC en biométrie

- **Développement de systèmes biométriques**
  - Faible enrôlement
  - Multimodalité

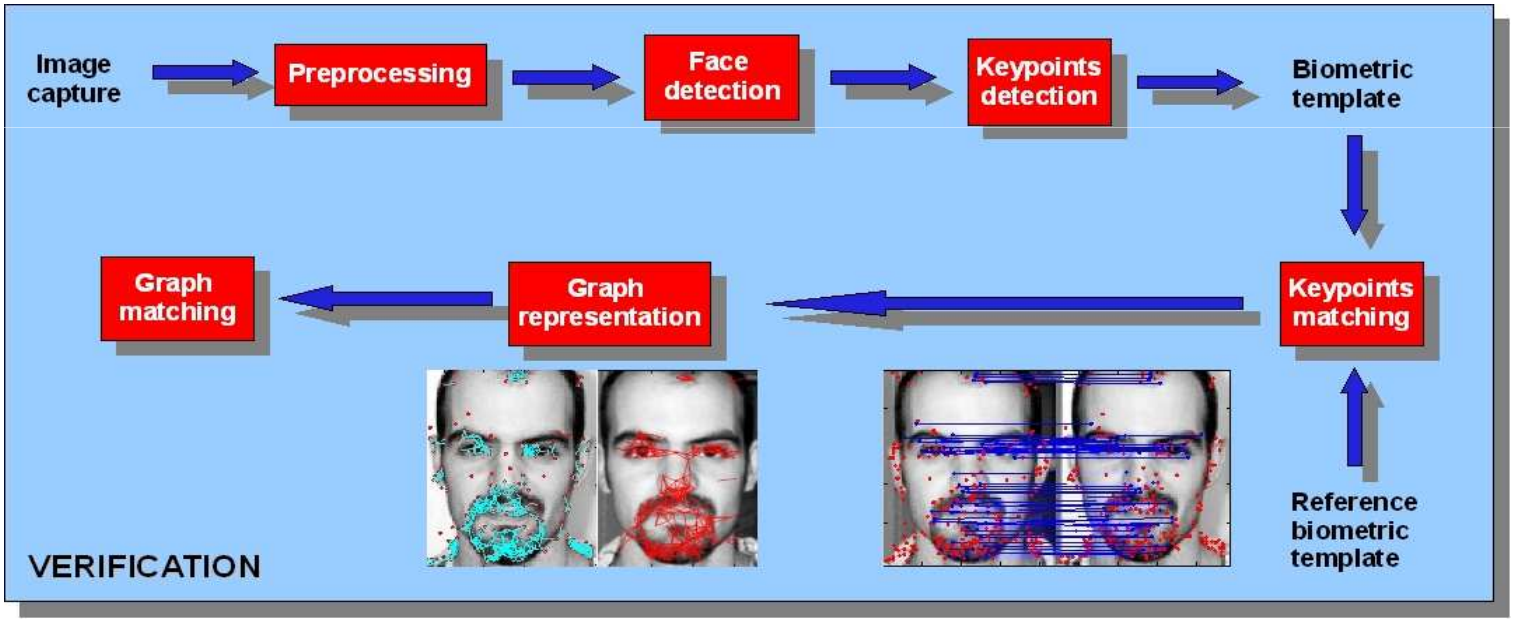


- **Évaluation de systèmes biométriques**
  - Performance
  - Acceptabilité des utilisateurs
  - Sécurité du système

- **Protection de la biométrie**
  - Stockage et traitement carte à puce Global Platform
  - Biométrie révocable

Authentification faciale :

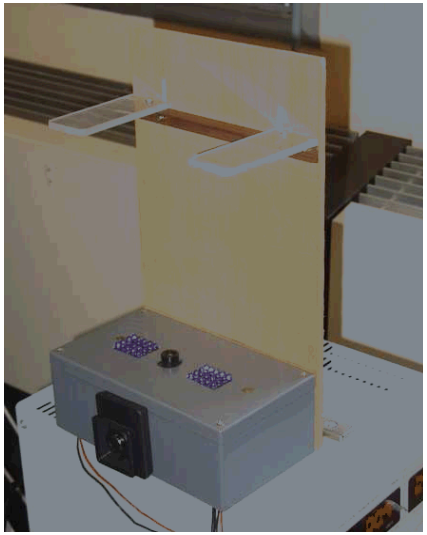
- 1 seule image de l'individu
- acquisition non contrôlée (détection du visage)
- EER = 4% en mode opérationnel

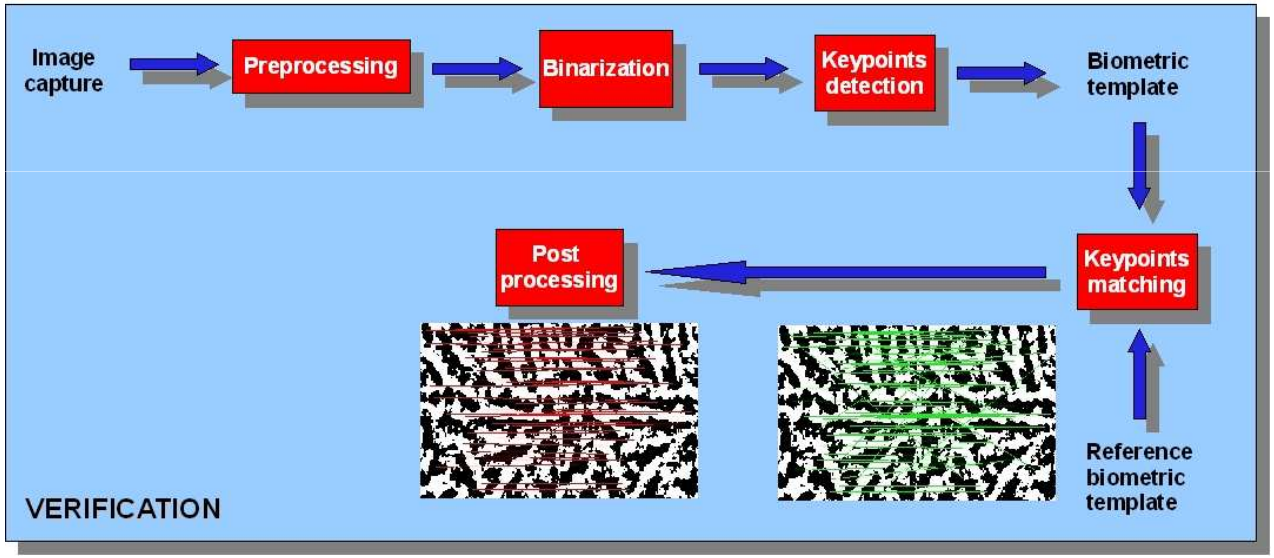


C. Rosenberger, L. Brun "Similarity-Based Matching for Face Authentication", IEEE International Conference on Pattern Recognition (ICPR), 2008.

Authentification par le réseau veineux de la main :

1 seule image de l'individu à l'enrôlement
EER = 0% sur une base de 24 personnes





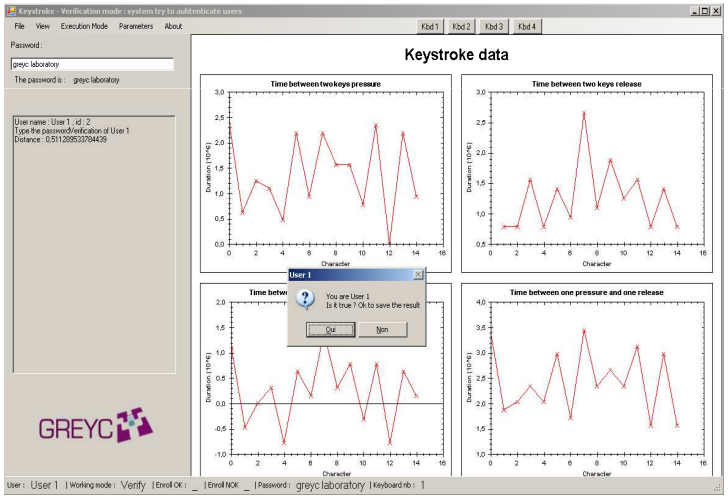
P.-O. Ladoux, C. Rosenberger, B. Dorizzi, "Hand Vein Verification System based on SIFT matching", The 3rd IAPR/IEEE International Conference on Biometrics (ICB), 2009.

Authentification par dynamique de frappe au clavier

Utilisation des temps de pression, de relâchement et de vol lors de la saisie d'un mot de passe.

5 acquisitions à l'enrôlement

EER = 6% sur une base de 100 personnes



R. Giot, M. El-Abed, C. Rosenberger, "Keystroke Dynamics With Low Constraints SVM Based Passphrase Enrollment",IEEE Third International Conference on Biometrics : Theory, Applications and Systems (BTAS), Washington DC USA, Sept. 28-30, 2009

Evaluation de systèmes biométriques

Qu'est ce qu'un bon système biométrique ?

- **performance :** erreur minimale, rapidité de la vérification..

- **acceptabilité** : confiance, facilité d'usage…

- **sécurité** : référence biométrique difficile à dupliquer, failles logicielles et matérielles…

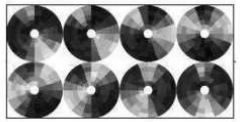
→ Rapport d'expertise d'un système donné

M. El-Abed, R. Giot, B. Hemery, C. Rosenberger, "A study of users' acceptance and satisfaction of biometric systems", IEEE International Carnahan Conference on Security Technology (ICCST), 2010.

Biométrie révocable :

Image originale

Extraction de paramètres



Fingercode

seed

BioHashing

Salage

- ❑ L'image originale n'est pas stockée
- ❑ Le biocode est stocké
- ❑ Impossible de retrouver l'image à partir du biocode
- ❑ Un biocode peut être regénéré
- ❑ Le procédé améliore la performance

$m \leq n$

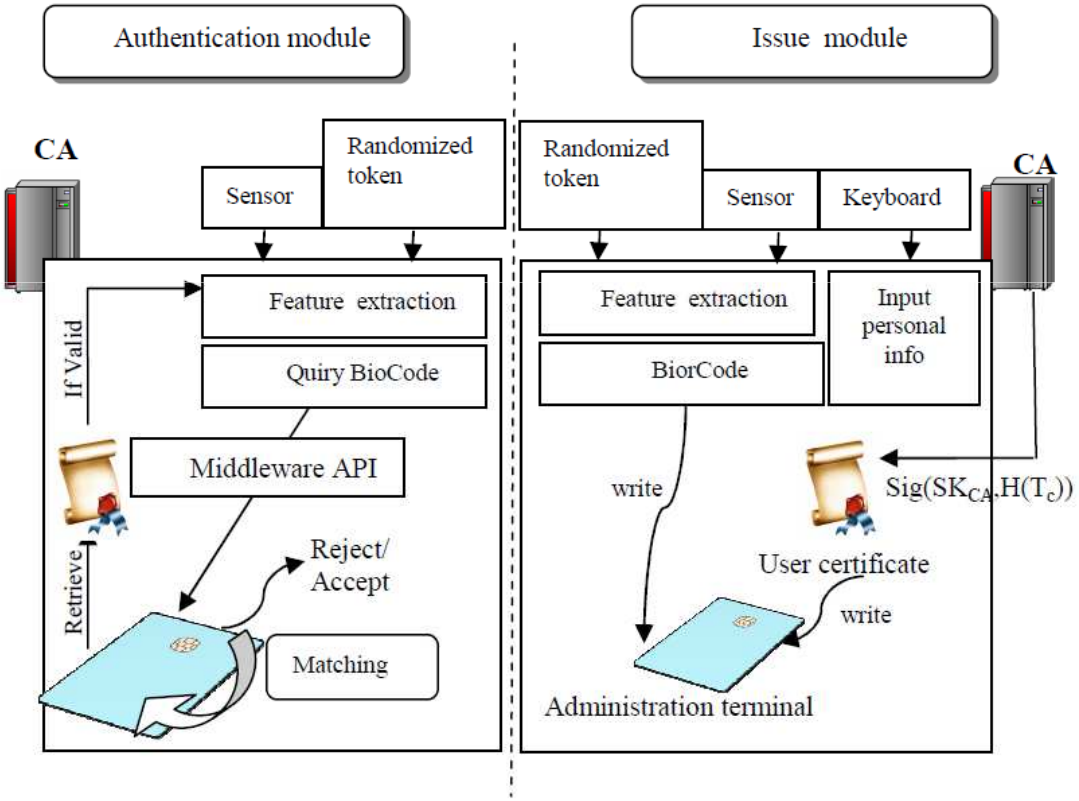
$b_i \in \{0,1\}$

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

BioCode

R. Belguechi, C. Rosenberger, S. Ait Aoudia, "BioHashing for securing fingerprint minutiae templates", International Conference on Pattern Recognition (ICPR), 2010.

Stockage et traitement sécurisé d'une donnée biométrique révocable



- Stockage sur carte à puce
- Calcul d'un biocode
- Vérification dans la carte
- Architecture Global Platform

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

PLAN

- Motivations
- Les principes de la biométrie
- Les enjeux de la biométrie
- Les activités de recherche au GREYC

Conclusion

- **Intérêt** : Relation étroite entre le client et son authentifiant

- **Inconvénients** :
  - performance (EER>0%)
  - aspects juridiques et éthiques
  - acceptation des utilisateurs

- **Perspectives** :
  - améliorer les algorithmes
  - protéger la vie privée des utilisateurs
  - favoriser l'acceptation par les utilisateurs

Christophe Rosenberger
christophe.rosenberger@ensicaen.fr