Techniques et Usages Biométriques

Bernadette Dorizzi

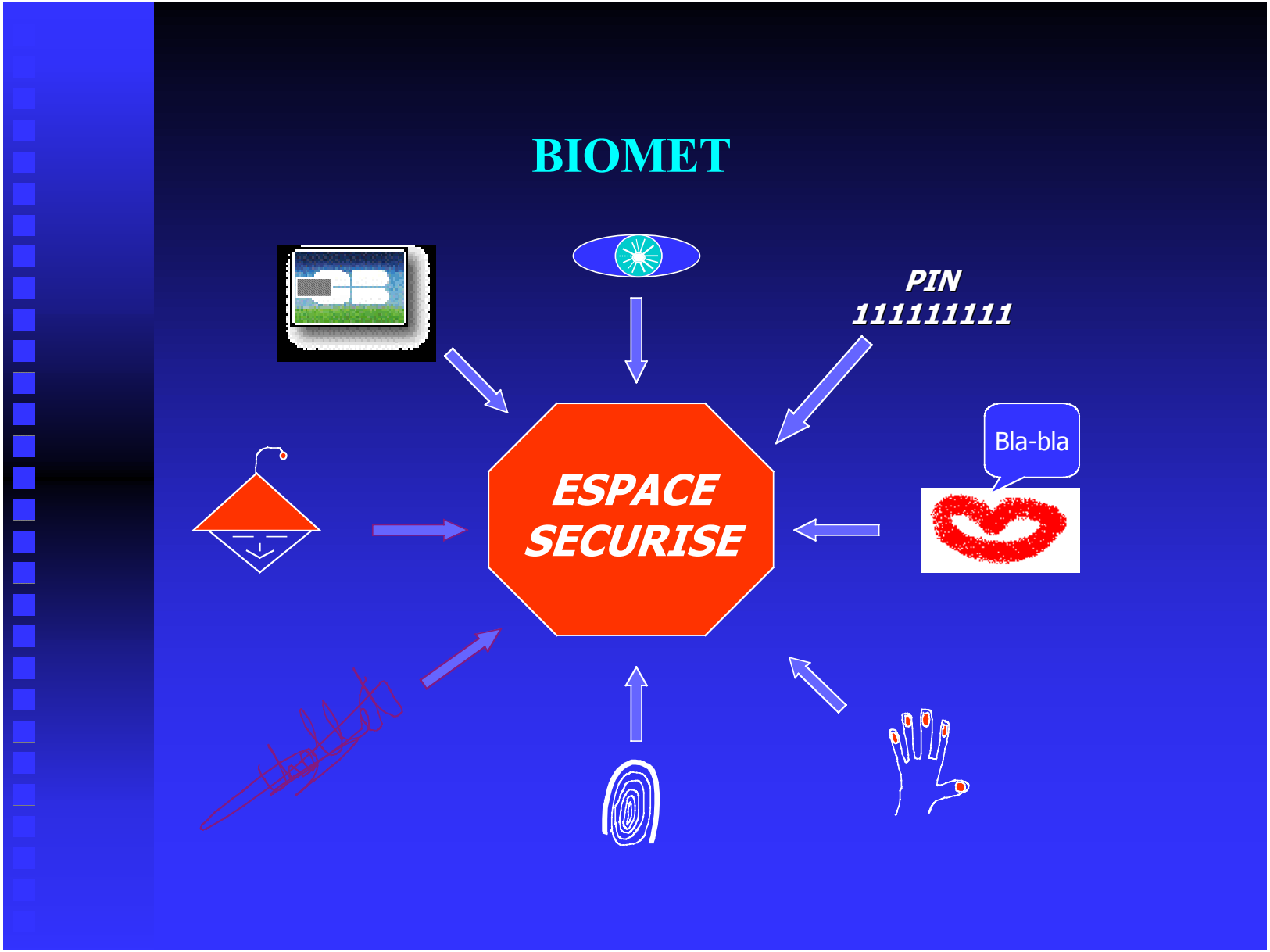
GET/INT Evry

Bernadette.Dorizzi@int-evry.fr

La Biométrie

Vérifier l'identité d'une personne à l'aide d'une ou plusieurs modalités qui lui sont propres (voix, iris, empreintes digitales, visage …)

- Pourquoi la Biométrie ?
  - Besoins accrus en terme de sécurité
  - Les systèmes de vérification standards : cartes à codes, badges magnétiques présentent des inconvénients : perte, vol, falsification
  - L'usage de la biométrie reste encore très limité: problème d'acceptabilité, de performances, d'usages, de législation...
- Un essor nouveau dû aux nouvelles dispositions au niveau de la circulation transfrontalière des personnes : vers le passeport et les visas biométriques


BIOMET
PIN
111111111
Bla-bla
ESPACE
SECURISE

Qu'est ce que l'identification?

- Reconnaissance d'un individu produisant une annonce (ex. une signature, une phrase parlée...), parmi *N* individus
- Classification à *N* classes

Qu'est ce que la vérification?

- Plus simple: problème de classification à 2 classes
- Vérifier si l'identité qu'une personne a annoncée est vraie ou fausse

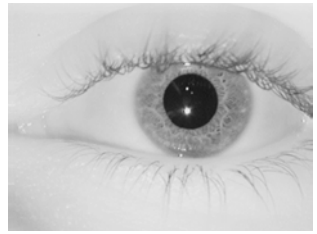
Système de vérification

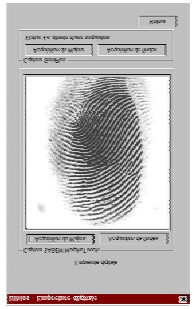
Le problème de la vérification

- On est en présence d'un certain nombre de personnes:clients (ex. banque)
- On dispose d'un nombre limité de « signatures » de référence de chaque client
- Etant donné une personne, elle déclare son identité comme celle d'un des clients
- Problème : cette personne est elle bien le client qu'elle prétend être ou est-elle un imposteur?

Une « signature »
se prétendant
être celle de X

→ Image, signal





↓

Suite de vecteurs de caractéristiques: gabarit

Représentation comprimée de la forme à partir de laquelle sera faite la comparaison

Apprentissage enrôlement

Utilisation des exemples
de la signature de X pour apprendre
un modèle qui sera associé à X

Reconnaissance

La « signature » est présentée
en entrée du modèle de X.
A l'aide d'un algorithme de mise en correspondance et d'un seuil, on va décider si elle appartient à X ou pas.

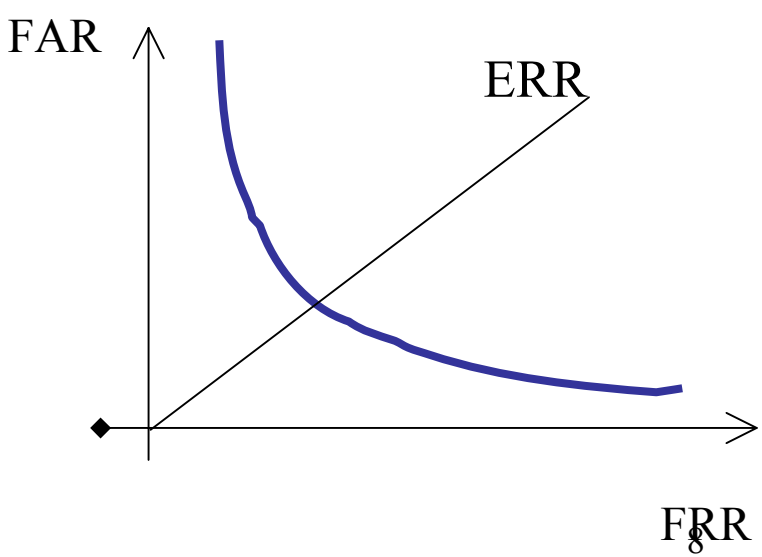
Comment mesurer les performances d'un tel système?

- Les erreurs que l 'on peut faire sont de deux sortes:
  - FR=False Rejection : rejeter faussement un client
  - FA=False Acceptation : accepter faussement un imposteur

$$FRR = \frac{\text{Nb de FR}}{\text{Nb de clients}}$$

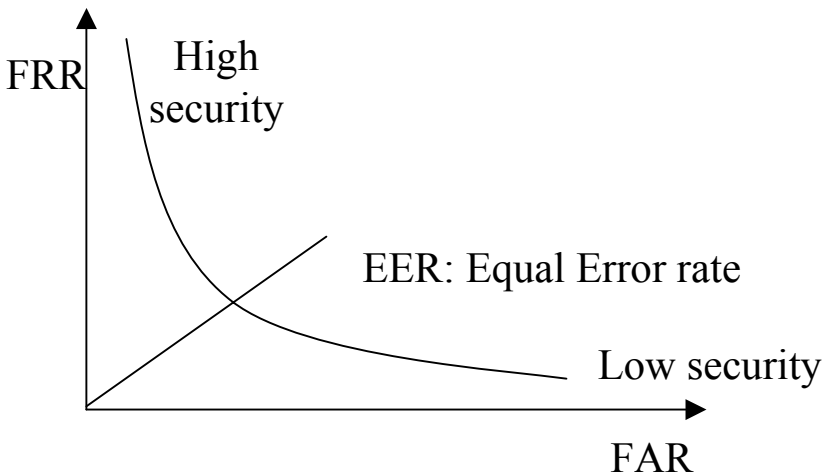
$$FAR = \frac{\text{Nb de FA}}{\text{Nb imposteurs}}$$

$$TER = \frac{\text{Nb de FR} + \text{Nb de FA}}{\text{Nb total d'accès}}$$

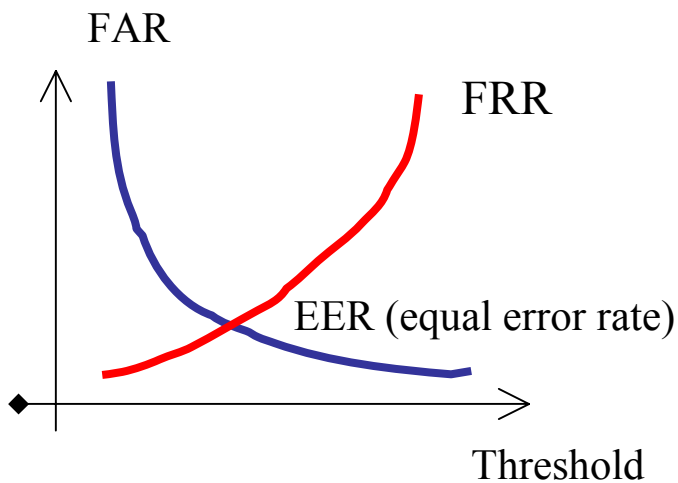


Performance curves

ROC curve



In order to make a decision a threshold has to be settled



Stockage des données biométriques Identification/Vérification

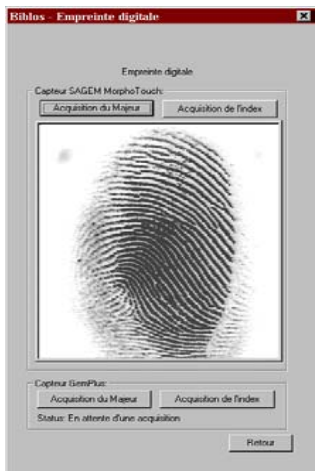
- L'identification nécessite le stockage centralisé ou local des gabarits dans des bases de données et des algorithmes permettant de chercher un élément dans ces grandes bases de données
- La vérification peut se faire sans accès à de grandes bases de données, en préservant l'anonymat (par exemple si on stocke les gabarits cryptés sur une carte à puce)
- Risque de falsification (lentilles de contacts, faux doigts etc…) Plusieurs systèmes prennent maintenant en compte ces risques : détection des vrais v.s. faux doigts, yeux qui se rétractent à la lumière, chaleur des doigts …

Les différentes modalités biométriques

- Une seule modalité ne suffit pas:
  - Il y a des personnes réfractaires pour chaque modalité
  - Selon les situations d'usage, une modalité sera plus adaptée qu'une autre
  - Il y a aussi des critères de coût à mettre en relation avec les objectifs visés
  - Les performances peuvent être encore insuffisantes pour une utilisation large
- Une voie à explorer : la multimodalité

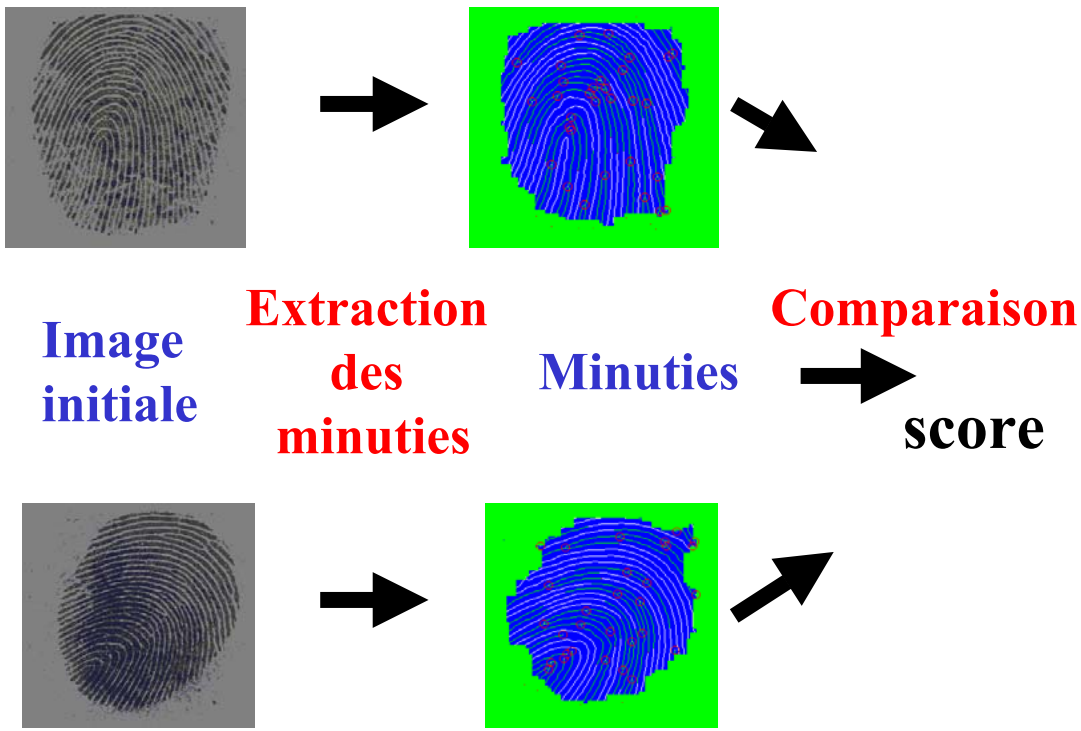
Empreintes digitales

- Technologie la plus ancienne et la plus répandue
- Il existe différents types de capteurs, plus ou moins chers, plus ou moins robustes aux impostures (faux doigts)
- Ce sont les performances du couple (capteur-algorithme) qui devraient être vérifiées et ceci en fonction du contexte d'utilisation

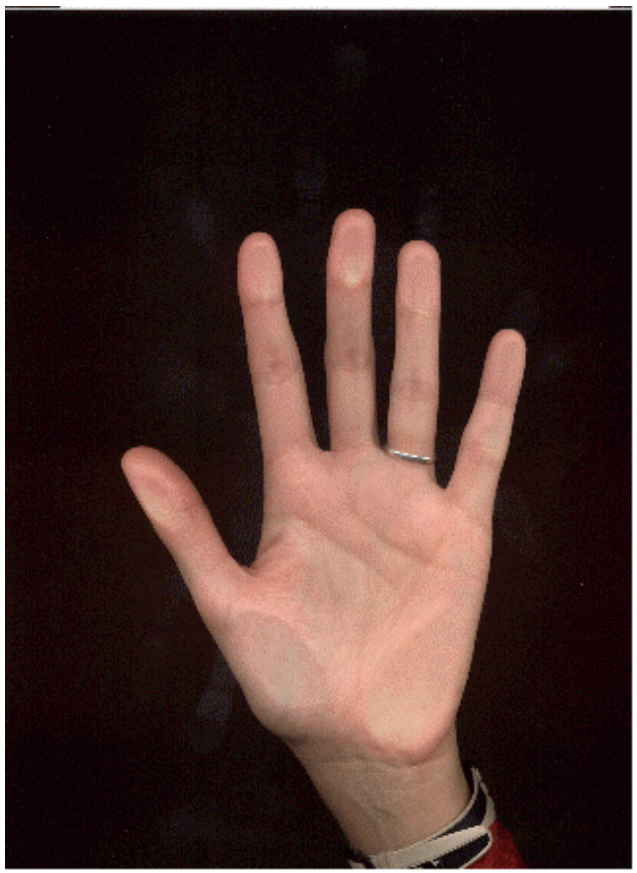


Identification
Coopérative
moyennement intrusive
Laisse des traces
Relativement Variable
Tres fiable : *FAR entre 0,005 et 0,1%*
FRR entre 0,01 et 0,2%

Empreintes : traitement



Forme de la main

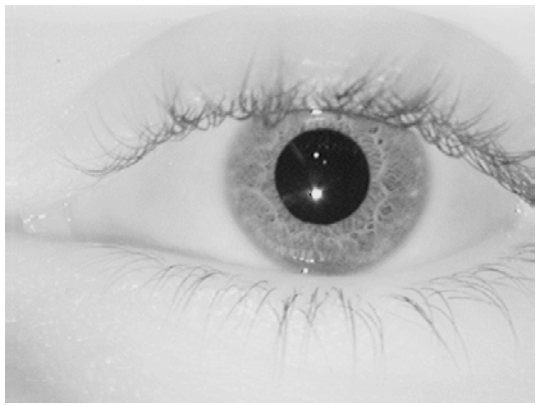


Contour de la main, mais aussi épaisseur et éventuellement le réseau veineux

Authentification
Coopérative
Peu intrusive
Peu de traces
Relativement variable
Relativement fiable
FAR autour de 0,1%
FRR autour de 0,1%

Souvent préféré aux empreintes mais moins fiable et plus variable dans le temps

Iris



Identification
Coopérative
Intrusive
Très stable
Très fiable
FAR : 0,0001%
FRR entre 0,25 et 0,5%

- En Asie, l'iris est préféré aux empreintes digitales
- Technologie assez coûteuse/ images en proche infra-rouge
- Un secteur assez fermé (existence de brevets)

Le visage

Authentification
Coopérative ou pas
Bien acceptée/naturelle
Très Variable
Peu fiable
FAR entre 0,3 et 5%
FRR entre 5 et 45%

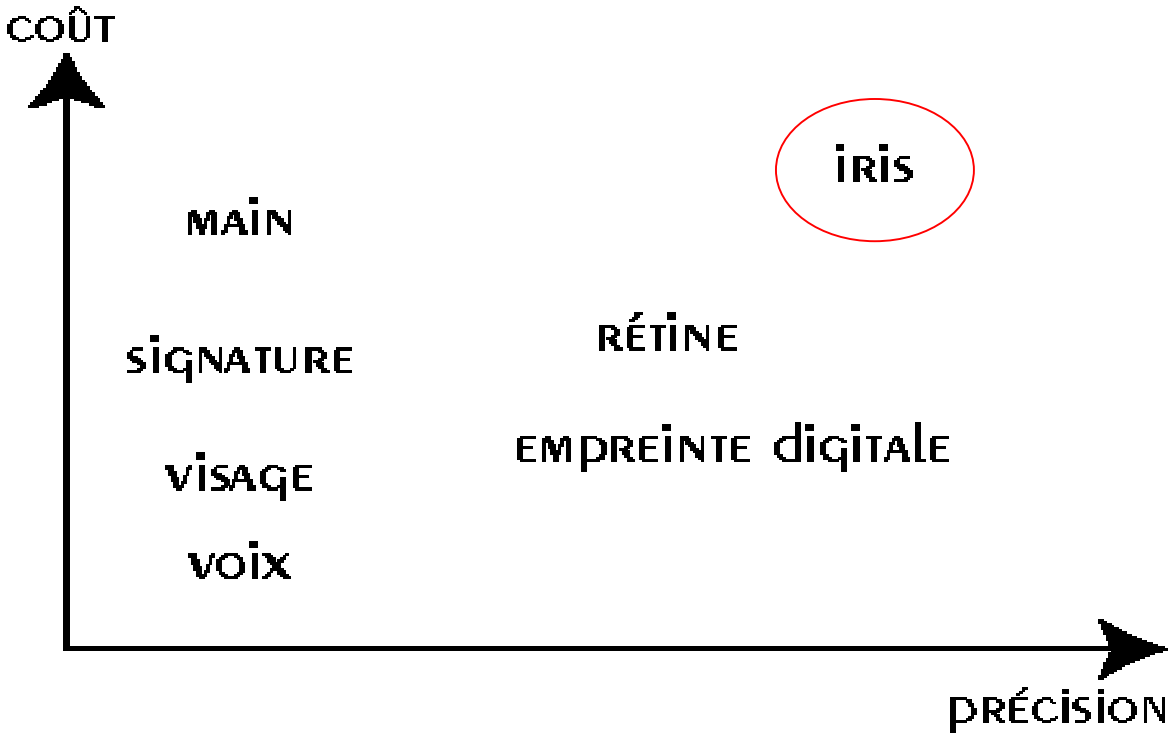
Beaucoup de recherche en cours en ce moment
Une grande compétition organisée par NIST : FRVT
Des premières expériences décevantes en identification à partir de séquences vidéo (aéroport de Boston, Tampa-Floride, Newham (banlieue de Londres)…)

La voix

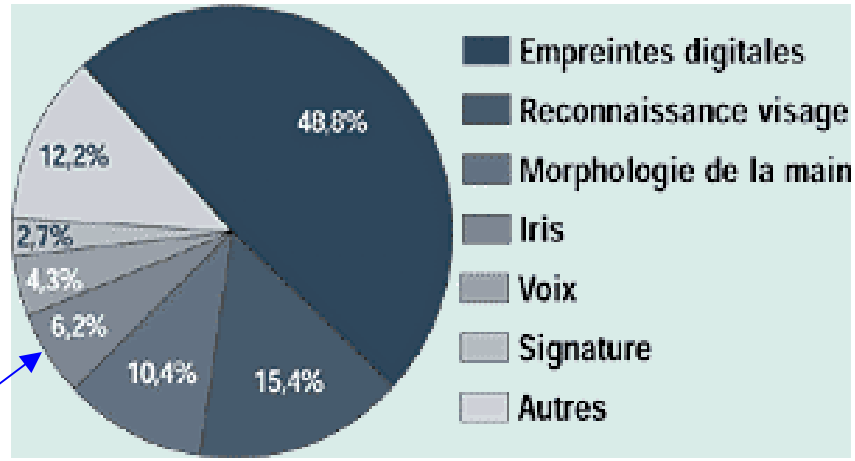
Authentification
Coopérative ou pas
Bien acceptée/ naturelle
Intérêt : authentification lors des communications téléphonique ou sur internet
Relativement Variable
Peu fiable (imposteurs)

Etudes en cours sur le couplage voix/visage

Comparaison des différents systèmes

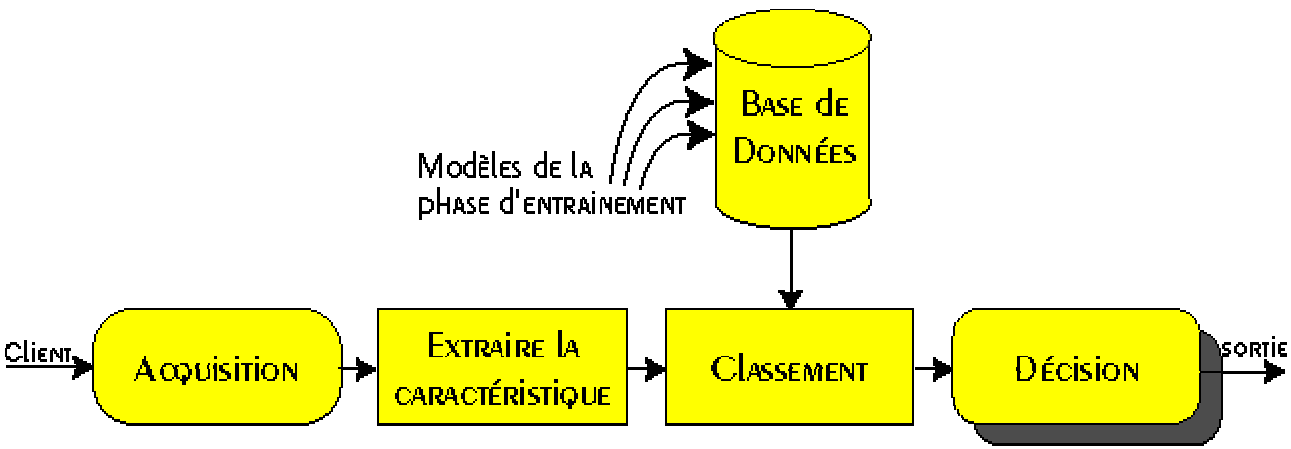


- Distribution du marché des systèmes biométriques pour 2001



Iris

- Modèle d'un système Biométrique



Limites des systèmes unimodaux

- Des défauts
  - Bruit d'acquisition :
    - Dûs à la personne (rhume pour la voix, blessure au doigt etc.)
    - Capteurs défectueux ou sales, illumination en imagerie
  - Variations intra-classes :
    - Différence entre les conditions d'enrôlement et de test
    - Problème d'interopérabilité
  - Limite de la capacité discriminante
  - Non universel : individus réfractaires à l'enrôlement
  - Imitations, Faussaires

Vers des Systèmes Multimodaux

- Modalités intrusives (iris, empreintes digitales) plutôt fiables , versus modalités non intrusives (visage, voix, signatures dynamiques) moins performantes
- Utilisation alternative : s'adapter aux situations d'usage
- Utilisation conjointe :
  - Fiabiliser les performances
  - Mieux résister aux imposteurs
  - Meilleure capacité d'enrôlement

Les applications possibles

- Lutte contre la criminalité (police)
  - Identification/authentification
  - Empreintes digitales (traces), ADN
- Délivrance et usage des droits institutionnels (Etats) (Visas, passeports,)
  - Grosses bases de données, besoins d'identification élevés
- Produits commerciaux de contrôle d'accès physique (bâtiments, aéroports) et logique (PC, transactions sur internet)
- Personnalisation d'environnements

Evaluation des algorithmes biométriques

- Nécessite des bases de donnée de taille suffisante en fonction de ce que l'on veut tester ainsi que des protocoles associés et des systèmes de référence
- Plus ou moins avancée selon les modalités :
  - (en Parole ou Visage existance de campagnes d'évaluation proposées par NIST depuis longtemps,
  - en signature ou forme de la main, cela n'existe pas.
- Un effort dans ce sens : le réseau d'excellence BioSecure, coordonné par l'INT

Evaluation des systèmes biométriques

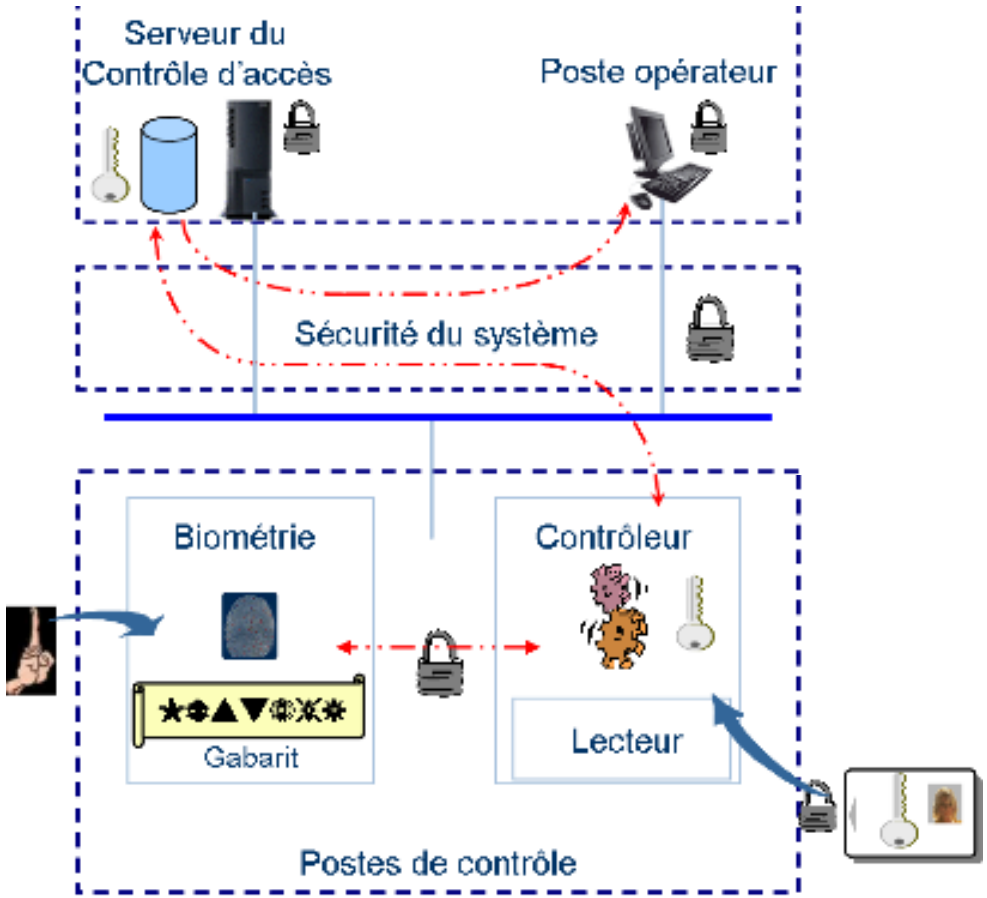
Très difficile car peu de standards et dépendant du contexte

- Evaluation théorique *:*
  - *Mesure de taux d'erreur* : les taux fournis par les brochures correspondent souvent aux performances des algorithmes seuls et rarement aux taux en situation opérationnelle
  - *Veille technologique* nécessaire : les techniques évoluent rapîdement
  - *Choix des équipements (coût, qualité, robustesse)*
- Evaluation pratique :
  - Protocole pour évaluer l'adéquation du système avec l'utilisation qui doit en être faite / tests sur un petit nombre d'utilisateurs
  - Critères à prendre en compte :
    - Convivialité (qualité de l'interface, temps de réponse, facilité d'enrôlement)
    - Réalité des performances
    - Fonctionnement en situations extrêmes
    - Résistance à la fraude

Protection des systèmes biométriques

- La sécurisation d'un système biométrique repose sur un ensemble de dispositifs depuis la capture de la caractéristique biométrique jusqu'à la gestion centralisée des données

Sécurisation dans un système de contrôle d'accès: protection des données du serveur, contrôle d'accès aux postes opérateurs, protection et chiffrement des communications, cryptage des données stockées dans le badge.



Cadre juridique : protection des données personnelles

- Directive européenne 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- En France, pas encore de loi correspondant à cette directive . La CNIL émet des avis au cas par cas.
- L'exemple québecois : en 2001, nouvelle loi sur les technologies de l'information dans laquelle des dispositions spécifiques sur la biométrie ont été incluses
- Aux USA : la législation en matière de protection des données personnelles est embryonnaire et la préoccupation sécuritaire est prioritaire. Plusieurs expérimentations de vidéosurveillance et reconnaissance faciale ont été réalisées. Existence d'associations assez actives mettant l'accent sur les dysfonctionnements des techniques biométriques

Biométrie : Quel avenir?

Besoins

- **Contrôle d'accès**
- **Systèmes d'information**
- **Etat / Administration**

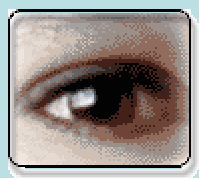
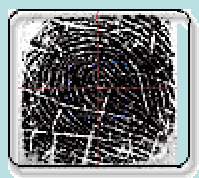



Moyens

La biométrie évite :

Copie, Perte, Oubli et Vol



Voix Visage Iris Empreinte

Limitations

- Coûts élevés
- Réticences publiques
- Manque d'information
- Barrières juridiques (CNIL...)