




Authentification biométrique (Systèmes et usages)

Plan

- **Introduction à l'authentification biométrique**
 - **Architecture technique des systèmes biométriques**
 - **Sécurité, attaques et résilience des systèmes biométriques**
 - **Usages, législation et enjeux éthiques**
- 

Introduction à l'authentification biométrique

- **Objectifs**

- Comprendre les concepts fondamentaux de l'authentification biométrique.
- Distinguer les types de biométries (biologiques, physiques vs comportementales).
- Identifier les critères de qualité d'un système biométrique.
- Interpréter les courbes d'évaluation : FAR, FRR, EER.

Introduction à l'authentification biométrique

- **Introduction**

- **Contexte de la cybersécurité** : montée des besoins en authentification fiable.
- **Limitations des méthodes traditionnelles** (mots de passe, cartes).
- **Arrivée de la biométrie** : usage massif dans téléphones, e-gates, paiements...

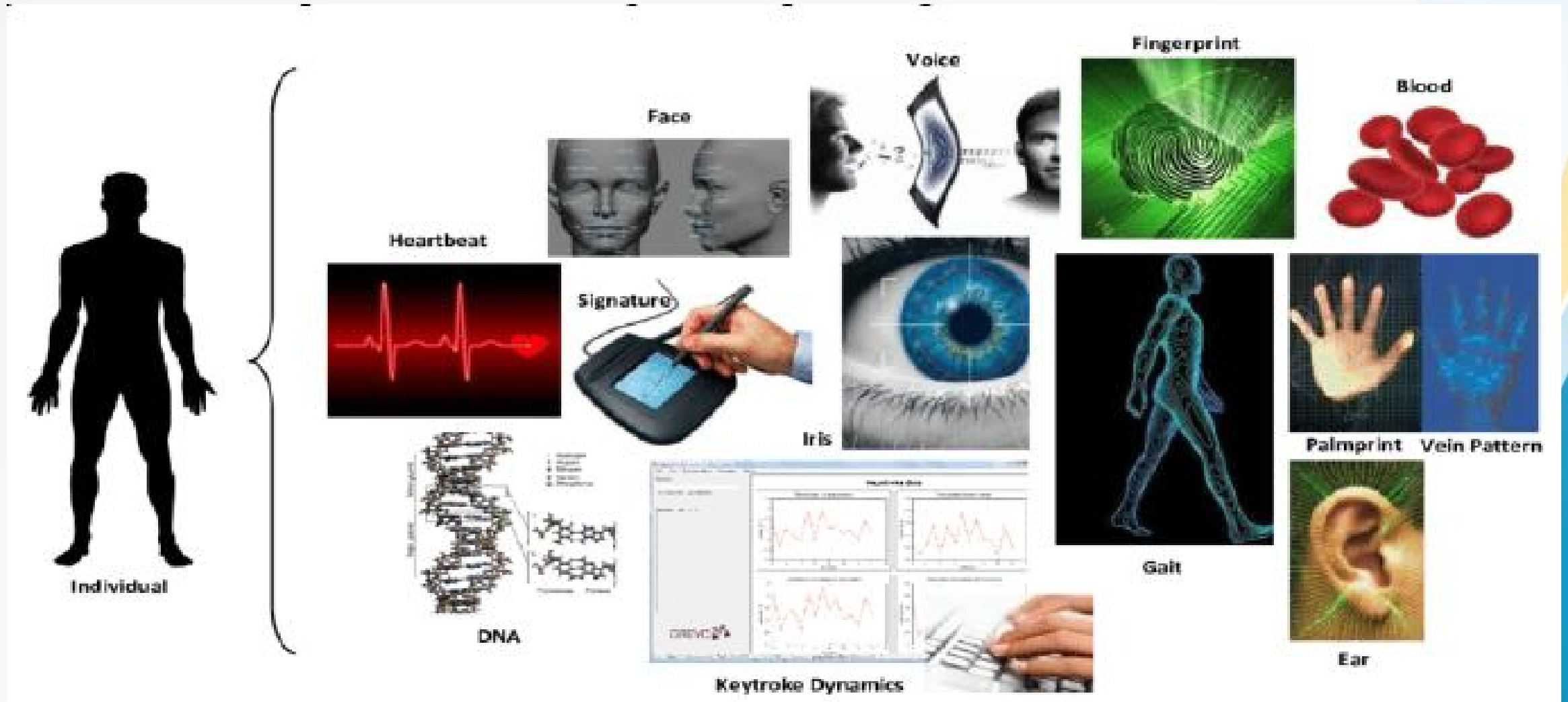
Introduction à l'authentification biométrique

- **Définitions fondamentales**

- **Identification** : Qui est-ce ? $\rightarrow 1:N$
- **Authentification** : Est-ce bien cette personne ? $\rightarrow 1:1$
- **Biométrie** : ensemble des techniques qui permettent d'identifier ou d'authentifier une personne à partir de caractéristiques physiques ou comportementales uniques.

Introduction à l'authentification biométrique

- Types de biométries



Introduction à l'authentification biométrique

- **Types de biométries et capteurs associés**

Type de biométrie	Catégorie	Capteur ou dispositif utilisé
Empreinte digitale	Physique	Capteur d'empreinte (optique, capacitif, à ultrasons)
Reconnaissance faciale	Physique	Caméra RGB, caméra infrarouge, capteur 3D (ex : FaceID)
Iris	Physique	Caméra infrarouge haute résolution
Rétine	Physique	Scanner de rétine (analyse du réseau vasculaire)
Forme de la main	Physique	Scanner de main (3D ou infrarouge)
Veines (paume/doigt)	Physique	Caméra à lumière proche infrarouge (Near-Infrared, NIR)
Voix	Comportementale	Microphone, capteur audio
Signature dynamique	Comportementale	Tablette graphique (capture pression, vitesse, rythme)
Frappe clavier	Comportementale	Clavier classique + logiciel d'analyse comportementale
Démarche (gait)	Comportementale	Caméras vidéo, capteurs inertiels (IMU) ou capteurs au sol

Introduction à l'authentification biométrique

- **Types de biométries**

- **Biologiques :**

- Salive
 - ADN

- **Physiques (Morphologiques) :**

- Empreinte digitale
 - Iris
 - Rétine
 - Visage
 - Forme de la main

- **Comportementales :**

- Voix
 - Signature dynamique
 - Frappe clavier (keystroke dynamics)
 - Démarche (gait)

Introduction à l'authentification biométrique

- **Propriétés d'un bon système biométrique**

- **Universalité** : tout le monde en dispose ?
- **Unicité** : est-elle propre à chaque individu ?
- **Permanence** : reste-t-elle stable dans le temps ?
- **Collectabilité** : peut-elle être mesurée facilement ?
- **Performance** : rapidité, précision
- **Acceptabilité** : les utilisateurs sont-ils prêts à l'utiliser ?
- **Résistance à la fraude (sécurité)** : peut-on la contourner ?

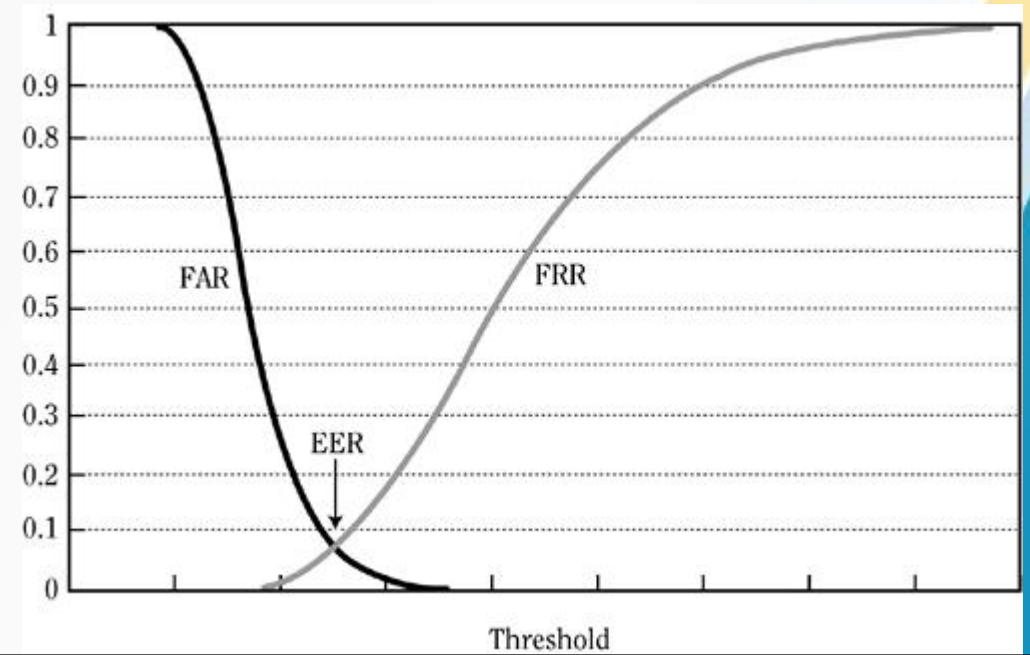
🗣️ *Activité en binôme : évaluer 3 biométries selon ces critères*

Introduction à l'authentification biométrique

- **Évaluation des performances**

- **FAR** (False Acceptance Rate) : taux d'acceptation d'un imposteur
- **FRR** (False Rejection Rate) : taux de rejet d'un utilisateur légitime
- **EER** (Equal Error Rate) : point d'équilibre $FAR = FRR$
- **Courbe ROC** : courbe qui trace FAR vs FRR
- **Seuil** : Valeur définie pour valider la prediction du modèle.

⚠ **Discussion** : Que choisir entre plus de sécurité ou plus d'accessibilité ?



Introduction à l'authentification biométrique

- **La biométrie et les méthodes d'authentification traditionnelles (O'Gorman)**

Authentification biométrique	Authentification par mot de passe/clé
<ul style="list-style-type: none">- basée sur des mesures morphologiques, comportementales ou biologiques- utilisation facile (pas de secret à retenir)- authentifie l'individu- l'information est en relation étroite à l'utilisateur de façon permanente- utilise une comparaison probabiliste- l'information biométrique peut être modifiée et/ou altérée avec le temps, il est incertain- problème de respect de la vie privée- difficile de révoquer l'information	<ul style="list-style-type: none">- basée sur que <i>l'on sait</i> ou <i>possède</i>- pouvant être plus compliquée (mots de passe complexe)- authentifie la clé- il peut être perdu, volé ou oublié- utilise une comparaison exacte- l'information ne varie pas, elle est sûre- moindre impact sur la vie privée- changement aisé

Introduction à l'authentification biométrique

- **Limitations des systèmes biométriques**

- 1. Performance (moins précis)**
- 2. Contraintes d'utilisation (ex : empreintes digitales \Leftrightarrow l'identification de criminels)**
- 3. Vulnérable aux attaques (ex : reproduire des empreintes digitales en utilisant des images résiduelles sur le capteur).**

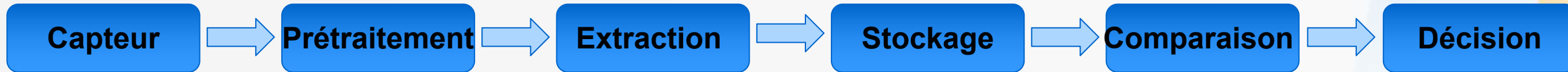
Introduction à l'authentification biométrique

- **Mini-quiz**

- Quelle est la différence entre identification et authentification ?
- Donnez un exemple de biométrie physique et un comportementale.
- Que signifie EER ?
- Pourquoi l'empreinte digitale est-elle couramment utilisée ?

Architecture technique des systèmes biométriques

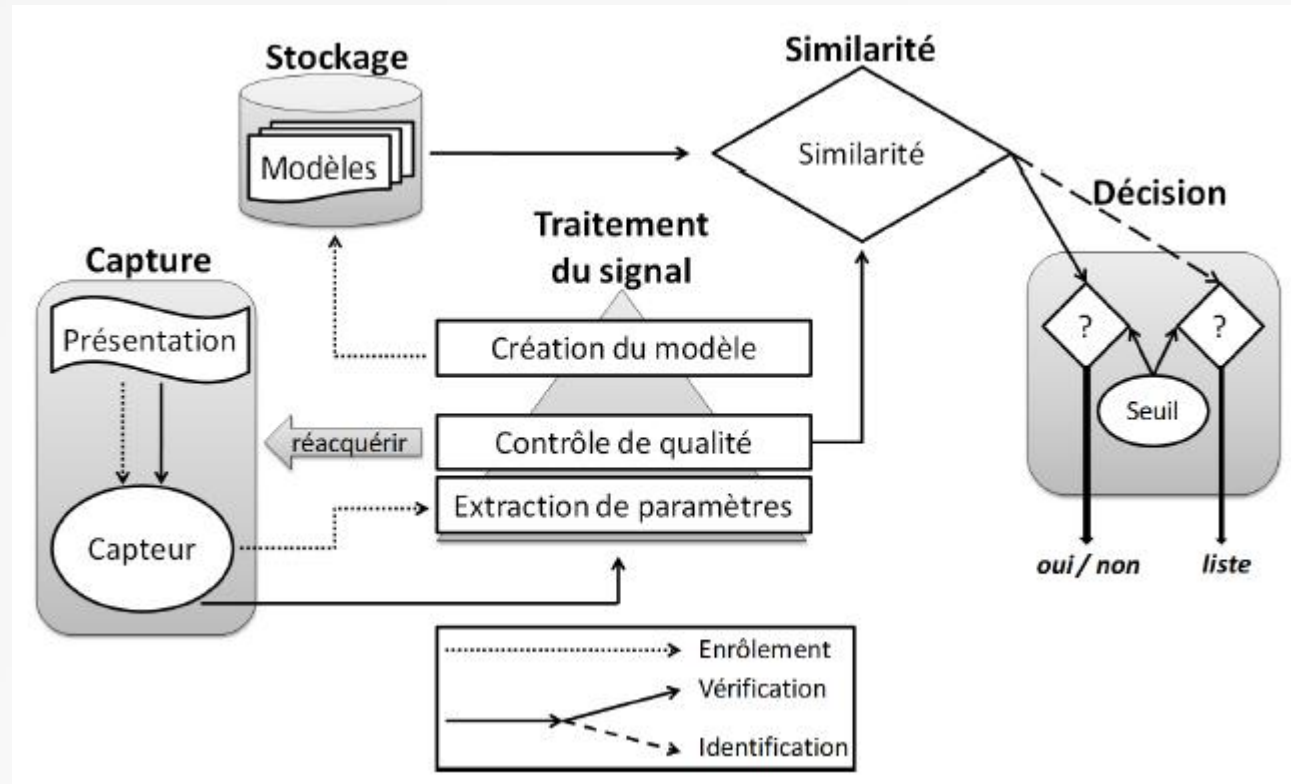
- **Architecture d'un système biométrique**



- **Capteur** : capture l'image brute (ex: caméra, scanner d'empreinte)
- **Prétraitement** : amélioration (nettoyage, centrage, redimensionnement...)
- **Extraction** : calcule un vecteur caractéristique (feature vector)
- **Stockage** : modèle (ou "template") enregistré dans une base sécurisée
- **Comparaison** : distance entre le modèle stocké et celui extrait
- **Décision** : acceptation ou rejet selon un seuil

Architecture technique des systèmes biométriques

- Architecture d'un système biométrique



Sécurité, attaques et résilience des systèmes biométriques

- **Risques et défis spécifiques à la biométrie**

- Irrevocabilité des données biométriques : on ne peut pas “changer de visage”
- Vol de gabarits biométriques : accès à la base = compromission durable
- Dérives possibles :
 - Surveillance massive (ex : Chine)
 - Reconnaissance faciale sans consentement
 - Discrimination algorithmique

⚠ **Discussion ouverte** : la biométrie est-elle trop “dangereuse” pour certains usages ?

Sécurité, attaques et résilience des systèmes biométriques

- **Typologie des attaques**

- Spoofing (usurpation biométrique)
 - Empreinte moulée (gélatine, silicone)
 - Masque 3D ou photo
 - Enregistrement vocal
- Attaque par injection
 - Image modifiée injectée dans le système (replay attack)
- Reconstruction inverse
 - À partir d'un modèle biométrique → tentative de reconstituer l'image d'origine (ex : empreinte à partir d'un template)
- Attaques sur les bases de données
 - Accès aux modèles stockés
 - Attaque sur les communications (interception des données biométriques)

Sécurité, attaques et résilience des systèmes biométriques

- **Contre-mesures et résilience**

- Détection de vivacité (Liveness Detection)
 - Détection de clignement, texture de peau, micro-mouvements
 - Challenge-réponse pour la voix
- Fusion biométrique (Multimodal)
 - Empreinte + visage + mot de passe
 - Plus difficile à usurper
- Chiffrement des gabarits
 - Gabarit non inversible
 - Technique : Fuzzy vault, Cancelable biometrics
- Audit et surveillance
 - Journaux d'accès, détection d'anomalies
 - Analyse comportementale complémentaire

Conclusion : sécurité biométrique \neq sécurité parfaite \rightarrow elle nécessite des couches défensives multiples.

Sécurité, attaques et résilience des systèmes biométriques

- **Mini-Quiz**

- *Citez deux types d'attaques contre un système biométrique.*
- *Quelle est la principale limite de l'usage d'une empreinte digitale comme identifiant unique ?*
- *Qu'est-ce que la "détection de vivacité" et pourquoi est-elle utile ?*
- *Qu'est-ce qu'une "attaque par reconstruction inverse" ?*
- *Expliquez en quoi le chiffrement des gabarits biométriques est important dans un système d'authentification.*

Sécurité, attaques et résilience des systèmes biométriques

- **Activité de groupe (débat)**
 - *Sujet : La reconnaissance faciale dans les lieux publics : sécurité ou intrusion ?*
 - *Groupes de 3-4 étudiants*
 - *Chaque groupe prépare un argumentaire pour ou contre*
 - *Présentation orale de 2 min / groupe*

Usages, législation et enjeux éthiques

- **Objectifs pédagogiques**

- *Identifier les principaux usages concrets de la biométrie dans les domaines publics et privés.*
- *Comprendre les enjeux juridiques, réglementaires et éthiques liés à l'usage de données biométriques.*

Usages, législation et enjeux éthiques

- **Usages réels des technologies biométrique**
 - *Dans le secteur public*
 - *Frontières et immigration : e-gates, passeports biométriques*
 - *Police et surveillance : reconnaissance faciale en temps réel*
 - *Vote électronique : tests en Afrique, Amérique Latine*
 - *Dans le secteur privé*
 - *Smartphones : Face ID, Touch ID, capteurs sous écran*
 - *Banques : authentification vocale / faciale pour les comptes*
 - *Contrôle d'accès en entreprise : badge biométrique, empreinte*

Usages, législation et enjeux éthiques

- **Cadre juridique national**

Le Burkina Faso dispose d'un cadre juridique et institutionnel encadrant les données personnelles:

- *Commission de l'Informatique et des Libertés (CIL) :*
 - *par la Loi N ° 010-2004/AN du 20 avril 2004 portant protection des données à caractère personnel.*
 - *Elle est devenue fonctionnelle en décembre 2007.*
 - *Site web : <https://cil.bf/>*

Usages, législation et enjeux éthiques

- **Mini-Quiz**

- *Citez un exemple d'usage de la biométrie au Burkina Faso.*
- *Quels sont les deux grands enjeux éthiques liés à l'usage de la reconnaissance faciale dans les lieux publics ?*