# Thème : La Biométrie

**Travail élaboré par :**
**Barry Alpha Mamadou Douah**
**Bessy Kouakou Desiré**
**Mohamed Sacko**

**Chargé du cours :**
**Mr Hamed Aouadi**

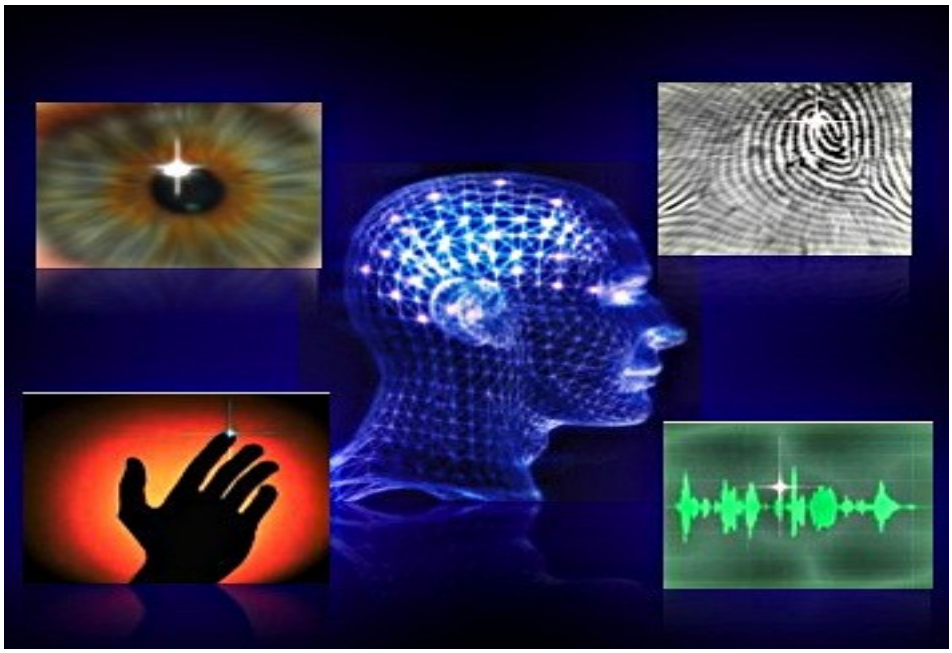
**Année Universitaire 2023-2024**

# I. INTRODUCTION A LA BIOMETRIE

**Qu’est ce que la biométrie**

La biométrie est une technique d’identification d’un individu au moyen de ses caractéristiques morphologiques : empreinte digitale, géométrie de la main, structure de l’iris ou de la rétine, le timbre de la voix, forme du visage etc…. Les caractéristiques sont choisies pour varier peu au cours de la vie de l’individu et être différents d’un individu à un autre (même pour des jumeaux).
Les lecteurs biométriques sont parmi les dispositifs de lecture les plus sûrs supprimant le risque d’oubli de code, de vol, duplication ou perte de carte que l’on retrouve sur les systèmes classiques. Grâce à ces techniques on est certain que la personne identifiée est bien celle prétendue être.

En d’autres termes,
La biométrie est une discipline technologique et scientifique qui se concentre sur l'identification des individus en se basant sur des caractéristiques biologiques et comportementales uniques. Cette méthode d'identification repose sur l'utilisation de caractéristiques intrinsèques à un individu, offrant une alternative aux méthodes traditionnelles basées sur des cartes d'identité, des codes PIN ou des mots de passe.



# II. OBJECTIFS DE LA BIOMETRIE

La biométrie vise principalement à identifier et à authentifier des individus en se basant sur des caractéristiques physiques ou comportementales uniques. Les objectifs principaux de la biométrie incluent :

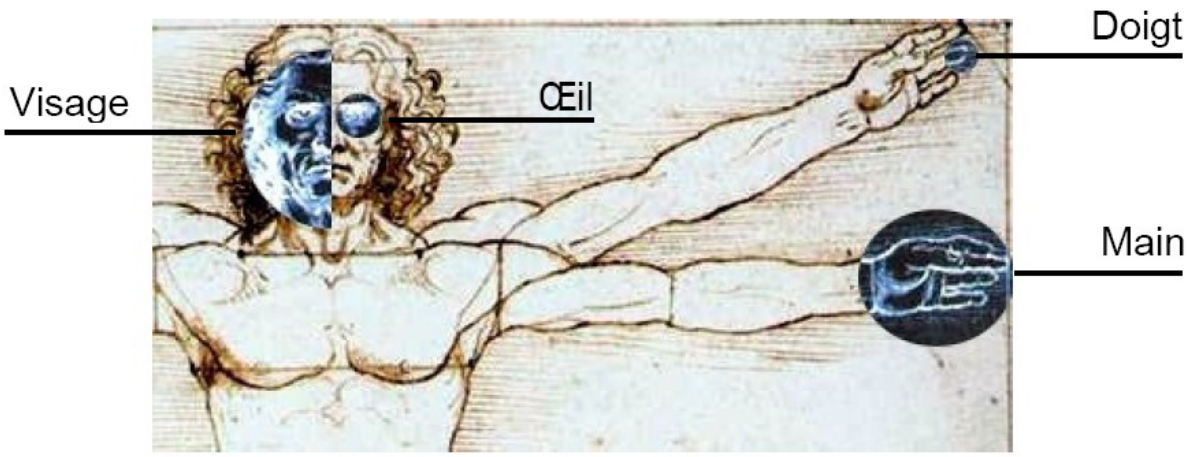
1. **Identification précise :** Utiliser des caractéristiques biométriques uniques, telles que les empreintes digitales, l'iris, la rétine, la voix, etc., pour identifier de manière précise et fiable les individus.
2. **Sécurité renforcée :** Améliorer la sécurité en remplaçant ou complétant les méthodes traditionnelles telles que les mots de passe, cartes d'identité ou clés par des caractéristiques biométriques plus difficiles à falsifier.
3. **Facilitation de l'accès :** Simplifier et accélérer les processus d'authentification, permettant aux individus d'accéder plus facilement à des lieux sécurisés, à des appareils ou à des informations sensibles.
4. **Prévention de la fraude :** Réduire les risques de fraude en rendant plus difficile la contrefaçon ou l'utilisation abusive d'identités.
5. **Protection de la confidentialité :** Assurer la confidentialité des données biométriques en utilisant des méthodes de stockage et de traitement sécurisées pour éviter leur utilisation abusive ou leur accès non autorisé.

# III. Les technologies biométriques

La biométrie utilise les caractéristiques physiques de certaines parties du corps humain. On trouve parmi les plus courantes :

Quelque soit le mode de reconnaissance la technique utilisée reste la même :

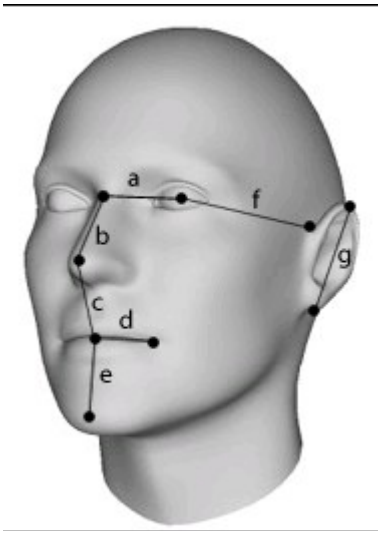
- Un capteur prend « une image » de l’empreinte.
- L’image est ensuite analysée par un logiciel de traitement d’image qui repère les points caractéristiques.
- L’ensemble de ces données est traité par un algorithme puis transformé en un code unique.
- Ce code sera délivré par le lecteur biométrique à l’unité de contrôle d’accès auquel il est raccordé.




## A.Visage (reconnaissance faciale)

Ce type de mesure consiste à faire une photographie du visage pour en extraire un ensemble de points caractéristiques propres à chaque individu. Ces points concernent des zones du visage tel que les coins de la bouche, la distance entre les orbites des yeux, la longueur du nez, etc.

Utilisation : aéroport



## B.Œil (scan de l'iris & de la rétine)

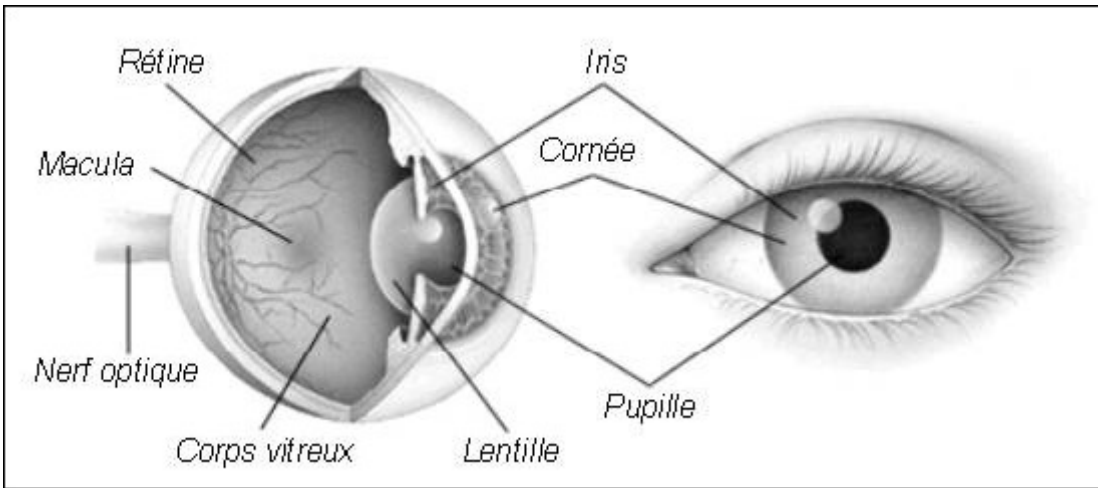
L'analyse de l'œil utilise 2 techniques de mesure de 2 parties de l'œil : l'iris et la rétine.

**Iris**

L'iris est la zone colorée visible entre le blanc de l'œil et la pupille. L'iris est un réseau de tubes fins dont l'enchevêtrement varie très peu durant la vie de l'individu contrairement à la couleur (des tubes) qui varie un peu avec le temps.

**Rétine**

La rétine est la pellicule photosensible située au fond de l'œil. Cette technique utilise les dessins formés par les vaisseaux sanguins de la rétine unique pour chaque individu et assez stable durant la vie de la personne.




## C.Empreinte digitale

Ce type de mesure exploite le dessin représenté par les crêtes et sillons de l'épiderme des doigts. Ce dessin est unique et différent pour chaque individu. On en extrait les caractéristiques principales (Extraction des minuties) telles que les bifurcations de crêtes, les "îles", les lignes qui disparaissent, etc.

*- Empreintes digitales de différents individus*

## D.Veines du doigt

Hitachi a développé une technologie utilisant le réseau veineux des doigts de la main comme identifiant biométrique. Cette approche permet d'accroître la sécurité tout en préservant la vie privée des utilisateurs.

En effet, une telle technologie constitue une biométrie « sans trace » dans la mesure où les informations utilisées ne sont pas accessibles sans le libre consentement de son porteur.
Elle permet une augmentation accrue de la sécurité car les informations ne sont pas accessibles et donc capturables sans une participation volontaire de l'utilisateur.

## E.Géométrie de la main

Ce type de mesure consiste à prendre les dimensions de plusieurs caractéristiques de la main telle que la forme, longueur et largeur des doigts, formes des articulations, longueurs inter-articulations, etc.

### F.La voix

L'identification de la voix n'est pas intrusive et n'exige aucun contact physique avec le lecteur du système.

La plupart des systèmes d'identification de la voix utilisent l'affichage d'un texte, des mots spécifiques doivent être lus puis parlés afin de vérifier que la personne à authentifier est bien présente et qu'il ne s'agit pas d'un enregistrement.

Cette variabilité de la voie de chaque individu est utile pour différencier les locuteurs, est également mélangée à d'autres types de variabilité - variabilité due au contenu linguistique, variabilité intra-locuteur (qui fait que la voix dépend aussi de l'état physique et émotionnel d'un individu), variabilité due aux conditions d'enregistrement du signal de parole (bruit ambiant, microphone utilisé, lignes de transmission) - qui peuvent rendre l'identification du locuteur plus difficile.

Malgré toutes ces difficultés apparentes, la voix reste un moyen biométrique intéressant à exploiter car pratique et disponible via le réseau téléphonique comme la plupart de ses concurrents.

Enfin , nous avons aussi d'autres types de biométrie qui sont appelées Biométries comportementales
Exemple :
**Signature Dynamique :** Analyse des caractéristiques de la signature manuscrite.

**Analyse de la Frappe au Clavier :** Identification des utilisateurs par leur style de frappe.

## IV. Conclusion

En conclusion, la biométrie représente une avancée majeure en matière de sécurité informatique grâce à son potentiel d'authentification robuste et précise basée sur des caractéristiques uniques de chaque individu. Son adoption présente des avantages significatifs, notamment une meilleure protection contre la fraude, une simplification de l'expérience utilisateur et un renforcement de la sécurité globale des systèmes.

Cependant, son utilisation soulève également des défis, notamment en ce qui concerne la sécurité des données biométriques, la nécessité de garantir des protocoles de stockage et de traitement sécurisés, ainsi que la prise en compte des préoccupations liées à la vie privée.

La biométrie est une composante importante dans le paysage de la sécurité informatique, mais son déploiement efficace nécessite une approche équilibrée prenant en compte à la fois ses avantages et ses défis, tout en mettant l'accent sur la protection des données personnelles et la garantie d'une sécurité adéquate.