Chapitre 1

La biométrie

Sommaire

I. Introduction. 2
II. La biométrie. 3
a. Historique. 3
b. Définitions. 4
c. Intérêt 4
d. Les systèmes biométriques. 7
e. Performances d'un système biométrique. 8
f. Caractéristiques de la biométrie. 12
g. Types de reconnaissance par biométrie. 13
1. La reconnaissance comportementale. 14
2. La reconnaissance physiologique. 17
h. Comparaison des systèmes biométriques. 22
III. Conclusion. 26

Résumé

Ce chapitre propose une introduction générale à la biométrie. Il introduit la notion d'identité et les questions inhérentes à la reconnaissance d'un individu. Il présente ensuite les problématiques et contraintes liées à l'utilisation des systèmes automatiques de biométrie. Différentes modalités peuvent être utilisées afin de reconnaître un individu et sont présentées dans ce chapitre. La technique qui nous intéresse le long de ce mémoire est la biométrie par images rétiniennes. Une description brève et générale de cette technique est donnée. Finalement, et pour clore ce chapitre introductif, une analyse comparative des techniques biométriques est discutée.

I. Introduction.

De nos jours, l'authentification automatique des individus devient une approche primordiale dans le domaine de la sécurité et de contrôle d'accès au sein des infrastructures et des systèmes informatiques.

D'une part, la croissance internationale des communications, telle que Internet, tant en volume qu'en diversité (déplacement physique, transaction financière, accès aux services...), implique le besoin de s'assurer de l'identité des individus.

D'autre part, l'importance des enjeux motive les fraudeurs à mettre en échec les systèmes de sécurité existants.

Il y a donc un intérêt grandissant pour les systèmes électroniques d'identification et d'authentification. Leur dénominateur commun est le besoin d'un moyen simple, pratique, fiable et peu onéreux, pour vérifier l'identité d'une personne, sans l'assistance d'une autre personne.

Nous pouvons distinguer deux rôles essentiels de reconnaissance d'individus :

- *L'identification* d'une personne pour établir son identité.
- *L'authentification* qui vérifie la validité de l'identité d'un individu.

Le marché du contrôle d'accès s'est ouvert avec la prolifération des systèmes dont aucun ne se révèle efficace contre la fraude, car tous utilisent un identifiant externe tel que : badge, carte, clé, code, mot de passe...Ces identifiants présentent un gros problème dans la garantie de la sécurité car ils sont exposés à plusieurs risques tels que : la duplication, le vol, l'oubli, la perte… etc.

Au contraire, la biométrie est l'un des moyens les plus fiables et les plus utilisés dans la reconnaissance et authentification des individus. C'est une science basée sur les attributs biologiques, physiques ou comportementaux des personnes, tels que l'ADN, l'urine, la forme du visage, la forme des mains, les empreintes digitales, la voix, la démarche…etc.

Les techniques biométriques basées sur les attributs biologiques (ADN, salive, urine, odeur,…) sont des techniques très couteuses et difficiles à mettre en œuvre pour un usage courant. Pour cela, nous nous limiterons, dans ce chapitre, à la présentation des deux autres classes de méthodes biométriques (physiologiques et comportementales).

Par sa robustesse, sa fiabilité et sa possibilité d'intégration dans un grand nombre de systèmes de sécurité et de contrôle d'accès, la biométrie a pu acquérir une place importante parmi les techniques de haute sécurité. Ce qui explique l'intérêt permanent des chercheurs pour cette technologie.

L'un des points forts des systèmes biométriques se traduit par le faible taux d'erreur commis dans l'identification, puisque les attributs des individus se distinguent d'une personne à une autre (même pour des jumeaux). Un autre avantage de ces systèmes est la possibilité de numériser les informations et les signatures biométriques, acquises à l'aide de capteurs sensoriels ou visiophoniques appropriés, pour des opérations de traitement, de stockage dans des bases de données qui, à leur tour, serviront pour la prise de décision dans un contexte d'authentification.

Dans ce chapitre, nous définirons des généralités sur la biométrie dans l'état de l'art, nous présenterons quelques exemples des techniques de reconnaissance par biométrie et leurs domaines d'application et établirons un tableau général (plus ou moins comparatif) des techniques les plus utilisées sur terrain.

Dans la partie finale de ce chapitre, nous nous intéresserons essentiellement à la technique, qui est sujet de notre mémoire, portant sur la reconnaissance des individus par la rétine (fond de l'œil).

II. La biométrie.

a. Historique.

Depuis son existence, l'homme a toujours essayé de trouver les différences existantes entre lui-même et son entourage et les exploiter dans ses besoins quotidiens.

Les chinois ont été les premiers à utiliser, il y a 1000 ans, les empreintes digitales à des fins de signature de documents. Après, c'était le tour de l'anatomiste MARCELLO MALPIGHI (1628–1694) qui les a étudiées avec un nouvel instrument nommé microscope. Puis le physiologiste tchèque JAN EVANGELISTA PURKINGE (1787–1869) a essayé de les catégoriser selon certaines caractéristiques **[8]**.

Vers la fin du XIX^{è} siècle, le DR HENRY FAULDS (1843–1930), chirurgien à Tokyo, a marqué le premier pas vers l'élaboration d'un système d'identification d'individus en se basant sur des méthodes statistiques pour la classification des empreintes.

En ce moment, un de ses contemporains, le français ALPHONSE BERTILLON (1853-1914), était en train de tester une méthode d'identification des prisonniers nommée anthropométrie judiciaire. BERTILLON procédait à la prise de photographies de sujets humains, mesurait certaines parties de leurs corps (tête, membres, etc.) et on notait les dimensions sur les photos et sur des fiches à des fins d'identification ultérieure. C'était la naissance de la première base de données contenant des informations des individus **[8]**. Et depuis, ces systèmes de reconnaissance ne cessent de se développer et de devenir plus performants.

b. Définitions.

Le terme de **biométrie** est originaire d'une contraction des deux anciens termes grecs : *« bios »* qui signifie : la vie et *« metron »* qui se traduit par : mesure. **[2]**

La biométrie est apparue pour combler les manques des systèmes d'accès classiques, et dans la littérature il existe plusieurs définitions de la biométrie telles que :

« La reconnaissance automatique d'une personne à partir de son comportement ou d'une caractéristique physique ». Source : ISO [1]

« La biométrie recouvre l'ensemble des procédés tendant à identifier un individu à partir de la mesure de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques ou comportementales ». Source : CNIL [2]

La biométrie est la science d'établir l'identité d'une personne basée sur les attributs physiques (empreintes digitales, visage, géométrie de la main, iris, rétine…) ou comportementaux (démarche, signature, dynamique de clavier…) liés à un individu.

Un système biométrique typique utilise les sondes convenablement conçues pour capturer le trait biométrique d'une personne et le compare à l'information stockée dans une base de données pour établir l'identité. **[4]**

Les techniques biométriques permettent donc la mesure et la reconnaissance de **ce que l'on est**, à la différence d'autres techniques de mêmes finalités, mais permettant de mesurer ou vérifier **ce que l'on possède** (carte, badge, document, ...) ou **ce que l'on sait** (mot de passe, code pin, ...).

Un système biométrique peut fonctionner en deux modes distincts : en mode de vérification, le système confirme ou nie une identité réclamée, alors qu'en mode d'identification, il détermine l'identité d'un individu.

La biométrie offre une solution naturelle est fiable pour certains aspects de la gestion d'identité en utilisant des systèmes entièrement automatisés ou semi-automatisés de reconnaissance des individus. **[13]**

c. Intérêt.

La biométrie se rapporte à la classe entière des technologies et techniques pour identifier uniquement des humains. La biométrique est un domaine émergeant où la technologie améliore notre capacité à identifier une personne. La protection des consommateurs contre la fraude ou le vol est un des buts de la biométrie. L'avantage de l'identification biométrique est que chaque individu a ses propres caractéristiques physiques qui ne peuvent être changées,

[1] International Organization for Standardization : http://www.iso.org/
[2] Commission nationale de l'informatique et des libertés : http://www.cnil.fr/

perdues ou volées. La méthode d'identification biométrique peut aussi être utilisée en complément ou remplacement de mots de passe.

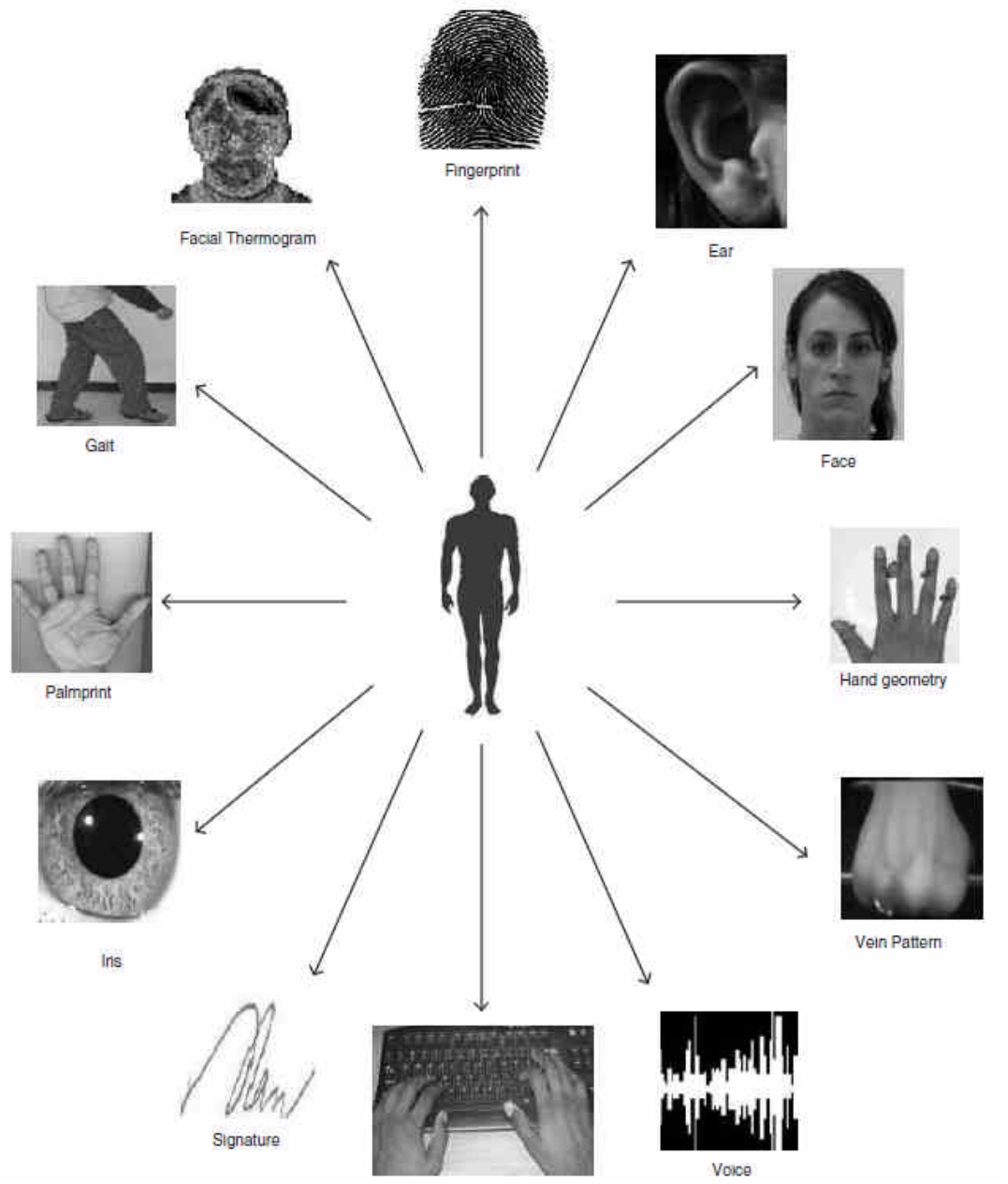


Figure II.1 - Exemples des traits biométriques utilisés pour l'identification [1].

Bien que la technologie biométrique ait de diverses utilisations, son but primaire est de fournir une alternative plus sécurisée aux systèmes traditionnels de contrôle d'accès employés pour protéger les capitaux personnels ou de corporation. Parmi les nombreux problèmes résolus grâce à l'usage des techniques biométriques, les faiblesses qui ont été décelées dans les systèmes actuels de contrôle d'accès sont les suivantes :

- ✓ **Mots de passe faibles** : Les utilisateurs d'ordinateur sont notoirement susceptibles d'employer des pauvres mots de passe facilement devinés, ayant pour résultat des cambriolages où les intrus peuvent deviner les qualifications d'un autre utilisateur et gagner l'accès non autorisé à un système informatique. Ceci peut mener à une violation de la sécurité du personnel ou à un vol de secrets d'affaires par un étranger.
- ✓ **Qualifications partagées** : Dans de petits et grands organismes, nous entendons parler souvent des cas comme ceci : Un utilisateur d'ordinateur partage son mot de passe avec un collègue qui a besoin de l'accès - quoique, dans la plupart des organismes (et dans beaucoup de lois et de règlements liés à la sécurité), ceci est interdit par la politique. Les personnes de nature sont disposées à aider un collègue dans le besoin même si cela signifie violer la politique pour réaliser un plus grand but.
- ✓ **Cartes d'accès principales perdues** : Beaucoup de fois dans nos carrières nous avions trouvé des cartes principales perdues dans des parkings et d'autres endroits publics. Souvent ils ont le nom de l'organisation sur eux, ainsi c'est comme si on trouvait une clef avec une adresse là-dessus, permettant à la personne qui l'a trouvée une libre incursion dans une certaine société.

La biométrie peut résoudre tous ces problèmes en exigeant des crédibilités additionnelles - quelque chose liée au propre corps de la personne - avant d'accorder l'accès à un bâtiment, à une salle des ordinateurs, ou à un système informatique. Un système de contrôle d'accès qui utilise la biométrie inclura un appareil électronique qui mesure un certain aspect spécifique du corps ou du comportement d'une personne qui l'identifie positivement. Le dispositif pourrait être un lecteur d'empreinte digitale, un appareil photo numérique pour atteindre un bon regard dans un iris, ou un lecteur de signature. (Nous discutons tous les types communs de biométrie dans une prochaine section.)

En résumé, plusieurs raisons peuvent motiver l'usage de la biométrie:

- ❖ **Une haute sécurité** : en l'associant à d'autres technologies comme le cryptage, le single sign-on...

- ❖ **Confort** : en remplaçant juste le mot de passe, exemple pour l'ouverture d'un système d'exploitation, la biométrie permet de respecter les règles de base de la sécurité (ne pas inscrire son mot de passe à côté du PC, ne pas désactiver l'écran de veille pour éviter des saisies de mots de passe fréquentes). Et quand ces règles sont respectées, la biométrie évite aux administrateurs de réseaux d'avoir à répondre aux nombreux appels pour perte de mot de passe (que l'on donne parfois au téléphone, donc sans sécurité).

- **Sécurité / Psychologie** : dans certains cas, particulièrement pour le commerce électronique, l'usager n'a pas confiance. Il est important pour les acteurs de ce marché de convaincre le consommateur de faire des transactions. Un moyen d'authentification connu comme les empreintes digitales pourrait faire changer le comportement des consommateurs.

Les systèmes d'authentification biométriques mettent fin aux problèmes liés à l'utilisation des systèmes d'authentification classiques tels que :

- La duplication.
- Le vol.
- L'oubli.
- La perte.

L'usage de la technologie biométrique pour la protection des capitaux remonte à longtemps dans quelques domaines bien précis. Les forces militaires, l'intelligence, et les organismes de police avaient employé la biométrie pour élever le niveau de sécurité des contrôles d'accès physiques et logiques pendant des décennies.

	Copie	Vol	Oubli	Perte
Clé	●	●	●	●
Badge	-	●	●	●
Code	●	-	●	-
Empreinte	-	-	-	-

Tableau II.1- Inconvénients des systèmes d'authentification classiques.

Mais dans ces dernières années, il y a eu une importante hausse dans l'utilisation de la biométrie pour la protection des capitaux de haute valeur. Les centres de traitement des données emploient souvent la biométrie pour contrôler l'accès du personnel dans l'espace du centre de données. Les dispositifs de reconnaissance des empreintes digitales apparaissent partout - même incorporés aux ordinateurs portables, au PDAs, et aux commandes d'USB. L'identification faciale est disponible sur quelques modèles d'ordinateur portable. Et pour la sécurité des entreprises et des résidences, des portes à verrouillage par empreintes digitales sont disponibles sur le marché…

d. Les systèmes biométriques.

Un système biométrique est essentiellement un système qui acquiert des données biométriques d'un individu, extrait un ensemble de caractéristiques à partir de ces données, puis le compare à un ensemble de données stocké au préalable dans une base de données pour pouvoir enfin exécuter une action ou prendre une décision à partir du résultat de cette comparaison. **[1]**

Par conséquent, un système biométrique est composé de quatre modules principaux : **[1]**

- ✓ **Le module d'acquisition** : un lecteur, un scanner ou autre module de balayage approprié est requis pour l'acquisition des données biométriques brutes d'un individu. Pour obtenir les images des empreintes digitales, par exemple, un capteur optique peut être utilisé pour acquérir l'image de la structure des arêtes sur le bout des doigts. Il joue le rôle de l'interface homme-machine et représente un pivot élémentaire du système biométrique. Une interface mal conçue peut influencer sur la fiabilité de tout le système.

- ✓ **Le module d'évaluation de qualité et d'extraction de caractéristiques** : La qualité des données biométriques obtenues lors de la capture doit être évaluée par ce module afin de déterminer sa convenance pour le processus de reconnaissance. Généralement, les données acquises doivent être soumises à des algorithmes de perfectionnement afin d'améliorer la qualité du signal. Ce module exige, parfois, la recapture des données avant de les traiter s'il s'avère que la qualité des données déjà capturées est inacceptable. Les données biométriques sont alors traitées d'une manière à extraire les traits fondamentaux et les caractéristiques qui permettront d'obtenir la signature biométrique de l'individu. Par exemple, la position et l'orientation des points de minuties pour les empreintes digitales, la position et l'orientation des points de bifurcations pour la reconnaissance rétinienne…etc.

- ✓ **Le module de comparaison (*matching*) et de prise de décision** : ce module comprend le processus de comparaison entre l'ensemble des caractéristiques extrait et les autres ensembles ou modèles existants dans la base de données. Le résultat de cette comparaison va être utilisé pour prendre une décision sur le taux de correspondance de la signature biométrique pour la validation ou le rejet de l'identité de l'individu à reconnaitre.

- ✓ **Le module de base de données** : il sert de dépôt des signatures biométriques obtenues lors de la phase d'enrôlement. Cette phase permet d'inscrire dans la base de données les informations biométrique et biographique (nom et prénom, n° d'identification, adresse…) des utilisateurs. Dans un sens figuré, ce module joue le rôle d'un annuaire des signatures biométriques.

e. Performances d'un système biométrique.

Le principe de fonctionnement des systèmes biométriques, tels que décrit dans la littérature **[5], [1]** (et comme montré dans la Figure II.2*)*, comporte (03) trois modes principaux :

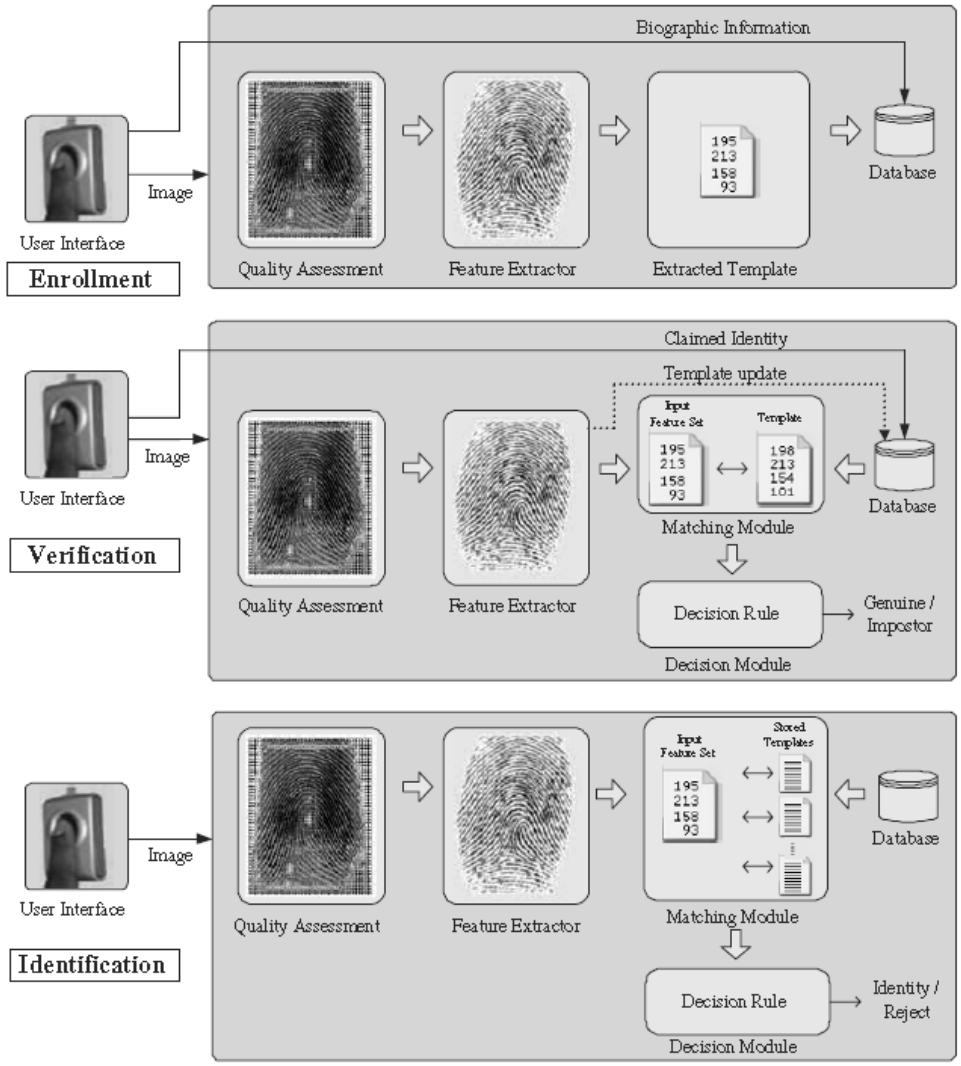


Figure II.2 - Principe de fonctionnement des systèmes biométriques [1].

- **Enrôlement :** c'est l'étape d'enregistrement des signatures biométriques de chaque utilisateur dans la base de données. Chaque utilisateur présente un ou plusieurs échantillons d'une caractéristique biométrique qui vont être traités et stockés dans la base sous un identifiant, accompagnés parfois de références biographiques (nom, prénom, adresse…), correspondant à cet utilisateur. Ces données serviront plus tard dans la phase d'identification.

- **Authentification :** ou vérification qui permet de vérifier l'authenticité d'un individu. Ce dernier fournit un échantillon biométrique ainsi qu'un identifiant et le système s'assure que le pattern enregistré dans la base sous cet identifiant correspond bien à la signature biométrique fournie par l'utilisateur. Le module de décision produit une réponse oui/non selon l'authentification/rejet de l'identité. Dans cette phase, les systèmes biométriques effectuent une mise à jour des patterns pour les types de traits biométriques qui changent légèrement à travers le temps (Reconnaissance faciale).

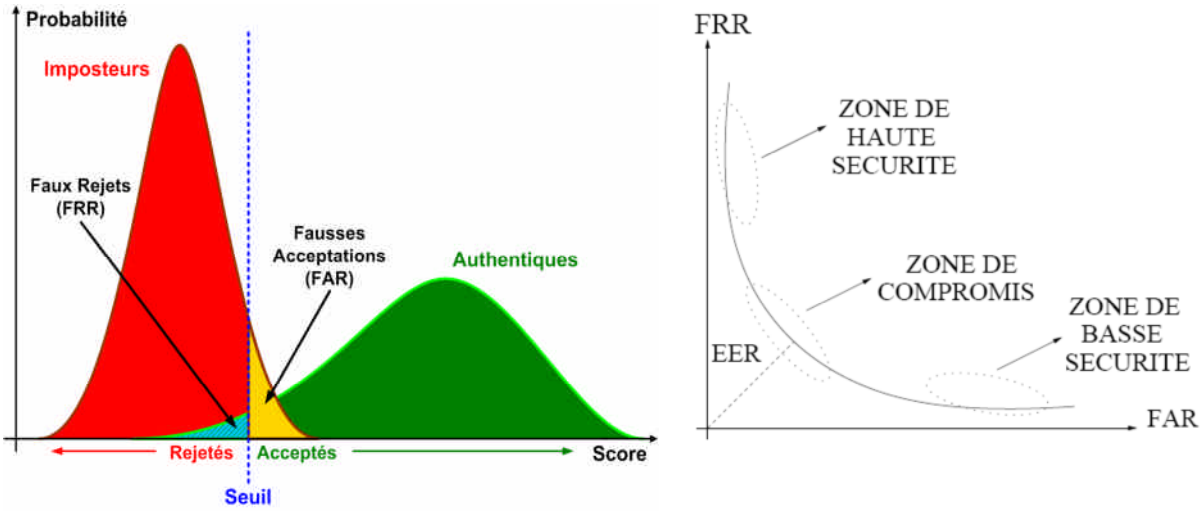
- **Identification :** c'est l'étape de reconnaissance des individus. L'échantillon présenté pour l'identification est soumis, après traitement, à des algorithmes de comparaison avec les différents patrons stockés dans la base de données, afin de permettre au module de décision d'établir l'identité de l'individu en question.

Dans les systèmes d'identification classiques, tels que l'identification par mot de passe, la correspondance doit être parfaite et absolue (100% de similitude) entre l'identifiant présenté pour la reconnaissance et celui enregistré dans la base de données (ex.: Dans le cas d'identification par mot de passe, la chaine de caractère saisie par l'utilisateur du système doit correspondre exactement à la chaine qui identifie cette personne et lui attribue les droits d'accès appropriés).

En revanche, dans les systèmes biométriques, la correspondance n'est pas absolue. Ceci est dû à :

- des conditions imparfaites lors de l'acquisition des échantillons biométriques (ex.: empreinte digitale bruitée à cause d'un disfonctionnement du lecteur),
- des variations de la caractéristique biométrique de l'utilisateur (ex.: des problèmes respiratoires peuvent affecter l'échantillon vocal de l'utilisateur),
- des changements des conditions ambiantes (ex.: Mauvaise illumination influe sur la reconnaissance du visage),
- la différence dans l'interaction de l'utilisateur avec les dispositifs d'acquisition (ex.: iris occlus, empreinte partielle),

Cependant, il est très rare d'obtenir un ensemble de caractéristiques exactement similaires lors de deux acquisitions d'échantillons biométriques d'un individu. En effet, une correspondance parfaite de deux échantillons déclenche une mise en garde du système contre une tentative de fraude par reproduction.



(a) La courbe FRR Vs FAR *(b) La courbe ROC*

Figure II.3 - Courbes représentatives des taux de similitude FAR, FRR.

Le degré de similitude entre deux ensembles de caractéristiques est appelé : le taux de similarité (*Similarity Score*). Le taux de similarité d'une comparaison entre deux échantillons d'un trait biométrique du même individu est appelé : taux d'authenticité (*Genuine Score* ou *Authentic Score*). Le taux de similarité entre deux échantillons de deux individus différents est appelé : taux d'imposture (*Impostor Score*).

Comme montré sur la Figure II.3 (a), il est question d'un compromis, défini par un seuil, entre le taux de fausses acceptations et le taux des faux rejets. C'est-à-dire qu'un taux d'authenticité en dessous du seuil génère un faux rejet, tandis qu'un taux d'imposture qui dépasse le seuil résulte une fausse acceptation.

La performance d'un système biométrique est quantifiée par le taux de deux erreurs fondamentales définies dans **[4], [1]** par :

- **F.A.R. :** *(False Acceptation Rate)* ou **F.M.R.** (*False Match Rate*) dans certains ouvrages, ces taux déterminent la probabilité pour un système de « reconnaître » une personne qui normalement n'aurait pas dû être reconnue. C'est un ratio entre le nombre de personnes qui ont été acceptées alors qu'elles n'auraient pas dû l'être et le nombre total de personnes non autorisées qui ont tenté de se faire accepter.
- **F.R.R. :** *(False Reject Rate)* ou **F.N.M.R** (*False Non Match Rate*), ces taux déterminent la probabilité pour un système donné de ne pas « reconnaître » une personne qui normalement aurait dû être reconnue. C'est un ratio entre le nombre de personnes légitimes dont l'accès a été refusé et le nombre total de personnes légitimes s'étant présentées.

Techniques testées	*FAR*	*FRR*	*EER*
Iris	0,0001 %	0,25 %	~ 0,5 %
Empreintes digitales (2)*	0,008 %	2,5 %	~1 %
Voix	0,03 %	2 %	~ 0
Empreintes digitales (1)*	0,08 %	6 %	~1 %
Géométrie de la main	0,70 %	0,5 %	~0
Empreintes digitales (optique)	0,45 %	11 %	~2 %
Face	0,45 %	17 %	~ 0

* Algorithmes différents

Tableau II.2 - Mesures des FAR, FRR et EER sur quelques exemples techniques biométriques.

Cela nous ramène à dire que la variation du seuil implique la variation inversement proportionnelle des deux taux F.A.R. et F.R.R. cités précédemment. La courbe ROC[1] (*Receiver*

[1] En réalité, la courbe ROC représente le GAR Vs FAR, mais par abus de langage on fait allusion à la courbe DET (*Detection Error Trade-off*) qui représente le FRR en fonction du FAR.

Operating Characteristic), donnée par la Figure II.3 (b), est une représentation graphique du compromis des deux taux. Dans un système biométrique, la minimisation simultanée des deux taux n'est pas possible, or le choix de minimisation d'un taux dépend de la qualité du système souhaitée. Pour un système de haute sécurité, par exemple, on s'intéresse à minimiser le F.A.R., tandis que si la commodité est la préoccupation première, on minimise le F.R.R.

Outre le F.A.R. et le F.R.R., il existe d'autres types d'erreurs dans les systèmes biométriques. Le E.E.R. (*Equal Error Rate*) est le taux qui définit un compromis généralement retenu pour les applications civiles consistant à obtenir une égalité entre le FFR et le FAR (ou entre le FMR et le FNMR). Il y a aussi le FTE (*Failure To Enrol*) qui mesure la probabilité qu'une personne ne puisse être enrôlée pour des raisons physiques tenant à la personne ou techniques liées au dispositif de capture. Mais, l'augmentation du taux d'échec à l'enrôlement, lorsqu'elle est délibérée et destinée à éliminer les images de mauvaise qualité ne pouvant servir de référence pour les comparaisons futures, peut produire une diminution des taux d'erreurs (FM ou FNM). Ce phénomène peut aussi survenir lors de l'identification, à ce moment on parle d'une erreur F.T.A. (*Failure To Acquire*).

f. Caractéristiques de la biométrie.

Un certain nombre de caractéristiques sont utilisées dans diverses applications. Chaque trait biométrique a ses avantages et ses inconvénients, c'est pourquoi, le choix de la technique pour une application particulière dépend d'une variété de questions en plus de sa performance. JAIN ET AL **[6]** ont identifié sept facteurs déterminant la convenance des traits physiques ou comportementaux pour être utilisés dans une application biométrique : **[1]**

- **Universalité** : toute personne ayant accès à l'application doit posséder le trait.
- **Unicité** : le trait doit être suffisamment différent d'une personne à une autre.
- **Permanence** : le trait biométrique d'une personne doit être suffisamment invariant au cours d'une période de temps.
- **Mesurabilité** : il devrait être possible d'acquérir et de numériser les données biométriques à l'aide d'un dispositif approprié.
- **Performance** : la précision de la reconnaissance et les ressources nécessaires pour atteindre la précision que doit satisfaire les contraintes imposées par l'application.
- **Acceptabilité** : les individus qui vont utiliser cette application doivent être disposés à présenter leurs traits biométriques au système.
- **Contournement** : il s'agit de la facilité avec laquelle le caractère d'un individu peut être imité en utilisant des objets (par exemple : faux doigts dans le cas de traits physiques et le mimétisme, dans le cas de traits de comportement).

g. Types de reconnaissance par biométrie.

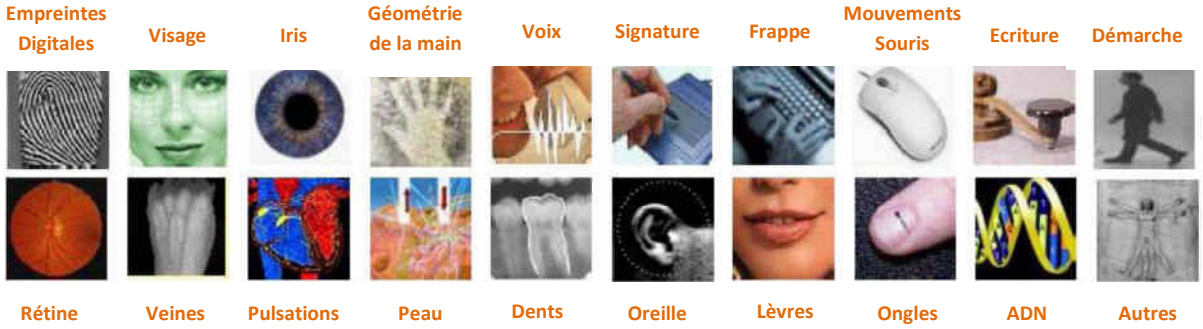


Figure II.4 - Différentes modalités biométriques.

Bien qu'il existe un très grand nombre de modalités biométriques, nous pouvons distinguer deux grandes catégories:

- **L'analyse des traces biologiques** : basées sur les caractéristiques biologiques des individus (ADN, salive, urine, odeur…). Ce type de biométrie est très complexe à mettre en œuvre dans un système usuel de reconnaissance et n'est utilisé que dans un cas d'extrême nécessité (ex.: Enquête criminelle, test de paternité…etc.)

- **L'analyse des traits physiques** : ce type de méthodes est beaucoup plus facile à mettre en œuvre dans un système de contrôle d'identité et ne nécessite pas autant de moyens. Comme montré dans le schéma de la Figure II.5, nous pouvons représenter les types de biométries physiques les plus connus et les plus utilisés dans les deux grandes classes : **[2]**

✓ **la biométrie physiologique ou morphologique :** utilisant les caractéristiques physiologiques de l'individu (exemple: la forme de la main, la forme du visage, les empreintes digitales, l'iris, la rétine…etc.)

✓ **la biométrie comportementale :** qui se base sur le comportement de l'individu. (exemple: la démarche, la voix, les mouvements…etc.)

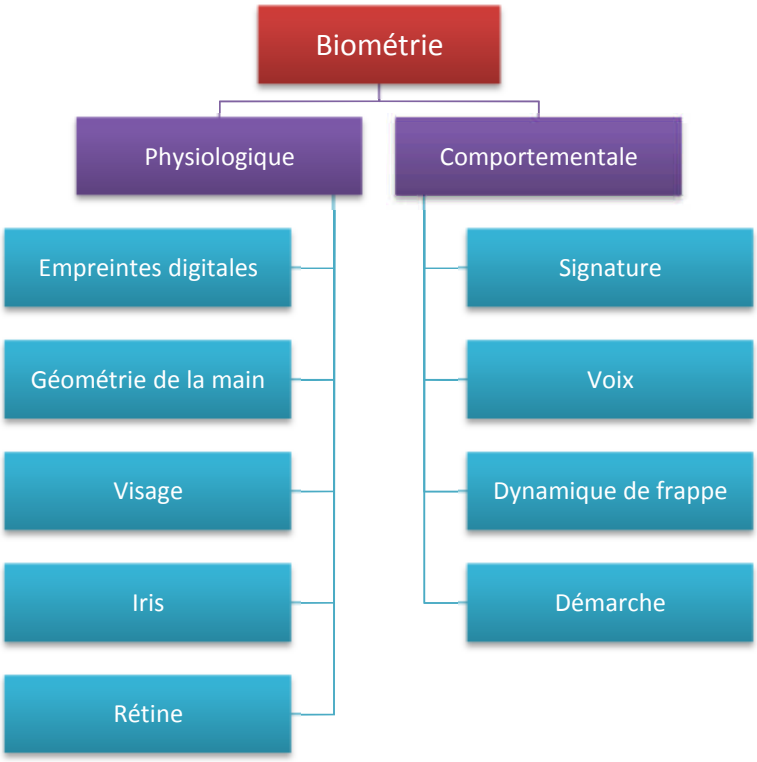


Figure II.5 - Catégories des méthodes d'identification biométriques [2].

1. La reconnaissance comportementale.

Dans ces techniques de reconnaissance, on s'intéresse aux caractéristiques physiques en activité des individus qui peuvent être typiques et permettent de distinguer une personne d'une autre. Plus explicitement, on étudie la manière de faire des individus.

Comme exemple nous citons :

i. La signature.

La vérification par signature comme technique était parmi les premières utilisées dans le domaine de la biométrie. Il y avait plusieurs systèmes concurrents dans ce domaine. Elle semblait être une application évidente de la biométrie car il y avait tant de processus familiers qui avait utilisé la signature comme moyen de vérification d'identité.

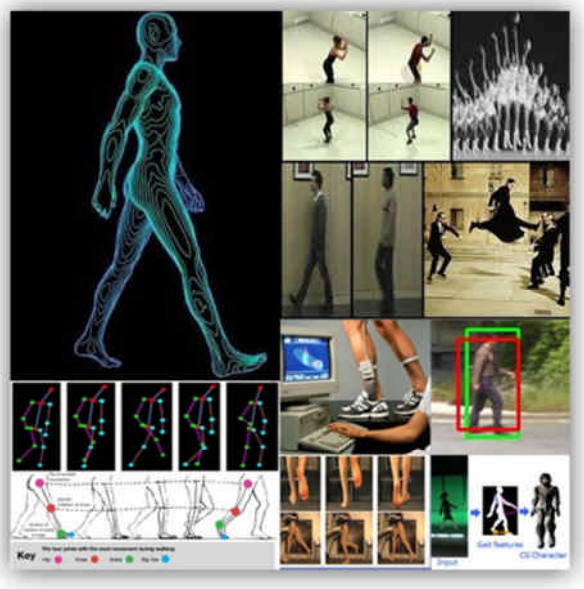
En outre, la signature biométrique, du moins en théorie, fournissait une profondeur d'analyse autre que celle de la mesure de la dynamique inhérente dans son écriture, la précision géométrique de la signature. Dans des tests indépendants, la vérification de la signature a donné une raisonnable présentation d'elle-même. Cependant, dans les situations réelles, l'utilisation des tablettes graphiques disponibles dans le marché et les systèmes adéquats n'était souvent pas une chose aussi aisée. En outre, il est intéressant, en termes proportionnels, de voir les incohérences de certaines personnes en signant leur nom dynamiquement et graphiquement. Tandis qu'un observateur humain peut tolérer ces incohérences tant que la signature est correcte, l'algorithme de vérification automatique de la signature prenait un temps important, particulièrement quand il essayait de fonctionner avec un niveau de tolérance serré. En conséquence, la vérification par signature biométrique reste une technique traditionnelle, bien qu'il puisse y avoir des applications où elle peut s'avérer utile. **[7]**

ii. La dynamique de frappe.

Selon **[7],** c'est une autre technique primitive dans laquelle un énorme apport en temps et en effort a été investi, notamment par quelques grandes compagnies de technologie de l'information. L'idée d'identifier un individu par sa dynamique particulière de frappe était clairement attrayante parmi les perspectives de la technologie de l'information et des réseaux. Tandis qu'il semblait possible de déterminer une signature dynamique individuelle de frappe dans des conditions soigneusement contrôlées, les utilisateurs réels sous de réelles conditions de fonctionnement n'étaient pas aussi cohérents qu'on le voudrait dans la manière d'utiliser un clavier afin de mettre en application cette technologie. En outre, en utilisant les claviers standards, il n'y avait pas vraiment une richesse d'information individualiste avec laquelle travailler. Après beaucoup de recherches et quelques démonstrations intéressantes, l'idée de la dynamique de frappe en tant que technique biométrique comportementale viable semblait se faner, particulièrement quand d'autres techniques ont été vues accomplir de bons progrès.

iii. La voix.

La vérification par la voix est une autre technique pilote et il y avait quelque différents systèmes disponibles pendant un bon moment, certains d'entre eux étaient considérés comme une perspective des systèmes. Typiquement, les systèmes de vérification de la voix analysaient la dynamique inhérente des individus en annonçant une phrase type, générant un pattern en conséquence, qui pourra être utilisé dans une éventuelle reconnaissance d'un vif échantillon. Tandis que la théorie est assez logique et, sans doute, certains algorithmes de reconnaissance ont bien été développés, la vérification de la voix comme technique fût désavantagée sur plusieurs points. Premièrement, en utilisant les capteurs disponibles dans le marché tels que des combinés de téléphone, la qualité des capteurs est non seulement relativement pauvre en terme de réponse de fréquence et largeur de bande dynamique, mais notoirement variable d'échantillon à un autre. Deuxièmement, nous avons les contradictions et les bruits considérables dans les canaux de transmission (ex : lignes téléphoniques, routeurs, échangeurs…). Troisièmement, les variables environnements de point de présence auront les niveaux également variables de bruit ambiant et les propriétés acoustiques telles que la réflexivité, l'absorption, prépondérance vers les ondes stationnaires et ainsi de suite. Pour finir, la cohérence avec laquelle les utilisateurs interagissent avec le dispositif de capture laisse souvent à désirer, particulièrement avec les utilisateurs non-habitués. De telles conditions, une fois réunies, peuvent poser d'énormes défis pour les systèmes de vérification de la voix. Néanmoins, elles peuvent être bien adaptées dans certaines applications à circuit-fermé où la voix est le choix biométrique. **[7]**



iv. La démarche.

L'attraction potentielle de l'identification de démarche se situe dans la capacité d'identifier un individu à distance. Cependant, il y a des défis sérieux à surmonter à cet égard. L'idée qu'un individu marche typiquement avec

une démarche unique est intéressante et, sous des conditions de laboratoire, le concept de l'identification de démarche peut être démontré. Cependant, la vie réelle est pleine de désaccords dynamiques qui rendent l'exécution d'un tel système particulièrement difficile. En plus des complexités de comparaison, il y a des facteurs tels que l'occasion de saisir l'image mobile d'un individu en isolement et dont le détail est suffisant pour pouvoir entreprendre une telle comparaison. La création d'un modèle fiable est également quelque chose qui présente de vrais défis. L'identification de la démarche représente un exemple intéressant de la recherche biométrique conduite par une condition perçue : dans ce cas-ci, pour identifier un individu à une distance au-delà de laquelle la biométrie de contact et à bout-portant ne peuvent fonctionner. C'est peut-être une idée attrayante pour des applications militaires et de très haute sécurité, mais il est douteux que l'identification par la démarche deviendra une technique biométrique courante. **[7]**

2. La reconnaissance physiologique.

Ces types de reconnaissance mesurent une caractéristique spécifique de la structure ou de la forme d'une partie du corps humain. Nous pouvons citer les exemples les plus connus :

i. La géométrie de la main.

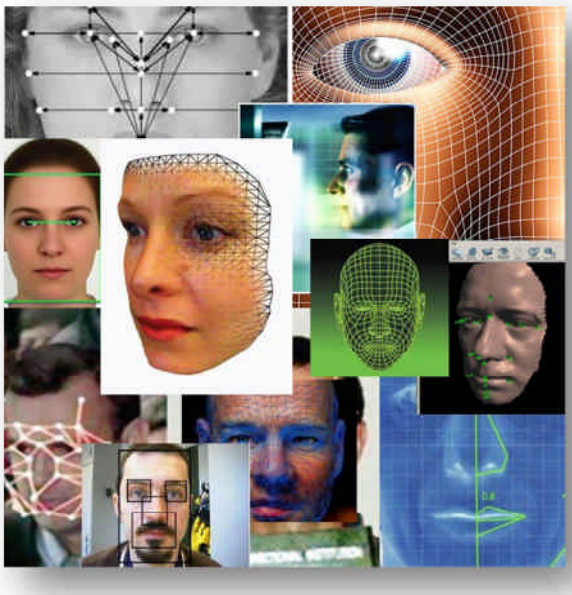
C'est l'une des techniques biométriques pilotes qui, à l'origine, mesurait la position et la taille des doigts, placés sur une surface plane. Le dispositif original était plutôt grand et encombrant, mais ceci a été aussitôt raffiné en créant le dispositif de la géométrie de la main ID3D, qui était beaucoup plus pratique et, comme son nom le suggère, a présenté un facteur tridimensionnel avec l'utilisation des miroirs. Il y avait beaucoup de points forts liés à ce dispositif, incluant la facilité d'utilisation relative et un pattern exceptionnellement petit d'environ 9 octets, facilitant son stockage sur des médias portatifs avec une basse utilisation de ressource du système dans le cas d'un stockage central ou, sur le dispositif lui-même. L'ID3D était également longuement mûri d'une perspective de systèmes, facilitant les réseaux RS485 simples à créer avec rien de plus que les lecteurs eux-mêmes et fournissant effectivement le stockage distribué de patterns. Les versions actuelles du lecteur original de la géométrie de main continuent à fournir une bonne fonctionnalité, la facilité d'utilisation et une performance tout à fait raisonnable. Elles restent particulièrement bien adaptées à certains types d'applications et sont employées

souvent dans le cadre du contrôle d'accès physique, la surveillance des temps et des présences et les applications semblables. **[7]**

ii. Les veines.

On a longtemps considéré que le modèle des veines dans l'anatomie humaine peut être unique aux individus. En conséquence, il y a eu de diverses réalisations du balayage de veine au cours des années, du balayage de main, au balayage de poignet et, plus récemment, au balayage de doigt. La plupart de ces techniques ont été utilisées sur terrain et ont pu certainement former la base d'un système biométrique viable de vérification d'identité. Le problème auquel elles font face n'est pas un problème de possibilités ou d'efficacité technique, mais plutôt un problème de réalité du marché. La prépondérance de systèmes d'empreinte digitale, de visage et d'iris, facilement disponibles à une large gamme de coûts, ne permet pas à une technique distincte de gagner la part de marché sans avantage clair et irrésistible. Même les techniques primaires, telles que la géométrie de main, ont une base qui est peu susceptible d'être réalisée par une technique plus récente de performance comparable. En conséquence, pour n'importe quelle nouvelle technique biométrique prenant place dans le marché, elle doit gagner le terrain et offrir des avantages clairs qui ne peuvent pas être réalisés par des méthodes contemporaines. Les diverses réalisations de balayage des veines, bien qu'assurément intéressantes, ne peuvent lutter que peu dans ce contexte. Cependant, le temps peut s'avérer un niveleur intéressant dans ces contextes et les demandes de la technique de balayage de veines peuvent s'accroître. **[7]**

iii. Le visage.



L'identification par visage a été disponible comme technique biométrique pendant longtemps, bien qu'elle soit probablement juste pour indiquer que les réalisations primaires ont laissé à désirer en termes d'exactitude et fiabilité de comparaison. Cependant, la technique a beaucoup d'applications potentielles, et le

développement continu a assuré qu'il a rapidement mûri dans une technique opérationnelle viable. Typiquement, la technique implique la métrique des et entre caractéristiques distinctes dans le visage, se fondant moins sur des facteurs d'une nature transitoire tels que la coupe de cheveux ou l'utilisation des produits de beauté. Néanmoins, le visage humain est sujet au changement avec le temps et cette réalité demeurera un défi pour des systèmes d'identification de visage, comme le changement d'expression, la maladie, la vieillesse et d'autres facteurs normaux. En outre, les facteurs humains et environnementaux joueront presque toujours un très grand rôle dans l'efficacité d'un système d'identification de visage, dans un scénario donné de déploiement. En conséquence, l'identification de visage peut tout à fait ne pas égaler l'exactitude fournie par certaines autres techniques. Cependant, elle se prête aisément aux applications où le visage est déjà employé dans un contexte de vérification d'identité. De même, la capacité de comparer avec une image stockée, peut-être d'une source différente, semblera attrayante dans quelques applications de secteur public. L'identification de visage a été parfois employée en même temps qu'une autre biométrie afin d'augmenter la confiance en procédé de vérification d'identité. Le visage et l'empreinte digitale sont une combinaison populaire dans ce contexte. Tout en n'offrant pas les niveaux superlatifs de l'exactitude ou de l'exécution opérationnelle, l'identification de visage néanmoins demeure une technique populaire, et une de celles qui tireront bénéfice sans doute d'un développement ultérieur. **[7]**

iv. L'iris.

L'identification d'iris est devenue une technique biométrique populaire. Elle est généralement reconnue qu'étant peut-être la technique la plus précise en termes d'apparier différents modèles d'iris. En conséquence, c'est une technique utile que ce soit pour l'assortiment linéaire aux fins de vérification individuelle d'identité, ou un assortiment un-à-plusieurs aux fins d'identifier un iris particulier parmi plusieurs dans une grande base de données. En outre, l'exécution opérationnelle relative de l'identification d'iris peut être très bonne. Dans des réalisations antérieures, le défaut d'acquisition d'image de qualité appropriée dans de vraies conditions de fonctionnement pouvait être un problème, également pour la possibilité d'acquérir des modèles référentiels de bonne qualité. Cependant, la technique a rapidement évolué et de tels problèmes sont rarement rencontrés aujourd'hui. Les lecteurs d'identification d'iris ont tendance à être un peu plus chers que ceux pour certaines autres techniques, en grande partie en raison de leur complexité relative. En outre, l'installation et le commandement peuvent être un peu plus

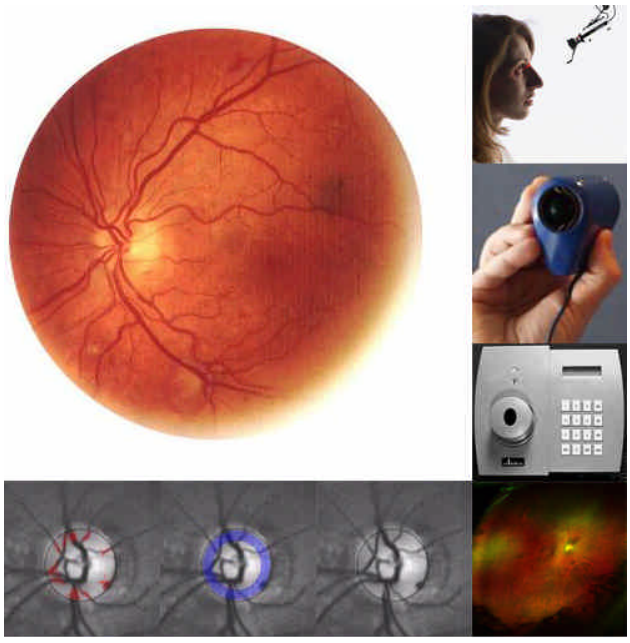
exigeants, particulièrement en ce qui concerne le placement environnemental et l'accommodation pour une large gamme d'individus de taille physique différente. Toutefois, de tels soucis de déploiement peuvent être surmontés et peuvent être considérés insignifiants pour des applications où l'exactitude et la performance de l'identification d'iris est exigée. En termes simples, la technique implique la localisation de l'iris dans un visage humain, le séparant de la pupille et de la sclérotique, divisant l'iris évident en segments et analysant chaque segment en conséquence. De cette analyse, un code relativement sophistiqué d'iris peut être dérivé et comparé à une référence précédemment stockée. La quantité de détails représentée dans le code d'iris permet un niveau important de confiance en entreprenant les comparaisons, même en recherchant dans des bases de données très grandes. Ceci est facilité par la quantité de l'information disponible qui peut être dérivée d'un iris typique, et l'unicité relative de l'iris dans la population humaine. En effet, même les iris gauche et droit du même individu ont tendance à être distincts et des iris sont considérés comme invariables durant toute la vie, une fois fixés peu de temps après la naissance. L'identification par iris s'accroit en popularité ces dernières années et c'est une technique qui continuera sans doute à être employée couramment. **[7]**

v. *Les empreintes digitales.*

L'identification par empreintes digitales est la technique biométrique que la plupart de gens connaissent. C'était toujours le choix biométrique évident pour les services de police, où la comparaison des empreintes digitales a été fondamentale à l'identification des criminels durant le siècle dernier. Cette réalité en soi a, au début, présenté une sorte de stigmate, en raison de l'alignement fort avec la criminologie dans la plupart des esprits. Il y a une dichotomie ici entre les systèmes d'identification d'empreinte digitale automatisée (AFIS), comme employé par des organismes chargés de faire appliquer la loi, pour la recherche dans de grandes bases de données, souvent en différé, afin d'identifier des criminels, et des systèmes biométriques d'empreinte digitale discrète, qui fonctionnent typiquement en temps réel afin de vérifier une identité individuelle, dans une marge des scénarii. Les deux fonctions sont de plus en plus liées dans les secteurs tels que le contrôle aux frontières, et ceci soulève quelques questions intéressantes. La technologie elle-même, cependant, a progressé rapidement dans les systèmes réalisables qui sont considérablement plus faciles à utiliser et plus fiables que certaines implémentations originales. Les lecteurs d'empreinte digitale peuvent utiliser une

sonde optique ou capacitive, qui a ses propres avantages selon l'application. Les sondes optiques peuvent offrir la résolution et pouvoir facilement saisir une image pleine à teintes de gris de l'empreinte digitale. Les sondes capacitives tendent à être plus petites, facilement intégrées et moins sensible à l'habillage de la crasse sur la surface de la sonde. L'algorithme de comparaison des empreintes digitales doit être basé sur l'identification des minuties selon un vecteur spatial, ou sur la comparaison des images par contrastes des pixels ou niveaux de gris. Quelques systèmes peuvent stocker l'information de minuties et une image complète de l'empreinte digitale. Dans la pratique, l'identification par empreintes digitales est devenue bien adoptée comme méthodologie biométrique à travers une large variété d'applications. Plusieurs de ces applications sont dans le secteur public, pour des applications telles que le contrôle aux frontières, documentation d'identité nationale, droit d'avantage et ainsi de suite. Beaucoup d'entre elles sont dans le secteur privé pour des applications telles que l'accès au réseau, la sécurité de dispositif mobile, les systèmes de paiement volontairement transportable et d'autres applications. Les sondes d'empreinte digitale sont devenues presque un article commode et sont souvent fournies en base dans un équipement original du fabricant (OEM) pour l'incorporation dans des PC, ordinateurs portables et une série d'autres dispositifs, ou bien fournies dans une gamme de formes distinctes comme les produits commerciaux disponibles immédiatement (COTS) pour l'intégration dans d'autres systèmes. L'exécution de l'identification d'empreinte digitale peut être robuste, selon le nombre d'empreintes digitales utilisées et la dépendance sur des facteurs humains et environnementaux. **[7]**

vi. La rétine.



Le balayage rétinien est une technique biométrique primaire, développée au début pour le contrôle d'accès dans les environnements militaires. Son exécution donnait de très bons résultats sous certaines conditions. Cependant, sa rentabilité était en général plutôt ennuyeuse, au moins en ce qui concerne les réalisations primaires, bien qu'elles soient améliorées dans des essais postérieurs. C'est principalement parce que son utilisation, à l'origine, imposait une fixation d'un dispositif binoculaire et d'aligner sa vision sur une cible chose que beaucoup de personnes ont, au début, eu du mal à faire- particulièrement ceux dont la vision est altérée. En outre, beaucoup d'utilisateurs n'ont pas beaucoup apprécié l'idée du contact physique avec l'interface binoculaire. En conséquence, alors que l'utilisation dans un environnement militaire

commandé a pu être acceptable (en grande partie parce que de tels utilisateurs n'ont eu aucun choix dans la matière) la technique trouvait peu de faveur au sein de la communauté intégrale. La technique d'exploration rétinienne impliquait de balayer les modèles de veine de la rétine avec un faisceau actionné bas brillant à l'intérieur de l'œil : une fonction intrusive qui n'a pas été typiquement considérée comme une proposition attrayante par les utilisateurs potentiels. En outre, les premières versions des modules de balayage rétiniens étaient excessivement chères pour n'importe qui en dehors des militaires. Les versions qui ont suivi sont devenues beaucoup moins coûteuses et étaient un peu mieux considérées en termes de connectivité, intégration de systèmes et interface utilisateurs. **[7]**

vii. Autres techniques.

Dans **[7],** l'auteur évoque d'autres techniques de vérification biométriques d'identité qui ont fait surface de temps à autre, telles que l'identification du lobe d'oreille et l'identification de l'odeur...etc. Presque n'importe quel caractéristique anatomique ou trait comportemental pourrait être considéré comme candidat pour un identifiant biométrique fonctionnel. Cependant, nous devons placer de telles idées dans leurs contextes et les aligner avec la condition perçue. Si cette condition est d'avoir une méthode par laquelle nous pourrions vérifier une identité individuelle avec un degré de confiance raisonnable, alors les méthodologies biométriques existantes nous fournissent les moyens de faire ceci d'une large série de manières, de ce fait, facilitant une large étendue d'applications. Peut-être, au moment adéquat, on développera d'autres techniques qui pourraient supplanter certaines des méthodologies existantes. Pour l'instant, nous pourrions utilement tourner notre attention vers une meilleure utilisation des techniques existantes dans des applications contemporaines, et la fourniture d'un meilleur arrangement du futur alignement avec des espérances sociales.

h. Comparaison des systèmes biométriques.

Une question qui se pose souvent dans ce domaine est la suivante :

« Quelle est la meilleure technique biométrique ? »

La réponse naturellement est qu'il n'y a aucune meilleure technique biométrique en termes absolus, tout dépend de la nature précise de l'application et des raisons de son

exécution. Néanmoins, nous pouvons analyser leur distribution du point de vue utilisation, et les comparer dans leurs propres contextes selon leurs critères de performance.

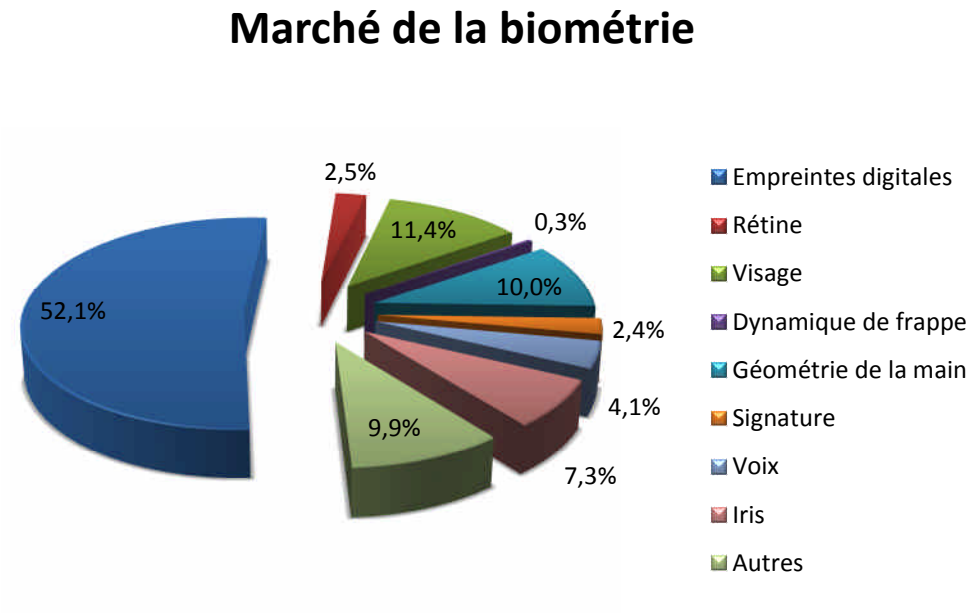


Figure II.6 - Distribution de l'utilisation des systèmes biométriques sur le marché mondial.

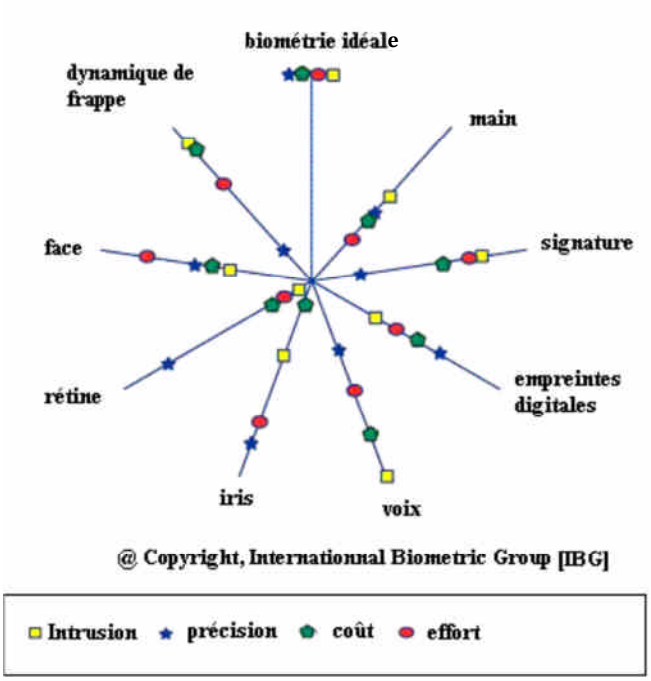


Figure II.7 - Comparaison des techniques biométriques selon les critères : Effort, Intrusion, Coût et Précision.

Sur le schéma présenté sur la Figure II.7, les différentes méthodes sont évaluées à l'aide d'une série de critères :

- ✓ **Effort** : effort fourni par l'utilisateur lors de l'authentification.
- ✓ **Intrusion** : information sur l'acceptation du système par les usagers.
- ✓ **Coût** : coût de la technologie (lecteurs, capteurs, etc.).
- ✓ **Précision** : efficacité de la méthode (liée au taux d'erreur).

Le Tableau II.3 montre qu'il n'existe pas de méthode idéale. Les méthodes se divisent en deux grands groupes. Le premier groupe englobe les méthodes conviviales pour les utilisateurs (effort à fournir faible, méthode peu intrusive, prix modéré) mais peu performantes. Ce groupe correspond aux méthodes basées sur la biométrie comportementale (reconnaissance de la voix, de la signature…). L'autre groupe contient les méthodes plus sûres (méthodes intrusives et prix élevés, performances très bonnes). Il est donc nécessaire de déterminer, au cas par cas, pour chaque problème, la méthode qui conviendra le mieux à la situation. Pour cela, il faut étudier attentivement le niveau d'exigence en sécurité, le budget pouvant être investi dans le système et la façon dont risquent de réagir les utilisateurs.

Actuellement, pour la mise en place des grands projets de passeports biométriques, les systèmes retenus par l'Europe semble être un stockage de la photo d'identité, des empreintes digitales et de l'iris sous forme numérique. A noter que le choix du ou des dispositifs biométriques peut aussi dépendre de la culture locale. Ainsi, en Asie, les méthodes nécessitant un contact physique comme les empreintes digitales sont rejetées pour des raisons d'hygiène alors que les méthodes basées sur l'iris sont très bien acceptées. La biométrie basée sur l'image rétinienne est très précise et très fiable mais c'est la méthode la plus intrusive et nécessitant un effort et un coût importants par rapport aux autres méthodes.

Le Tableau II.4 illustre une petite comparaison entre les systèmes biométriques les plus répandus. Nous pouvons constater que l'utilisation du système biométrique rétinien est rare malgré son excellente efficacité. Le retard de cette technique est dû surtout, comme déjà évoqué, au caractère invasif de l'acquisition de l'image rétinienne. Nous verrons dans les chapitres suivants que les méthodes d'acquisition sont en évolution continue, et que l'utilisation de ces systèmes d'identification par la rétine est de plus en plus sollicitée dans divers secteurs.

Caractères *Biometrics*	Universalité *Universality*	Unicité *Uniqueness*	Permanence *Permanence*	Facilité de collecte *Collectability*	Performance *Performance*	Acceptabilité *Acceptability*	Robustesse *Circumvention*
Face	Haut	Bas	Moyen	Haut	Bas	Haut	Bas
Empreinte digitale	Moyen	Haut	Haut	Moyen	Haut	Moyen	Haut
Géométrie De la main	Moyen	Moyen	Moyen	Haut	Moyen	Moyen	Moyen
Frappe sur le clavier	Bas	Bas	Bas	Moyen	Bas	Moyen	Moyen
Veines de la main	Moyen	Moyen	Moyen	Moyen	Moyen	Moyen	Haut
Iris	Haut	Haut	Haut	Moyen	Haut	Bas	Haut
Rétine	Haut	Haut	Moyen	Bas	Haut	Bas	Haut
Signature	Bas	Bas	Bas	Haut	Bas	Haut	Bas
Voix	Moyen	Bas	Bas	Moyen	Bas	Haut	Bas
Thermographie Faciale	Haut	Haut	Bas	Haut	Moyen	Haut	Haut
Odeur	Haut	Haut	Haut	Bas	Bas	Moyen	Bas
ADN	Haut	Haut	Haut	Bas	Haut	Bas	Bas
Démarche	Moyen	Bas	Bas	Haut	Bas	Haut	Moyen
Oreille	Moyen	Moyen	Haut	Moyen	Moyen	Haut	Moyen

Jain. 1999

Tableau II.3 - Les caractéristiques des différentes techniques biométriques.

Méthode	**Utilisation %**	**Nombre de points mesurables**	**Fiabilité**
Empreintes digitales	50	(80)	Assez bonne
Reconnaissance faciale	15	Selon la photo	Variable
Reconnaissance de la main	10	(90)	Bonne
iris	6	(244)	Proche de 99%
signature	< 5	Selon la signature	Variable
voix	Peu utilisé	Dépend des bruits de fond	Peu fiable
Rétine	Rare	400	Excellente

Tableau II.4 - Comparaison entre quelques méthodes d'identification biométriques.

III. Conclusion.

En résumé, l'exigence accrue pour des systèmes d'authentification fiables et commodes, la disponibilité des ressources informatiques peu coûteuses, le développement des capteurs biométriques bon marché, et les avancements dans le traitement du signal, ont contribué au déploiement rapide des systèmes biométriques dans les établissements s'étendant des épiceries aux aéroports.

L'apparition des systèmes multi-biométriques a nettement amélioré la performance des systèmes d'identification. C'est seulement une question de temps avant que la biométrie puisse s'intégrer dans le tissu même de la société et s'imposer dans notre vie quotidienne.

Par ailleurs, la biométrie n'est pas une science exacte : elle reste dépendante de la qualité des captures, du traitement de celles-ci, et donne des réponses en termes de « pourcentage de similitude ». Il faut donc tenir compte d'un facteur risque. En d'autre termes, la reconnaissance dans la plupart des systèmes biométriques n'est pas fiable à 100% comme c'était le cas pour les systèmes de reconnaissance classiques (Badge, carte à puce, mot de passe…), mais présentent bien des avantages qui leurs donnent un intérêt d'une grande importance dans la sécurité des infrastructures et des systèmes informatiques.

Bien qu'actuellement elle demeure moins utilisée que les autres techniques à cause de son caractère invasif et de son coût relativement élevé, la reconnaissance par images rétiniennes est d'une précision relativement importante et donne un résultat assez fiable. C'est pour cette raison que nous avons choisi d'étudier cette technique dans ce mémoire, et de détailler les différentes étapes depuis l'acquisition et le prétraitement des images, jusqu'à l'extraction des caractéristiques et la comparaison des signatures biométriques.

La technologie est en évolution continue et très rapide en ce qui concerne les instruments d'acquisition. Il est très probable que dans un proche avenir, d'autres techniques d'acquisition des images rétiniennes de caractère moins invasif verront le jour et permettront à cette méthode de gagner plus d'ampleur dans le marché de la biométrie.