

Introduction

Dans notre vie quotidienne, L'homme a utilisé les moyens de vérification d'identité pour accéder à plusieurs services via l'utilisation des mots passe, carte identité, etc. Néanmoins, ces éléments peuvent être oubliés, volés ou falsifiés, pour affronter ces limitations, un autre moyen de sécurité a été développé afin améliorer le niveau sécurité et construire une information propre liée de chaque individu. Cette nouvelle façon d'identification des individus est appelée la biométrie.

Les technologies biométriques sont des solutions alternative aux anciens moyens de vérification d'identité, les avantages de ces caractéristiques biométriques sont d'être universelles, c'est-à-dire présentes chez toutes les personnes à identifier. D'autre part, elles sont mesurables et unique: deux personnes ne peuvent pas posséder exactement la même caractéristique. Elles sont aussi permanentes ce qui signifie qu'elles ne varient pas ou peu au cours du temps.

Dans ce premier chapitre, nous présenterons la biométrie de manière générale, et les techniques biométriques.

1. La biométrie

1.1. La définition

La biométrie est un ensemble des technologies (appelées les technologies biométriques) qui exploitent des caractéristiques humaines biologiques et comportementales ou morphologiques. [4]

La biométrie consiste à déterminer ou vérifier l'identité d'un individu à partir de ses caractéristiques biologiques (comme l'ADN, le sang), comportementales (comme la voix, marche) ou morphologiques (comme l'empreinte digitale, l'oreille, iris). [22]

Pratiquement, n'importe qu'elle caractéristique biologique : morphologique, biologique ou comportementale, peut être considérée comme une caractéristique biométrique, dans la mesure où elle satisfait les propriétés suivantes :

- Universalité**: toutes les personnes à identifier doivent la posséder.
- Unicité**: l'information doit être aussi dissimilaire que possible entre les différentes personnes.

-**Permanence**: l'information collectée doit être présente pendant toute la vie d'un individu.

-**Collectabilité** : l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons.

-**Acceptabilité** : le système doit respecter certains critères (facilité d'acquisition, rapidité, etc.) afin d'être employé. [23]

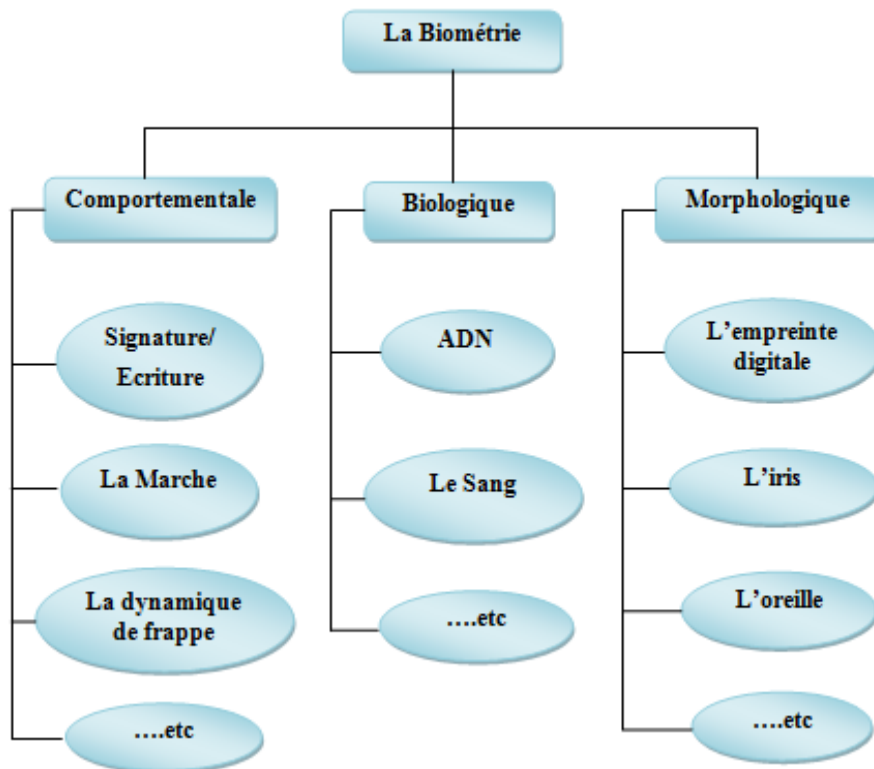


Figure 1.1 la classification de la biométrie.

1.1.1. Biologie

Cette catégorie s'appuie sur l'analyse de caractéristiques biologiques de l'individu. La prémisse à ce type d'analyse est que la donnée biologique de chaque individu constitue une signature personnelle. L'analyse biologique comprend : l'ADN, et les signaux physiologiques. Cette modalité n'est pas beaucoup utilisée pour du contrôle d'accès logique et physique. Nous ne détaillons pas plus ce type de biométrie. [23]

➤ ADN

Une empreinte génétique, ou profil génétique, est le résultat d'une analyse génétique, rendant possible l'identification d'une personne à partir d'une petite quantité de ses tissus biologiques (bulbe de cheveux, sang, salive, sécrétion vaginale, sperme).

L'empreinte génétique repose sur le fait suivant : bien que deux humains aient une large majorité de leur patrimoine génétique identique, un certain ensemble de séquences dans leur

ADN reste spécifique à chaque individu (en raison du polymorphisme). Ce sont ces séquences spécifiques d'un individu que l'analyse d'empreinte génétique permet de comparer. Si un échantillon de cellules présente la même empreinte génétique qu'un individu, on peut soutenir que ces cellules proviennent de cet individu, ou de son éventuel jumeau monozygote. Dans son acception initiale, l'expression *empreinte génétique*, est formée par analogie avec les empreintes digitales utilisées dans le cadre de l'identification des criminels, qui sont réputées propres à chaque individu. [37]



Figure 1.2 l'ADN.

➤ Le Sang

Devant une trace de sang présumée, il faut d'abord déterminer s'il s'agit bien de sang, puis s'il s'agit de sang humain avant d'essayer d'identifier son propriétaire. La caractérisation du sang a bénéficié des travaux de nombreux chercheurs.

L'identification de l'origine humaine d'une tache de sang est déterminée par des méthodes immunologiques. L'utilisation de sérum spécifique capable d'agglutiner ou de précipiter spécifiquement des éléments du sang humain permet de le distinguer du sang des autres animaux. [38]

1.1.2. Morphologiques

Elle est basée sur l'identification de traits physiques particuliers qui, pour toute personne, sont unique et permanents. Cette catégorie regroupe l'iris de l'oreille, les empreintes digitales, les traits du visage.etc.

➤ L’empreinte digitale

Les empreintes digitales sont les caractéristiques les plus populaires. Elles sont utilisées comme empreintes biométriques depuis très longtemps dans les milieux policiers et judiciaires. Elles ont de ce fait une connotation négative qui rebute souvent les utilisateurs, alors qu’ils acceptent plus facilement d’autres techniques. Elles n’en restent pas moins des biométries fiables puisque chaque individu a des empreintes digitales quasiment uniques. Ce sont les arêtes de l’empreinte qui sont pertinentes pour l’analyse. Des minuties en sont extraites. Il s’agit de points de rencontre entre arêtes, de points de séparation ou rebroussement d’arêtes ou d’autres motifs particuliers, Ils présentent des avantages comme : technologie connue et maîtrisée et relativement bon marché, par contre il contient des inconvénients : soumise aux aléas de la vie quotidienne, tels que les accidents domestiques (coupures) et risque de détérioration de l’empreinte [33].



Figure 1.3 L’empreinte digitale.

➤ Iris

L’iris est une technique extrêmement fiable car l’iris contient une infinité de points caractéristiques (ensemble fractal), la fraude étant néanmoins possible en utilisant des lentilles. L’acquisition de l’iris est effectuée au moyen d’une caméra pour pallier aux mouvements inévitables de la pupille. Elle est très sensible (précision, reflet) et relativement désagréable pour l’utilisateur car l’œil doit rester grand ouvert et il est éclairé par une source lumineuse pour assurer un contraste correct. [4]



Figure 1.4 Iris.

➤ L'oreille

En proposant l'oreille comme une nouvelle modalité de biométrie, il est nécessaire de montrer qu'elle est viable (c'est-à-dire universelle, unique, permanente, collectable). De la même manière que la personne ne peut prouver que les empreintes digitales sont uniques, il n'y a pas de façon absolue de montrer que chaque humain a une paire unique d'oreilles. Au lieu de cela, une affirmation que cela est probable peut être faite sur la base des preuves à l'appui de deux expériences conduites par Alfred Iannarelli. Il est évident que la structure de l'oreille ne change pas radicalement avec le temps. La littérature médicale indique que la croissance de l'oreille après les quatre premiers mois de naissance est proportionnelle. Il s'avère que, même si la croissance de l'oreille est proportionnelle, la gravité peut causer l'oreille à subir un étirement dans la direction verticale. L'effet de cet étirement est le plus prononcé dans le lobe de l'oreille, et les mesures montrent que le changement n'est pas linéaire. Le taux d'étirement est environ cinq fois supérieur à la normale pendant la période de quatre mois à l'âge de huit ans, après quoi il est constant jusqu'à environ 70 ans quand il augmente de nouveau. Puisque chaque individu a des oreilles, il est rationnel de conclure que l'oreille est universelle. L'oreille est également collectable en utilisant divers moyens. L'oreille humaine a trois sections principales, qui se composent de l'oreille externe, l'oreille moyenne et l'oreille interne. Elle présente des avantages sont : L'oreille est moins soumise aux conditions extérieures que l'œil par exemple. Les cheveux ou les lunettes ne gênent pas la reconnaissance, comme pourraient le faire des lentilles de contact, selon les chercheurs du domaine, la forme de l'oreille ne change pas au cours de la vie. Et des inconvénients tels que : elle est encore peu connue et peu utilisée sauf dans l'identification policière et peu de recul [30].



Figure 1.5 l'oreille.

1.1.3. Comportementales

Cette catégorie se base sur l'analyse de comportement d'un individu comme signature/Écriture, marche...ect.

➤ Signature/Écriture

Cette caractéristique peut se décliner sous plusieurs formes. Il est possible d'utiliser la signature de la personne mais également des textes écrits. De plus, elle peut s'effectuer de manière statique – comparaison du dessin du résultat uniquement – ou de manière dynamique – la «manière» d'écrire est prise en compte.

La dynamique d'une signature/écriture nécessite un matériel adéquat pour être capturée : une tablette graphique ou un stylo spécial équipé de capteurs électroniques. La vitesse, l'inclinaison du stylo, la pression exercée peuvent ainsi être calculées, en plus du dessin de l'empreinte. Une empreinte statique est plus facilement falsifiable puisqu'elle nécessite qu'un simple entraînement, tandis qu'une empreinte dynamique nécessite la réalisation fidèle d'une imitation en temps réel.

Il s'agit d'une caractéristique qui peut être combinée avec d'autres, comme la voix (on dit ce qu'on écrit), pour renforcer la sécurité des systèmes. [33]



Figure 1.6 signature/ Écriture.

➤ Marche

Chaque individu, en fonction de son corps et plus spécifiquement de sa musculature, développe une démarche qui lui est propre. En analysant, entre autres, la distance entre les pas, les enjambées, la vitesse, la cadence, l'angle des pieds, etc., il devient possible d'utiliser la démarche comme caractéristique biométrique. [33]

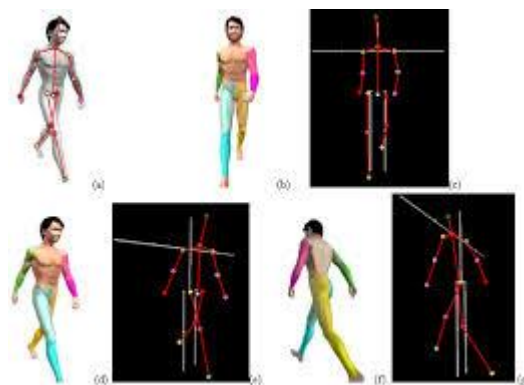


Figure 1.7 la marche.

➤ La dynamique de frappe

L'idée d'identifier une personne par sa dynamique de frappe était très attrayante parmi les perspectives de la technologie de l'information et des réseaux.

2. Les Systèmes biométriques

2.1. Définition

Un système biométrique est essentiellement un système de reconnaissance de formes qui fonctionne en acquérant des données biométriques à partir d'un individu, extrayant un

ensemble de caractéristiques à partir des données acquises, et comparant ces caractéristiques à la signature dans la base de données.

Selon le contexte d'application, un système biométrique peut fonctionner en mode d'enrôlement et mode de vérification ou mode d'identification.

➤ **Enrôlement**

L'enrôlement est la première phase de tout système biométrique. Il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois. Elle est commune à la vérification et l'identification. Pendant l'enrôlement, la caractéristique biométrique est mesurée en utilisant un capteur biométrique afin d'extraire une représentation numérique. Cette représentation est ensuite réduite, en utilisant un algorithme d'extraction bien défini, afin de réduire la quantité de données à stocker pour ainsi faciliter la vérification et l'identification. Dépendant de l'application et du niveau de sécurité souhaité, le modèle biométrique retenu, est stocké soit dans une base de données centrale soit sur un élément personnel propre à chaque personne. [23]

➤ **Identification**

En mode identification, le système doit deviner l'identité de la personne. Il répond donc à une question de type : « Qui suis-je ? ». Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données (problème de type 1 : N). En général, lorsque l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que toute personne qui utilise le système possède un modèle dans la base de données. [9]

➤ **Vérification**

En mode vérification, le système doit répondre à une question de type : « Suis-je bien la personne que je prétends être ? ».

L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de données (problème de type 1 :1). En mode vérification, on parle de problème ouvert puisque l'on suppose qu'un individu qui n'a pas de modèle dans la base de données (imposteur) peut chercher à être reconnu. [9]

2.2. Architecture d'un système biométrique

L'architecture d'un système biométrique contient cinq modules :

- Le **module de capture** qui consiste à acquérir les données biométriques afin d'extraire une représentation numérique. Cette représentation est ensuite utilisée pour l'apprentissage, la vérification ou l'identification. Il s'agit d'un capteur biométrique qui peut être de type sans ou avec contact

- Le **module de traitement d'information** qui permet de réduire la signature numérique extraite afin d'enlever l'information indésirable qui est influée sur la phase d'enrôlement. Ce module peut avoir un test de qualité pour contrôler les données biométriques acquises.

- Le **module du stockage** qui contient les modèles biométriques des utilisateurs enrôlés du système.

- Le **module de similarité** qui compare les données biométriques extraites par le module d'extraction de caractéristiques à un ou plusieurs modèles préalablement enregistrés. Ce module détermine ainsi le degré de similarité (ou de divergence) entre deux vecteurs biométriques.

- Le **module de décision** qui détermine si l'indice de similarité retourné, est suffisant pour déterminer l'identité d'un individu. [22]

2.3. Mesure de la performance d'un système biométrique

Tout d'abord, afin de comprendre comment déterminer la performance d'un système biométrique, il nous faut définir clairement trois critères principaux :

1. Le premier critère s'appelle le taux de faux rejet ("False Reject Rate" ou **FRR**). Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système. [7]

$$TFR = \frac{\text{nombre des clients rejetés (FR)}}{\text{nombre total d'accès de clients}}$$

Telle que FR Le faux rejet correspond au cas où le système rejette un client légitime.

2. Le deuxième critère est le taux de fausse acceptation (“**False Accept Rate**” ou **FAR**). Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.

$$TFA = \frac{\text{nombre des imposteurs acceptés (FA)}}{\text{nombre total d'accès imposteurs}}$$

Telle que FA correspond au cas où le système accepte un individu qui a proclamé une identité qui n'est pas la sienne. [7]

3. Le troisième critère est connu sous le nom de **taux d'égale erreur** (“**Equal Error Rate**” ou **EER**). Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations. [7]

2.4. Evaluation des performances des Systèmes biométriques

Chaque caractéristique (ou modalité) biométrique a ses forces et ses faiblesses, et le choix dépend de l'application visée. On ne s'attend à ce qu'aucune modalité biométrique ne réponde efficacement aux exigences de toutes les applications. En d'autres termes, aucun système biométrique n'est "optimal". Faire correspondre un système biométrique spécifique à une application dépend du mode opérationnel de l'application et des caractéristiques biométriques choisies. Plusieurs études ont été menées afin d'évaluer les performances des systèmes biométriques. La société américaine – l'*International Biometric Group* [IBG] – a par exemple effectué une étude basée sur quatre critères d'évaluation :

- *intrusivité*: ce critère permet de classer les systèmes biométriques en fonction de l'existence d'un contact direct entre le capteur utilisé et l'individu à reconnaître. La reconnaissance faciale est une technique « non intrusive », car il n'existe aucun contact entre le capteur (la caméra) et le sujet, elle est bien acceptée par les utilisateurs à l'inverse d'autres techniques « intrusives » comme l'iris où un contact direct est nécessaire entre le capteur et l'œil.
- *fiabilité* : dépend de la qualité de l'environnement (éclairage par exemple) dans lequel l'utilisateur se trouve. Ce critère influe sur la reconnaissance de l'utilisateur par le système. Nous verrons ce point en détail dans la section suivante.

- *coût* : doit être modéré. À cet égard nous pouvons dire que la reconnaissance faciale ne nécessite pas une technologie coûteuse. En effet, la plupart des systèmes fonctionnent en utilisant un appareil à photo numérique de qualité standard.
- *effort* : requis par l'utilisateur lors de la saisie de mesures biométriques, et qui doit être réduit le plus possible. La reconnaissance faciale est la technique biométrique la plus facile à utiliser car non contraignante. [31]

2.5. Applications des systèmes biométriques

Les applications de la biométrie peuvent être divisées en trois groupes principaux:

-Applications commerciales : telles que l'ouverture de réseau informatique, la sécurité de données électroniques, l'e-commerce, l'accès Internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance, etc.

-Applications gouvernementales : telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc.

-Applications légales : telles que l'identification de corps, la recherche criminelle, l'identification de terroriste, etc.

De nos jours les systèmes biométriques sont de plus en plus utilisés dans des applications civiles. Par exemple, le dispositif de Schiphol Privium à l'aéroport d'Amsterdam, utilise un capteur de l'iris pour accélérer la procédure de contrôle des passeports et des visas. [3]

2.6. Les limitations Les systèmes biométriques

La fiabilité d'un system biométrie est tout dépend les facteurs associes pour chaque application biométrie. Ces facteurs sont généralement intrinsèques et extrinsèques de contexte de la mise en ouvre d'une application biométrie ; ils existent plusieurs facteurs qui sont :

1 - *Bruit associes les données collectes* : Les données détectées peuvent être bruyantes ou déformées. Une empreinte digitale avec une cicatrice ou une voix altérée par le froid sont des exemples de données bruyantes. Des données bruyantes pourraient également d'être le résultat de capteurs défectueux ou mal entretenus (par exemple, accumulation de saleté sur un capteur d'empreinte digitale) ou de conditions ambiantes défavorables (par exemple, mauvaise illumination de la face d'un utilisateur dans un système de reconnaissance faciale). Les données biométriques bruyantes peuvent être associées de manière incorrecte aux modèles de la base de données, ce qui entraîne un rejet incorrect de l'utilisateur. [3]

2- *Variations intra-classe* : Les données biométriques acquises par un individu au cours de l'authentification peuvent être très différente des données qui ont été utilisées pour générer le modèle au cours de l'inscription, en affectant ainsi l'appariement processus. Cette variation est

généralement provoquée par un utilisateur qui interagit incorrectement avec le capteur figure ou lorsque les caractéristiques du capteur sont modifiées (par exemple en changeant de capteurs - le problème d'interopérabilité du capteur) pendant la phase de vérification. Comme autre exemple, la composition psychologique variable d'un individu pourrait aboutir à des traits de comportement très différents à différents moments. [3]

3- *Caractère distinctif* : Alors qu'un trait biométrique devrait varier considérablement d'un individu à l'autre, il peut y avoir de grandes similitudes inter-classes dans les ensembles de caractéristiques utilisés pour représenter ces traits. Cette limitation restreint la discriminabilité fournie par le trait biométrique. [3]

4- *Non universalité* : Alors que chaque utilisateur est censé posséder le trait biométrique acquis, en réalité, il est possible pour un sous-ensemble des utilisateurs de ne pas posséder un biométrique particulier. Un système biométrique d'empreinte digitale, par exemple, peut être incapable d'extraire des traits des empreintes digitales de certains individus, en raison de la mauvaise qualité des crêtes. Ainsi, il n'y a pas de taux d'inscription associé à l'utilisation d'un seul trait biométrique. Il a été estimé empiriquement que jusqu'à 4% de la population qui peut avoir des crêtes d'empreintes digitales de mauvaise qualité qui sont difficiles à image avec les capteurs d'empreintes digitales actuellement disponibles et entraîner des erreurs. [3]

2.7. De mono modalité vers Multimodalité

Bien que de nos jours il existe des techniques biométriques extrêmement fiables telles que la reconnaissance de la rétine ou de l'iris, elles sont coûteuses et, en général, mal acceptées par le grand public et ne peuvent donc être réservées qu'à des applications de très haute sécurité. Pour les autres applications, des techniques telles que la reconnaissance du visage ou de la voix sont très bien acceptées par les utilisateurs mais ont des performances encore trop peu satisfaisantes pour être déployées dans des conditions réelles.

Afin d'améliorer la sécurité des systèmes précédents, une première solution consiste à intégrer la biométrie avec l'identification basée sur une connaissance ou une possession. Cette méthode permet d'améliorer la sécurité du système.

La multimodalité est une alternative qui permet d'améliorer de manière systématique la performance d'un système biométrique, Par performance, nous entendons à la fois la précision du système mais aussi son efficacité, plus particulièrement en mode identification En effet, des classificateurs différents font en général des erreurs différentes, et il est possible de tirer parti de cette complémentarité afin d'améliorer la performance globale du système.

Les différentes formes de multimodalité sont les suivantes :

1. *systèmes multiples biométriques* : par exemple combiner reconnaissance du visage, reconnaissance des empreintes digitales et reconnaissance du locuteur. C'est le sens le plus classique du terme multimodal.
2. *systèmes multiples d'acquisition* : par exemple utiliser deux scanners différents (l'un optique, l'autre thermique) pour la reconnaissance d'empreintes digitales.
3. *mesures multiples d'une même unité biométrique* : par exemple faire la reconnaissance des deux iris ou des dix doigts d'un même individu.
4. *instances multiples d'une même mesure* : faire une capture répétée du même attribut biométrique avec le même système d'acquisition.
5. *algorithmes multiples* : utiliser des différents algorithmes de reconnaissance sur le même signal d'entrée. [15]

Conclusion

De nos jours la biométrie est considéré comme un moyen le plus fiable en termes de sécurité. Elle a devenu une technologie plus praticable dans différents secteurs telles que le contrôle d'accès, applications dans les téléphones portables, application dans l'e-commerce etc....

Dans ce chapitre nous avons présenté une motivation générale sur la biométrie ainsi que les applications associées à cette technologie biométrique telle que : les empreintes digitales, l'iris, l'oreille.