

1. Introduction

Dans tous les domaines de sécurité et de contrôle d'accès, on utilise des mots de passe, ou des clés qui se compose de chiffres, ou de lettres. Mais, dans ces derniers temps avec l'avancement de la technologie ces mots de passe sont devenus facilement falsifiables et franchissables. C'est pour ça, que les chercheurs de différents domaines ont orientés leurs travaux sur des clés et mots de passe impossible à falsifier, sûr et surtout efficace. La biométrie est devenue à la mode dans les domaines qui requiert un niveau élevé de sécurité et de contrôle des systèmes de reconnaissance biométriques, utilisés de plus en plus largement tant dans le domaine privé que public, comportent de nombreux avantages pour les personnes qui les introduisent et les personnes concernées. Toutefois, l'utilisation de données biométriques pour l'identification ou la vérification d'une identité prétendue comporte également des risques quant au respect des droits et des libertés fondamentales.

Le présent chapitre a pour objectif de définir la terminologie « Biométrie » et aussi « Les systèmes de reconnaissance biométriques ».

2. La Biométrie

2.1 Définition

La biométrie est un domaine émergent où la technologie améliore notre capacité à identifier une personne, pour la protection des consommateurs contre la fraude ou le vol est un des buts de la biométrie.

Tous d'abord la biométrie c'est l'étude mathématique des variations biologiques à l'intérieur d'un groupe déterminé [23], de plus le terme biométrie (*Biometrik – biometry*), fait référence à l'analyse des caractéristiques physiques d'une personne (voix, contour du visage, empreintes digitales, ...). [28]. On a trois catégories de technologies biométriques tel que l'Analyses biologiques qui contient (Odeur, sang, salive, urine, ADN, cheveux...), l'Analyses comportementales qui contient (la signature, la façon d'utiliser un clavier d'ordinateur, la voix, la manière de marcher) et dernièrement l'Analyses morphologiques (Empreintes digitales, forme de la main, traits du visage, dessin du réseau veineux de l'œil.)

L'avantage de l'identification biométrique est que chaque individu a ses propres caractéristiques physiques qui ne peuvent être changées, perdues ou volées. La méthode d'identification biométrique peut aussi être utilisée en complément ou remplacement de mots de passe.

2.2 Les caractéristiques biométriques

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques.

- ✓ *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..
- ✓ *Une haute sécurité* : en l'associant à d'autres technologies comme le cryptage, la carte à puce...
- ✓ *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'utilisateur 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. [22]

2.3 Les différentes modalités biométriques

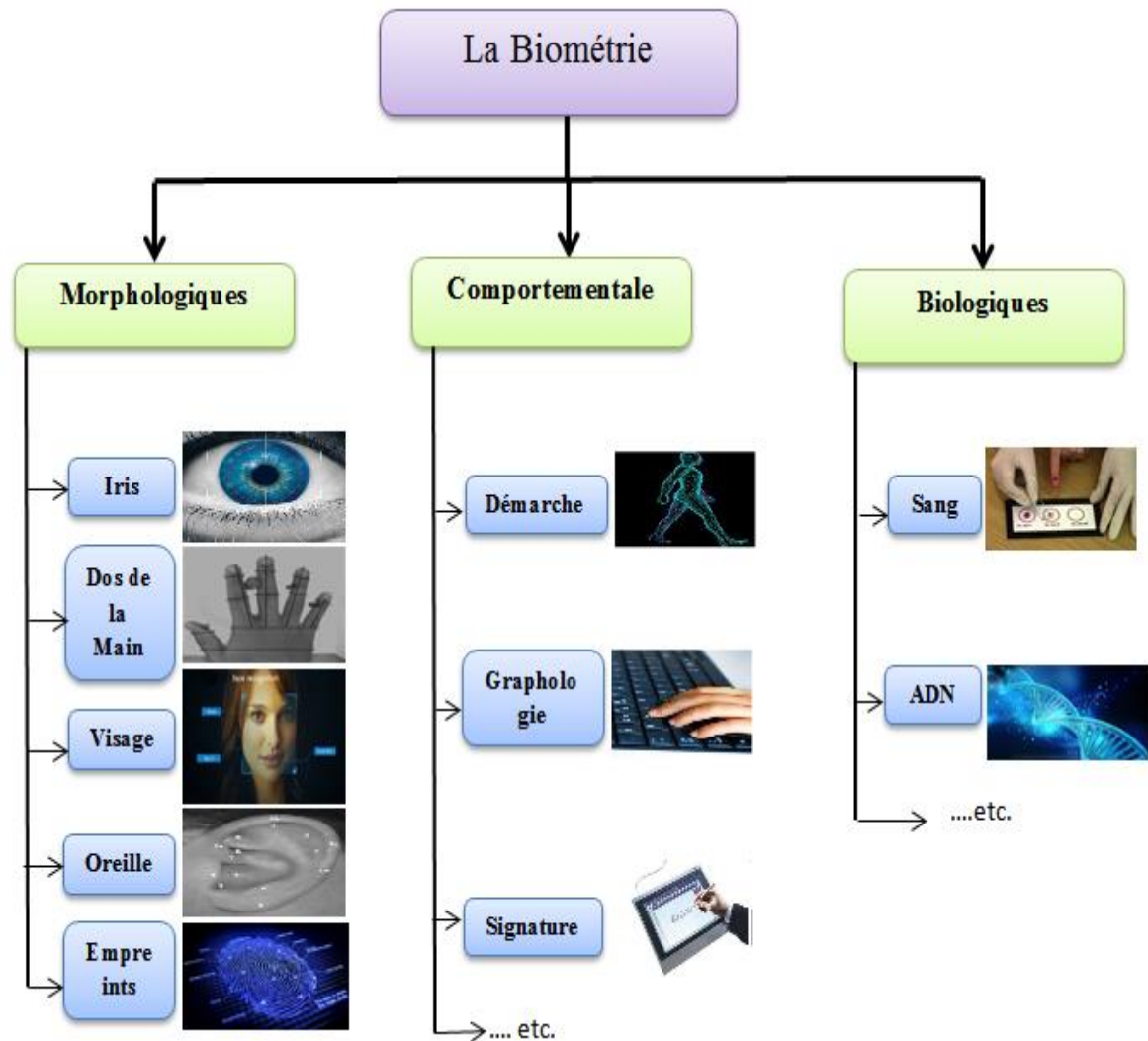


Figure 1.1 Différentes modalités biométriques.

2.3.1 Morphologiques

- **Iris**

L'iris est la partie colorée de l'œil, elle ne doit pas être confondue avec la rétine, le fond de l'œil, qui est également utilisée comme biométrie. Le dessin de chaque iris est unique et permet d'obtenir une très grande exactitude dans l'analyse. C'est une caractéristique difficile à falsifier, puisqu'elle est non seulement difficile à obtenir mais également difficile à reproduire. [27]



Figure 1.2 Image d'iris.

- **Dos de la main**

Cette caractéristique concerne la géométrie du dos de la main. Les mesures sont effectuées sur la longueur et la largeur mais également l'épaisseur des doigts avec des jeux de miroirs lors de la capture, Cette biométrie est utilisée depuis le début des années 1980. [27]

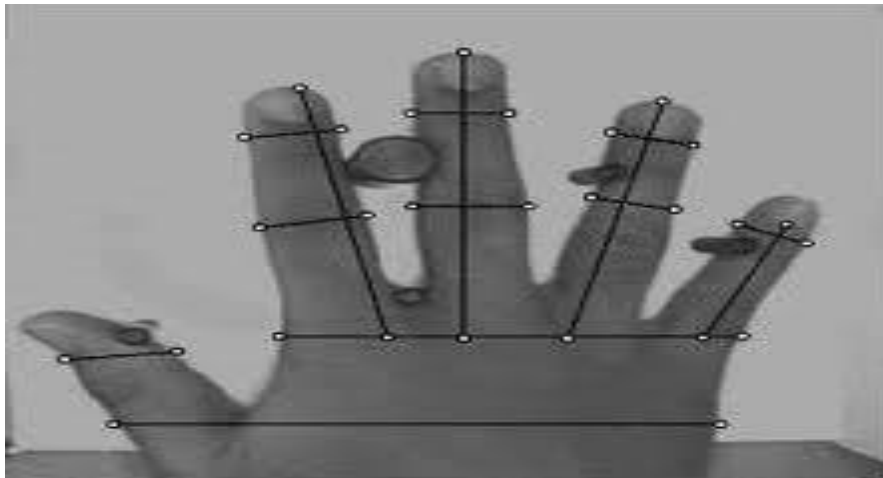


Figure 1.3 géométrie du Dos de la main.

- **Le Visage**

La biométrie du visage s'intéresse à la forme de celui-ci. Les mesures sont effectuées en particulier sur la distance entre les yeux, la longueur et la largeur du nez, la profondeur des orbites, la forme des pommettes, la longueur du menton, etc. Environ 80 points du visage peuvent être utilisés pour définir les mesures. Il s'agit d'une biométrie appréciée lorsque les connexions se font à distance au moyen d'une webcam, mais également pour les tâches de

surveillance (stades, casinos, etc.). Comme l'ensemble des biométries basées sur des images, elle n'exige que peu d'espace mémoire.

On fait une distinction entre la reconnaissance du visage en 2D, une seule caméra de face capture le visage, et la reconnaissance du visage en 3D où un mécanisme incluant plusieurs prises de vue crée un modèle en trois dimensions du visage. [27]



Figure 1.4 reconnaissance du visage.

- **Oreille**

La biométrie de l'oreille est l'une des caractéristiques les moins courantes et les moins utilisées. Elle peut rebuter l'utilisateur par son aspect peu conventionnel qui lui confèrera une image peu sécurisante. Elle présente toutefois certains avantages par rapport à la biométrie de l'œil ou du visage. Elle est ainsi moins soumise aux conditions extérieures. [27]

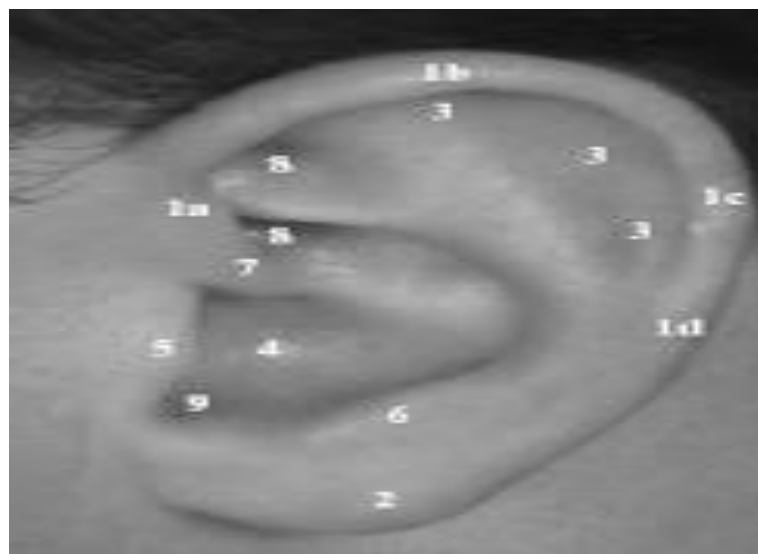


Figure 1.5 reconnaissance d'oreille.

- **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. [27]



Figure 1.6 Empreinte digitale.

2.3.2 Comportementales

- **Démarche**

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. [27]

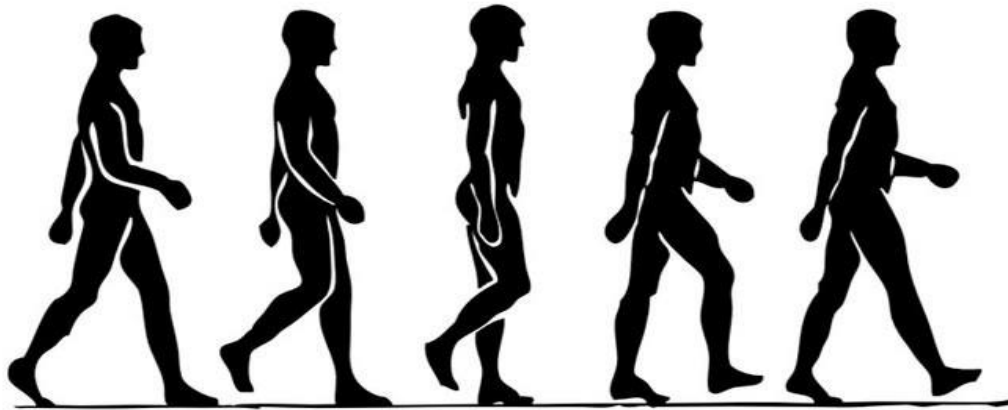


Figure 1.7 Démarche

- **Frappe au clavier (graphologie)**

Cette technique de reconnaissance biométrique est basée sur la dynamique des frappes sur le clavier. Chaque individu se distingue par le temps qu'il utilise pour appuyer sur une touche ainsi que le temps nécessaire pour passer d'une touche à la suivante. Le rythme de saisie est donc propre à chacun. Cette technique est intéressante car elle peut facilement être combinée avec la saisie d'un mot de passe par exemple. Elle remplace ainsi avantageusement l'authentification à deux facteurs. [27]



Figure 1.8 Graphologie.

- **Signature**

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 de résultat uniquement – ou de manière dynamique – la «manière» d'écrire est prise en compte.

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. [27]



Figure 1.9 La signature.

2.3.3 Biologiques

- **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. [34]

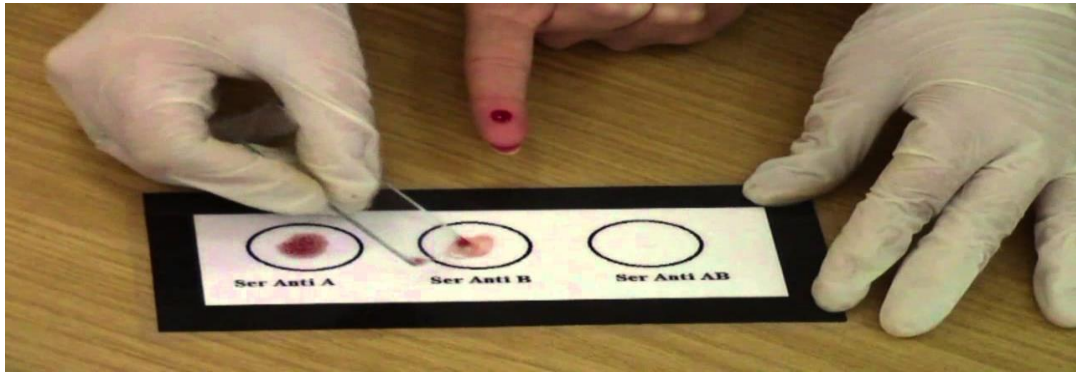


Figure 1.10 le Sang

- **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. [35]



Figure 1.11 géométrie de l'ADN.

2.4 Les Avantages et les Désavantages de ces modalités

Chaque système de reconnaissance biométrique a ses qualités et ses défauts. D'un point de vue de protection des données.

	Avantages	Désavantages
Dos de la main	<ul style="list-style-type: none"> -Technologie peu invasive et facile d'utilisation -Rapidité de traitement 	<ul style="list-style-type: none"> - Machine assez encombrante: elle nécessite de positionner la main de manière déterminée (doigts écartés, par exemple) afin d'améliorer les taux de faux rejet.
Empreinte digitale	<ul style="list-style-type: none"> -Technologie connue et maîtrisée. -Relativement bon marché. 	<ul style="list-style-type: none"> -Soumise aux aléas de la vie quotidienne, tels que les accidents domestiques (coupures). Risque de détérioration de l'empreinte.
Le visage	<ul style="list-style-type: none"> -Biométrie facile d'utilisation. -Exige peu de mémoire, donc permet un traitement rapide et suppose une technologie peu coûteuse. En effet, les lecteurs peuvent être des caméras simples, voire des webcams. 	<ul style="list-style-type: none"> -Les conditions extérieures (luminosité, ombres, positionnement de la personne, expression du visage, etc.) peuvent réduire la qualité de la reconnaissance. -La reconnaissance 3D implique un matériel beaucoup plus conséquent et plus coûteuse.
Iris	<ul style="list-style-type: none"> -Biométrie facile d'utilisation. -Exige peu de mémoire, donc permet un traitement rapide et suppose une technologie peu coûteuse. En effet, les lecteurs peuvent être des caméras numériques assez simples. 	<ul style="list-style-type: none"> -Les conditions extérieures doivent être contrôlées pour obtenir une bonne image de l'iris avant l'analyse. -La reconnaissance est plus délicate avec les personnes aux yeux bridés dont l'iris est partiellement caché.

Oreille	<ul style="list-style-type: none"> -L'oreille est moins soumise aux conditions extérieures que l'œil par exemple. -La forme de l'oreille ne change pas au cours de la vie. 	<ul style="list-style-type: none"> -Technologie encore peu connue et peu utilisée sauf dans l'identification policière. -Peu de recul.
Signature/ Écriture	<ul style="list-style-type: none"> Cette caractéristique peut être utilisée à distance, à l'aide de tablettes numériques. -Facilement combinable avec d'autres caractéristiques. -Technologie peu coûteuse et facile d'utilisation <ul style="list-style-type: none"> – tablette numérique, stylo numérique. 	<ul style="list-style-type: none"> -L'écriture et la signature évoluent avec le temps. Cela peut être plus problématique lors de l'analyse statique que dynamique. -La signature et l'écriture peuvent être conditionnées par des éléments extérieurs tels que le stress de la personne concernée.
Démarche	<ul style="list-style-type: none"> -Possibilité de reconnaître les personnes à distance. 	<ul style="list-style-type: none"> -L'identification prend beaucoup de temps parce que une image ne suffit pas, il faut une séquence qui permette de calculer les différentes mesures nécessaires à la comparaison.
Frappe au clavier (graphologie)	<ul style="list-style-type: none"> -Peu coûteuse puisque seul un logiciel est nécessaire, pas de matériel. -Facile à mettre en œuvre pour une augmentation de la sécurité des systèmes conséquente. Pas de risques de perte (badge, carte...). 	<ul style="list-style-type: none"> -Dépendant du type de clavier (QWERTY, AZERTY...). -Dépendant de conditions extérieures: le mot de passe devrait toujours être tapé de manière constante à travers le temps.

Tableau 1.1 Les Avantages et les Désavantages des modalités [27].

3. Les systèmes de reconnaissance biométriques

3.1 Définition

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Selon le contexte de l'application, un système biométrique peut fonctionner en mode d'enrôlement ou en mode de vérification ou bien en mode d'identification [8] :

- **Le mode d'enrôlement** est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier. Plusieurs campagne d'acquisitions de données peuvent être réalisées afin d'assurer une certaine robustesse au système de reconnaissance aux variations temporelles des données. Pendant cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis représentées sous forme numérique (signatures), et enfin stockées dans la base de données. Le traitement lié à l'enrôlement n'a pas de contrainte de temps, puisqu'il s'effectue « hors-ligne ».
- **Le mode de vérification ou authentification** est une comparaison "un à un", dans lequel le système valide l'identité d'une personne en comparant les données biométriques saisie avec le modèle biométrique de cette personne stockée dans la base de données du système. Dans un tel mode, le système doit alors répondre à la question suivante: *«Suis-je réellement la personne que je suis en train de proclamer?»*. Actuellement la vérification est réalisée via un numéro d'identification personnel, un nom d'utilisateur, ou bien une carte à puce.
- **Le mode d'identification** est une comparaison "un à N", dans lequel le système reconnaît un individu en l'appariant avec un des modèles de la base de données. La personne peut ne pas être dans la base de données. Ce mode consiste à associer une identité à une personne. En d'autres termes, il répond à des questions du type: *« Qui suis-je ? »*.

3.2 Modules de systèmes biométriques

Un système biométrique typique peut être représenté par quatre modules principaux :

- a. **Module de capture** : responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité...).

- b. Module d'extraction de caractéristiques :** Qui prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe.
- c. Module de correspondance :** Il compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux.
- d. Module de décision :** vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s). [4]

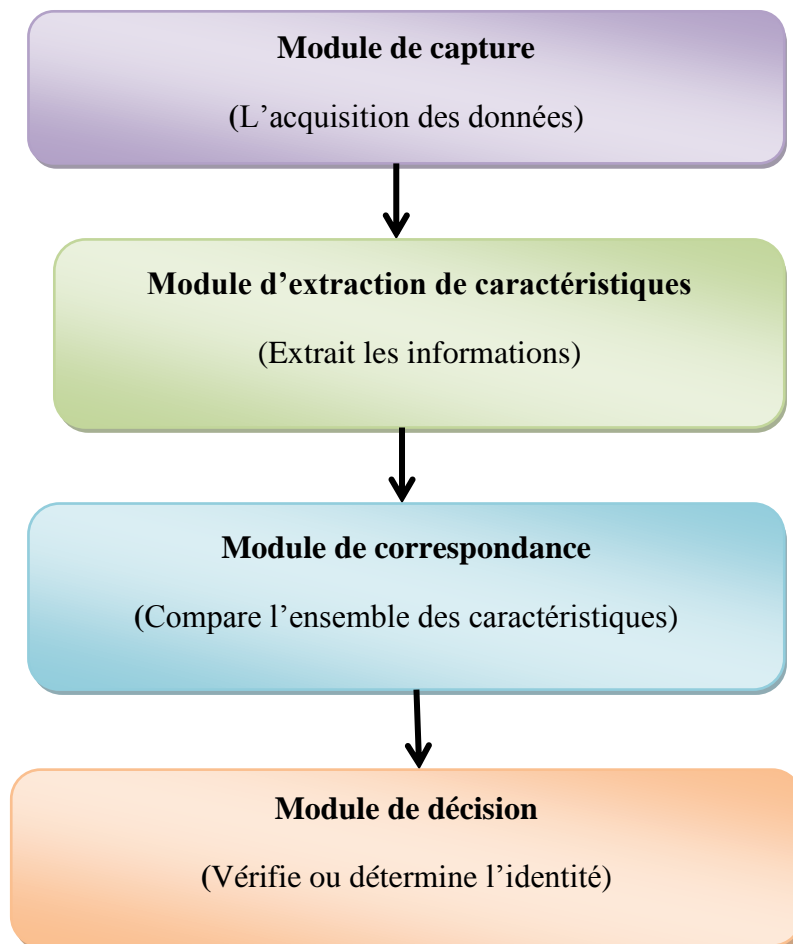


Figure 1.12 Modules de systèmes biométriques.

3.3 Limitation des systèmes Biométriques

L'installation réussie de systèmes biométriques dans diverses applications civiles n'implique pas que la biométrie soit un problème totalement résolu.

Car les systèmes biométriques qui fonctionnent en utilisant une seule caractéristique biométrique présentent les limitations suivantes : [19]

1) Bruit dans les données détectées :

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 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.

2) Variations intra-classe :

Les données biométriques acquises par un individu au cours de l'authentification peuvent être très différentes des données qui ont été utilisées pour générer le modèle au cours de l'inscription, affectant ainsi l'appariement processus. Cette variation est généralement provoquée par un utilisateur qui interagit incorrectement avec le capteur 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) 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.

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 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.

3.4 Les Système biométrique de mono vers multi modalité

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, mais elle possède les faiblesses inhérentes à l'identification basée sur une connaissance ou une possession. La multi modalité 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. [13]

3.5 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 classifier 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. [8]

3.6 Fiabilité des systèmes biométriques

Afin de mesurer la fiabilité d'un système biométrique en mode de vérification et/ou d'identification, deux principaux tests sont utilisés :

1. Test de vérification

Dans la tâche de vérification, un utilisateur final doit faire une demande d'authentification de son identité. Par exemple : il proclame "je suis Mr Dupont", alors le système biométrique doit déterminer si l'identité proclamée par l'utilisateur est acceptée ou rejetée. Deux taux sont alors calculés [8] :

❖ *Le Taux de Faux Rejets* ou False-Rejection Rate (FRR), il exprime le pourcentage d'utilisateurs rejetés alors qu'ils devraient être acceptés par le système.

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

❖ *Le Taux de Fausses Acceptations* ou False-Acceptance Rate (FAR), il exprime le pourcentage d'utilisateurs acceptés par le système alors qu'ils devraient être rejetés.

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

❖ *Le Taux d'Egale Erreur* ou Equal Error Rate (EER), il 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.

2. Test d'identification

Le test d'identification représente la mesure la plus couramment utilisée, mais il n'est pas toujours suffisant. En effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve parmi les N premières réponses du système. [8]

3.7 Les 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. [19]

Conclusion

Dans ce chapitre, nous avons présenté les différentes technologies utilisées dans les systèmes biométriques pour l'identification des personnes. Nous avons aussi donné un aperçu sur les systèmes de reconnaissances biométriques et une évaluation de leurs performances. Cette étude nous a permis de constater que les systèmes biométriques est plus efficace dans le domaine de sécurité.

Les différentes étapes de la reconnaissance de visage sont détaillées dans le chapitre suivant.