

1. Introduction

La biométrie est la science de l'établissement de l'identité d'un individu basée sur les attributs physiques, chimiques ou comportementaux de la personne. La pertinence de la biométrie dans la société moderne a été renforcée par le besoin de systèmes de gestion de l'identité à grande échelle dont la fonctionnalité repose sur la détermination précise de l'identité d'un individu dans le contexte de plusieurs applications différentes.

Dans ce chapitre, nous présenterons les technologies de la biométrie et leur fonctionnalités associées à chaque type de modalité.

2. La Biométrie

2.1 Définition

La biométrie est la science qui étudie les méthodes de vérification d'identité (authentification), qu'on utilise pour différencier des personnes entre elles en se basant sur la reconnaissance des caractéristiques biologiques (physiologiques ou comportementales) de l'individu.

Elle représente un moyen puissant de vérification d'identité dans quelques applications une fois correctement mise en application. D'ailleurs, une fois combinée avec les autres techniques de vérification (des clefs et des mots de passe) un certain niveau de sécurité peut être atteint [1].

2.2 Les caractéristiques biométriques

Pratiquement, n'importe quelle 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. [2]

2.3 Les différentes modalités biométriques

Une variété de systèmes biométriques monomodales sont à l'étude ou sur le marché, parce qu'il n'y a aucune modalité biométrique qui rassemble l'ensemble des différentes exigences (besoins). Le développement de ces systèmes biométriques, implique le coût, la fiabilité, le malaise en utilisant un dispositif, et la quantité de données requises. [1]

Les technologies biométriques d'analyse de caractéristiques, se classent en Trois catégories comme le montre dans Figure 1.1 :

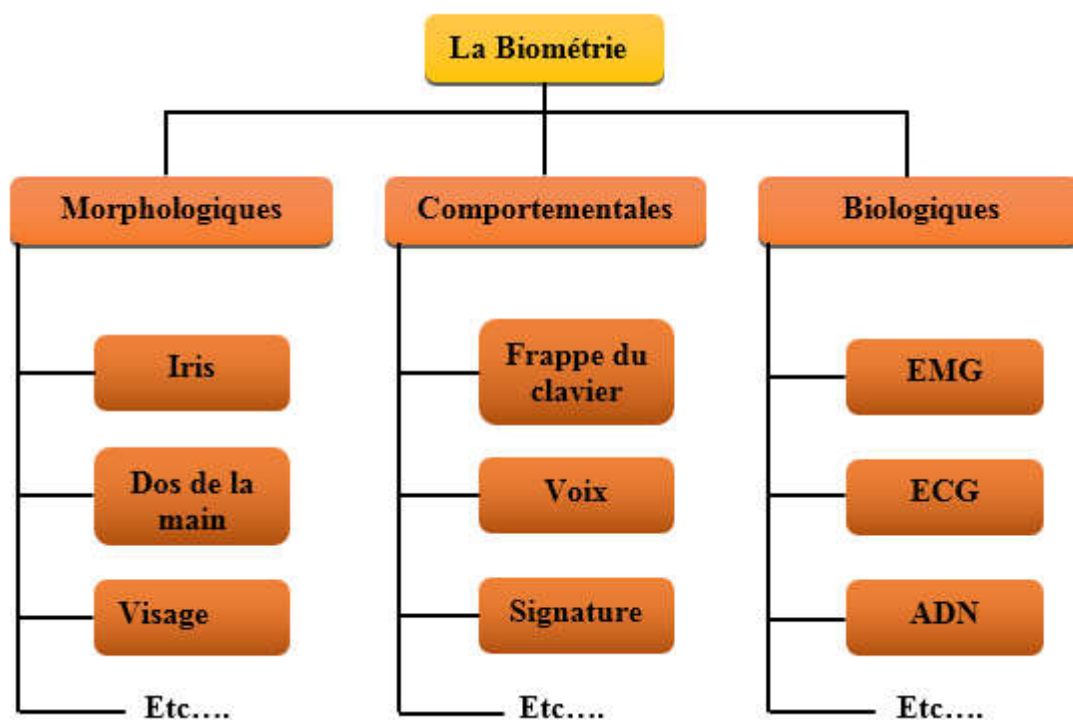


Figure 1.1 : Différentes modalités biométriques.

2.3.1 Morphologiques

- **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. [3]

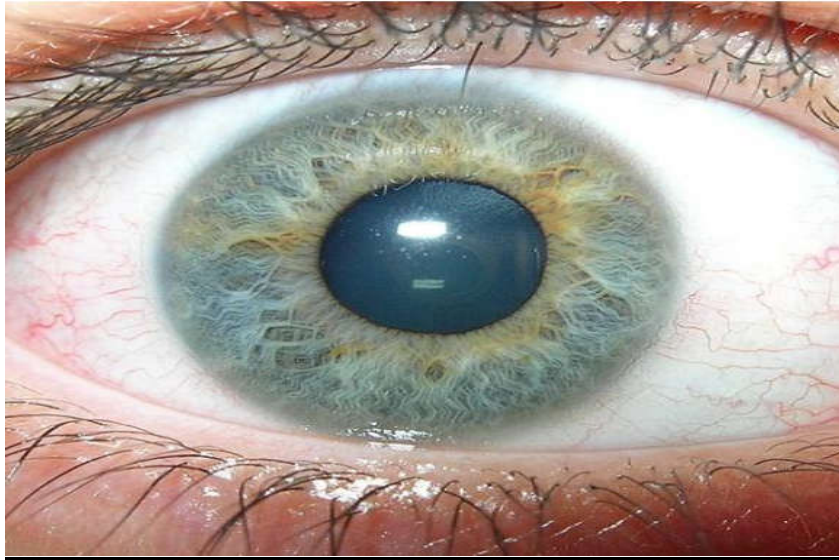


Figure 1.2 : Une texture d'Iris humain.

- **Dos de la main**

Ce type de mesure biométrique est également très répandu, notamment aux Etats-Unis. Il représente dix pour cent des applications. Il s'appuie sur une image en trois dimensions de la main. Cela consiste à mesurer plusieurs caractéristiques de la main telles que la forme de la main, la longueur et la largeur des doigts, les formes des articulations, les longueurs entre les articulations. Jusqu'à quatre-vingt-dix caractéristiques différentes peuvent être mesurées.

Cette technologie est peu sensible à l'état de la main: la saleté ou les coupures ne l'empêcheront pas de fonctionner. Elle est simple à mettre en œuvre. En revanche elle est sensible aux modifications de la forme de la main que peut provoquer le vieillissement ou encore un régime. La taille du capteur empêche son utilisation dans des applications bureautiques, dans une voiture ou encore sur un téléphone. De plus, avec cette technologie, il est assez difficile de différencier deux personnes de la même famille ou bien encore des jumeaux. [4]

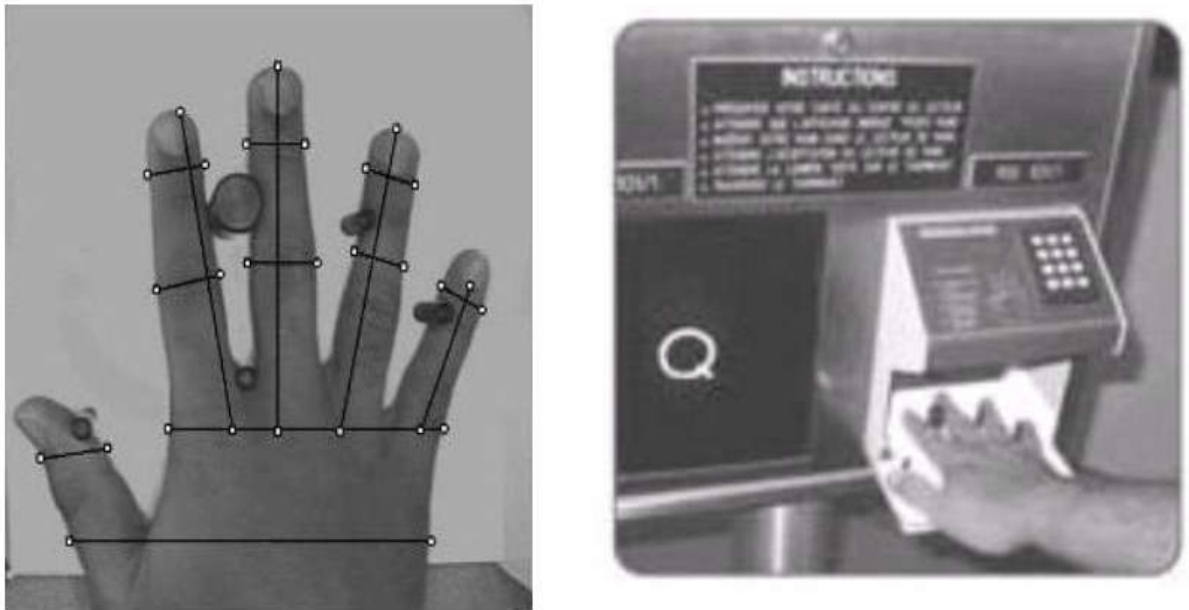


Figure 1.3 : géométrie du Dos de la main.

- **Le Visage**

C'est la technologie qui monte. Elle s'appuie sur les caractéristiques principales du visage l'éloignement des yeux, la taille de la bouche, etc. pour construire une carte du faciès [5]. Dans un système basé sur le visage, la photo d'une personne est prise volontairement ou involontairement. Un ensemble de caractéristiques, qui se veulent propres à chaque individu, sont extraites de la photo. Des exemples de ces caractéristiques comprennent des zones du visage telle que le tour du visage, la position des oreilles, les coins de la bouche, l'écartement des yeux et la taille de la bouche. D'autre part, les parties susceptibles d'être modifiées durant la vie de la personne, comme les zones occupées par des cheveux, sont évitées. Cette technique est capable de déjouer le port de lunettes, de barbe, le maquillage, etc. [6]

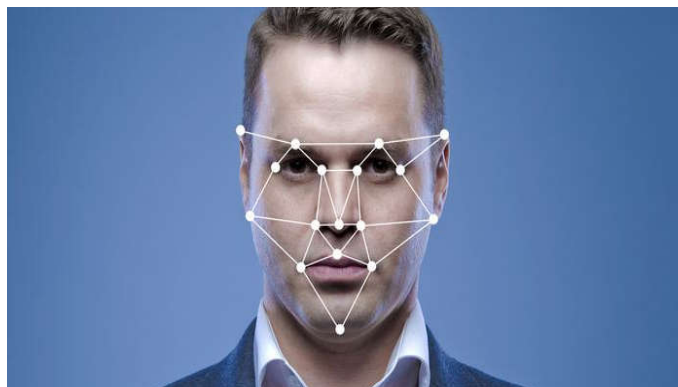


Figure 1.4 : reconnaissance du visage.

2.3.2 Comportementales

- **Frappe du clavier(graphologie)**

Cette technique est aussi appelée dactylographie dynamique. Elle mesure la façon dont l'utilisateur appuie sur les touches (temps d'appui et temps entre chaque frappe). Etant donné qu'une personne peut améliorer sa vitesse et sa technique de frappe sur un clavier, le système doit sans cesse renouveler son fichier référence.[7]



Figure 1.5 : Graphologie

- **La Voix**

La reconnaissance par voix utilise les caractéristiques vocales pour identifier les personnes en utilisant des phrases mot de passe 'pass-phrase'. Un téléphone ou un microphone peut être utilisé comme dispositif d'acquisition, ce qui rend cette technologie relativement économique et facilement réalisable, cependant elle peut être perturbée par des facteurs extérieurs comme le bruit de fond. [8]

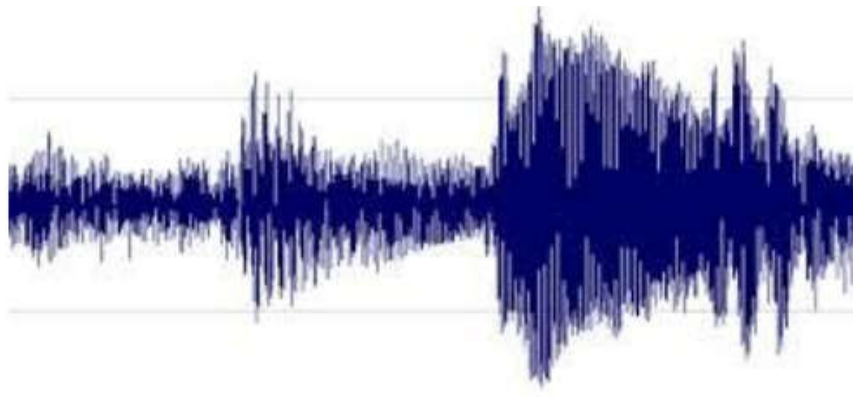


Figure 1.6 : La technologie de reconnaissance vocale.

- **La Signature**

La vérification par signature est une méthode automatique de mesure des signatures des personnes. Cette technologie examine un ensemble de dynamiques comme la vitesse, la direction, et la pression de l'écriture, le temps pendant lequel le stylo est relevé et abaissé sur le papier. [8]

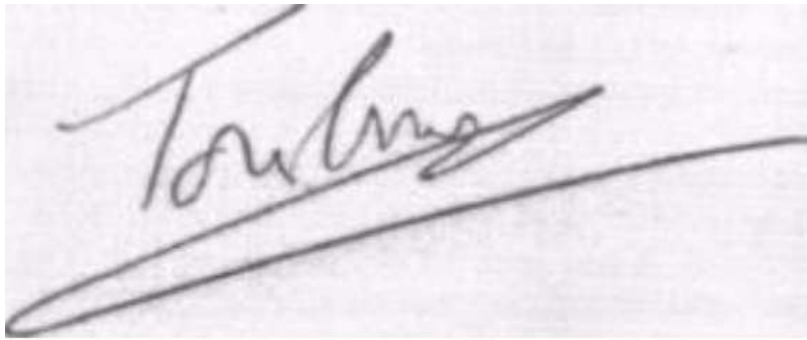


Figure 1.7 :La signature.

2.3.3 Biologiques

- **EMG**

Les signaux myoélectriques, appelés aussi électromyogrammes (EMG), sont des signaux électriques pouvant être enregistrés au niveau des muscles. L'interprétation de ces signaux peut conduire à de nombreuses applications, parmi lesquelles figure le contrôle de mains ou de bras artificiels.

Or, les électromyogrammes sont des signaux complexes, bruités et pouvant être influencés par de nombreux facteurs. Leur interprétation nécessite par conséquent de leur appliquer plusieurs traitements spécifiques.[10]

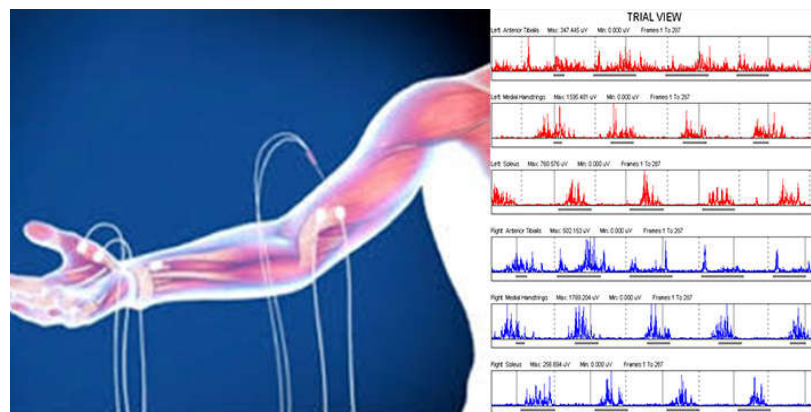


Figure 1.8 : l'EMG.

- **ADN :**

L'ADN est une double chaîne de molécules dites nucléotides qui ont 4 types: Adénine, guanine, thymine et cytosine. Cette chaîne est dans le noyau de toute cellule vivante, et définit la plupart des caractéristiques physiques des êtres vivants. Dans les êtres humains, elle diffère très peu pour les personnes directement apparentées, et elle est égale pour les jumeaux. Mais dans le reste des cas, elle permet de trancher facilement entre plusieurs individus.

Pour avoir un échantillon complet d'ADN, il faut l'extraire d'une cellule de la personne en question. Puis, par certaines procédures chimiques on peut l'extraire et le garder. La comparaison est aussi chimique ; comme la chaîne d'ADN est "double", deux chaînes ne peuvent se coller que si elles sont complémentaires, donc appartiennent à la même personne.[9]



Figure 1.9 : géométrie de l'ADN.

- **ECG :**

La validité de l'utilisation de l'ECG en biométrie est basée sur l'existence de différences physiologiques et géométriques cardiaques entre les individus humains ce qui rend le signal ECG unique pour chacun. Les différences entre les signaux ECG des différents individus sont dominées par la forme de l'onde, l'amplitude, l'intervalle PT en raison de la différence des conditions physiques du cœur. En comparaison avec les autres modalités biométriques, l'ECG est plus universel et difficile à falsifier. [17]

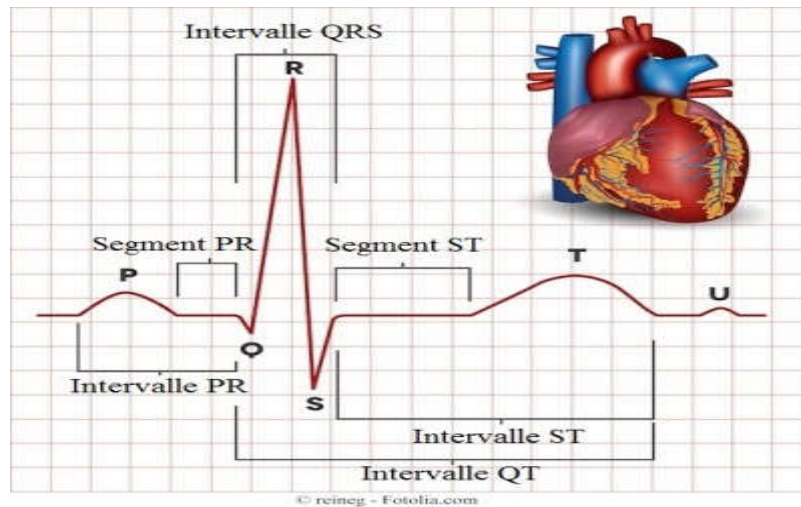


Figure 1.10 : L'ECG.

3. Les Systèmes biométriques

3.1 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. [12]

➤ 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. [13]

➤ 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. [13]

3.2 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. [14]

3.3 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. [15]

$$TFR = \frac{\text{nombre des clients rejetés (FR)}}{\text{nombre total d'accès de clients}} \quad (1.1)$$

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.

$$TFA = \frac{\text{nombre des imposteurs acceptés (FA)}}{\text{nombre total d'accès imposteurs}} \quad (1.2)$$

Telle que FA correspond au cas où le système accepte un individu qui a proclamé une identité qui n'est pas la sienne. [15]

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. [15]

3.4 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 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. [16]

3.5 Les Applications des systèmes biométriques

On distinguera quatre groupes importants d’utilisateurs de ces différentes techniques biométriques. On parlera alors de service public, application de la loi, transaction commerciale et bancaire, accès physique et logique.

- **Service public :**

Utilisée surtout pour le contrôle automatique des entrées et sorties d’un territoire, le contrôle des flux d’immigrations, dans les aéroports, on notera surtout l’utilisation de techniques telles que : l’iris, l’empreinte digitale, les traits du visage.

- **Application de la loi :**

Dans ce cas précis, la biométrie permet de faciliter certaines opérations comme l’authentification d’identité de criminels par reconnaissance automatique de leurs empreintes digitales.

Cette pratique qui a montré son efficacité se mondialise, du coup, la réalisation d’une base de données mondiale est en cours de réflexion. On trouve aussi d’autres utilisations, comme le

suivi des prisonniers à domicile assuré par des systèmes de vérification de la voix dans certains états des Etats Unis.

On trouvera même que certaines de ces techniques ont aidé à identifier des victimes lors de kidnapping ou à retrouver une identité masquée.

- **Transaction commerciale et bancaire :**

Utilisé aussi dans des opérations de commerce électronique visant à renforcer l'achat d'un bien ou d'un service.

Pour renforcer ces échanges, on a vu l'apparition de machines de retraits automatiques disposant d'un système de vérification par l'iris.

- **Accès physique et logique :**

On parle de contrôle d'accès physique lorsqu'on cherche à sécuriser l'accès à un lieu (entrée d'un bâtiment), alors que le contrôle d'accès logique concerne l'accès informatique à un terminal, serveur ou réseau informatique ou de télécommunication (ex : ordinateur, téléphone portable, base de données privée). [11]

Conclusion

Dans ce chapitre, nous avons présenté brièvement les systèmes de biométrie existants sur le marché technologique lequel se distingue par les types de fonctionnalités, le choix de modalité la robustesse et le niveau de sécurité. Ce dernier est considéré le grand challenge qui baisse les performances d'un système biométrique. Récemment, une nouvelle technologie s'appuie sur les signaux biologiques d'humaine (ECG, EEG, EMG, EOG, etc.) et devient une nouvelle gamme dans le marché biométrie.

Dans le chapitre suivant, nous allons décrire les différentes phases du système de reconnaissance de l'ECG.