

### 1. Introduction

Les systèmes biométriques sont de plus en plus utilisés depuis quelques années. L'apparition de l'ordinateur et sa capacité à traiter et à stocker les données ont permis la création des systèmes biométriques informatisés. Il existe plusieurs caractéristiques physiques uniques pour un individu, ce qui explique la diversité des systèmes appliquant la biométrie, selon ce que l'on prend en compte : L'empreinte digitale, La géométrie de la main, L'iris, La rétine, L'empreinte palmaire ... etc.

Ce chapitre est consacré à introduire quelques concepts de base de la biométrie. Nous commençons par présenter quelques définitions et nomenclatures de la biométrie. Ensuite, nous décrivons l'architecture générale des systèmes biométrique et leurs mesures d'évaluation. Enfin, nous citons quelques exemples d'application des systèmes biométriques qui existent dans la littérature.

### 2. Définition de la biométrie

La biométrie est une technique d'identification d'un individu au moyen de ses caractéristiques morphologiques : empreinte digitale, géométrie de la main, structure de l'iris ou de la rétine, le timbre de la voix, forme du visage ...etc. Les caractéristiques sont choisies pour varier peu au cours de la vie de l'individu et être différents d'un individu à un autre (même pour des jumeaux)[9].

### 3. Les techniques biométriques

Il existe plusieurs techniques biométriques utilisées dans plusieurs applications et secteurs, on peut en distinguer deux catégories :

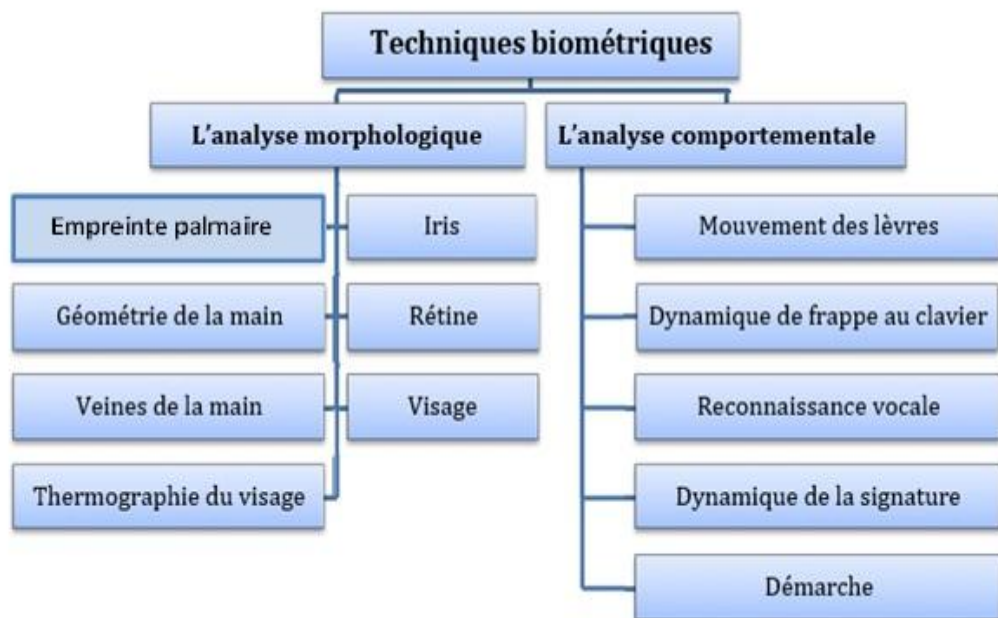
#### 3.1. L'analyse morphologique (physiologique)

Elle est basée sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe l'iris de l'œil, le réseau

veineux de la rétine la forme de la main, les empreintes digitales, les traits du visage, les veines de la main, etc.

### 3.2. L'analyse comportementale

Elle se base sur l'analyse de certains comportements d'une personne. Cette catégorie regroupe la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de la signature, l'analyse de la démarche, etc. Il existe, par ailleurs, une autre catégorie qui est l'étude des traces biologiques telles que : l'ADN, le sang, la salive, l'urine, l'odeur, etc.



**Figure 1.1-** Classification des techniques biométriques.

### 4. Modalités biométriques

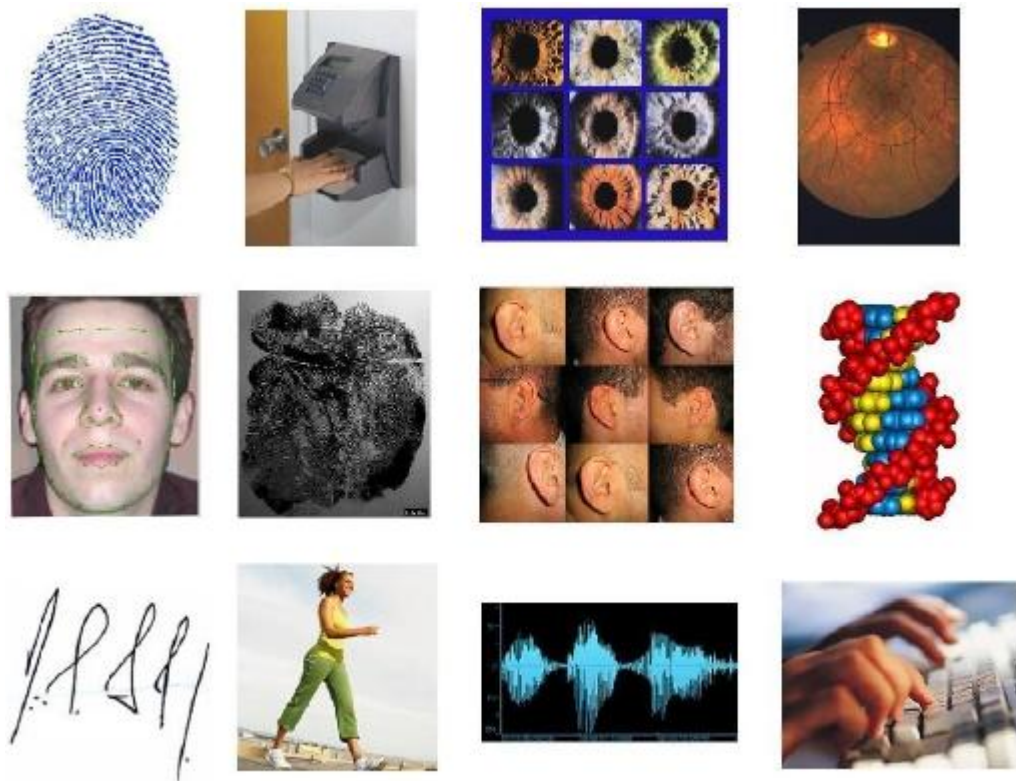
En fait, le terme biométrie regroupe plusieurs caractéristiques, traits, ou bien ce que l'on appelle : modalités biométriques. Contrairement à ce que l'on possède et que l'on peut donc perdre comme une clé, ou ce que l'on sait et que l'on peut donc oublier comme par exemple un mot de passe, les modalités biométriques représentent ce que l'on est et permettent de prouver notre identité.

Pour que des données collectées (images, audio, vidéo, etc.) puissent être qualifiées de modalité ou de trait biométrique, elles doivent être [3] :

- Universelles : exister chez tous les individus à identifier.

- Uniques : permettre de différencier un individu par rapport aux autres.
- Permanentes : suffisamment invariantes au fil du temps.
- Enregistrables : permettant d'être collectées et numérisées avec des capteurs appropriés sans provoquer un malaise excessive pour la personne.
- Mesurables : les données acquises peuvent être traitées pour en extraire des ensembles représentatifs permettant une future comparaison.

Comme le présente la Figure 1.2 empreinte digitale, la géométrie de la main, l'iris, la rétine, le visage, l'empreinte palmaire, la géométrie de l'oreille, l'ADN, la signature, la démarche, la voix et la dynamique de frappe au clavier sont les modalités biométriques les plus connus jusqu'à aujourd'hui dans le domaine de la reconnaissance biométrique.



**Figure 1.2-**Les traits biométriques connus.

### 4.1. Différentes modalités biométriques

Chacune des modalités biométriques possède ses propres capteurs, algorithmes, points forts et points faibles. Une brève introduction aux modalités biométriques, les plus courantes, est donnée dans ce qui suit :

#### 4.1.1. L’empreinte digitale

Une empreinte digitale est basée sur le modèle de crêtes et de vallées présenté sur la surface d'un doigt. La formation de cette surface est déterminée durant les sept premiers mois du développement de l’embryon. L’empreinte digitale est utilisée, dans le cadre de l’identification personnelle, depuis plusieurs décennies. Elle offre une haute précision d’identification des individus. Même les empreintes des jumeaux identiques sont discriminantes [7]. Cependant, les systèmes de reconnaissance des empreintes digitales à grande-échelle nécessitent une grande capacité de calcul [2]. De plus, l’empreinte elle-même n’est pas protégée. Elle peut être, complètement ou partiellement, déformée à cause de facteurs environnementaux et professionnels. Dans ce cas, elle devient inutile pour la reconnaissance automatique. D’autre part, l’empreinte est falsifiable parce qu’elle peut être reproduite artificiellement.

#### 4.1.2. Le visage

La reconnaissance faciale est basée sur les attributs du visage. Ces attributs sont les caractéristiques biométriques, les plus communes chez les êtres humains, utilisées pour se reconnaître entre eux. Les approches les plus courantes de la reconnaissance faciale sont fondées sur : (i) l’emplacement des attributs de visage comme les yeux, les sourcils, le nez, les lèvres et le menton, et les relations spatiales entre eux ou (ii) l’analyse globale de différentes images d’un visage afin de le représenter comme une combinaison d’un ensemble de visages (Eigen- Faces) [41]. Les systèmes de reconnaissance de visage disponibles ont montré une précision raisonnable [36]. Cependant, ils imposent un certain nombre de restrictions pendant l’acquisition de l’image faciale (sans mouvement, arrière-plan fixe, angle d’acquisition, conditions d’éclairage, etc.). D’autre part; ces systèmes ont aussi des difficultés à faire correspondre les images de visages capturées à des moments différents puisque les apparences du visage changent au fil du temps [2]. De plus, les apparences du visage peuvent être changées par esthétique.

### 4.1.3. La géométrie de la main

Les systèmes de reconnaissance de géométrie de la main sont basés sur un certain nombre de mesures à partir de la main humaine (la forme de la main, la taille de la paume et la longueur et la largeur de chaque doigt). Cette modalité est très simple, peu coûteuse, et relativement facile à utiliser [40]. Cependant, la géométrie de la main n'est pas assez discriminante pour une grande population [1]. De plus, les mesures géométriques de la main sont variables au cours de la période d'agrandissement de l'être humain. D'autre part, la grande taille du capteur de la géométrie de la main, ne permet pas son intégration sur certains dispositifs comme les ordinateurs portables [2]. Par conséquent, les domaines d'application de cette modalité sont limités.

### 4.1.4. L'iris

L'iris est la région annulaire de l'œil délimitée par la pupille de l'intérieur et la sclérotique (le blanc de l'œil) de l'extérieur. La texture de l'iris se forme pendant le développement embryonnaire et se stabilise au cours des deux premières années de la vie. La texture complexe de l'iris comporte des informations très discriminantes (chaque iris de la même personne est distinctif et même les iris de deux jumeaux identiques sont distincts) et utiles pour la reconnaissance biométrique des personnes [20]. Les systèmes de reconnaissance de l'iris, actuellement déployés, sont précis et rapides. Cela fait de l'iris une modalité adaptée pour les systèmes d'identification à grande-échelle [19]. Malgré cela, les systèmes de reconnaissance de l'iris commercialisés nécessitent une coopération des usagers lors de l'acquisition d'image. De plus, ils sont considérablement coûteux [2].

### 4.1.5. L'empreinte palmaire

Cette modalité combine quelques caractéristiques utilisées dans l'empreinte digitale et la géométrie de la main. La paume de la main contient également d'autres informations distinctives, telles que les lignes principales et les rides qui peuvent être capturées même avec un capteur à basse résolution (moins coûteux) [56]. Cependant, la grande taille des capteurs de cette modalité limite ses domaines d'application, la rendant impossible à utiliser dans certains dispositifs comme les téléphones mobiles, et les ordinateurs portables.

### 4.1.6. La signature

La façon dont une personne signe son nom est connue comme une caractéristique personnelle. Elle a été acceptée au sein de plusieurs secteurs (gouvernement, justice, commerce) en tant que méthode d'authentification [47]. Cependant, la signature d'une personne change selon les conditions physiques et l'état moral du signataire [2]. De plus, les falsificateurs professionnels sont capables de reproduire des signatures qui trompent les systèmes de reconnaissance basés sur cette modalité.

### 4.1.7. La démarche

La démarche consiste en la manière dont chaque personne marche. C'est une modalité biométrique qui peut être utilisée pour la reconnaissance des personnes à distance et par télésurveillance. Les algorithmes de reconnaissance de la démarche tentent d'extraire la silhouette. Cette dernière est un modèle de représentation du corps de la personne qui permet de dériver les attributs spatio-temporels d'un individu en mouvement [33]. Cependant, les systèmes de reconnaissance de la démarche sont encore au stade de développement [2]. De plus, la démarche d'une personne peut être affectée par plusieurs facteurs, comme le type de chaussures et de vêtements que la personne porte et la surface sur laquelle elle marche.

### 4.1.8. La voix

La voix est une combinaison d'une caractéristique physique et une autre comportementale. L'aspect physique de la voix d'un individu est décrit en fonction de la forme et la taille de la bouche, du nez, et des lèvres qui sont des caractéristiques invariantes chez une personne [2]. Cependant, l'aspect comportemental est décrit par les sons que l'on émet en parlant. Cet aspect change au fil du temps à cause de l'état émotionnel, l'âge et quelques maladies (comme la grippe) [21]. De plus, les caractéristiques de la voix sont sensibles à certains facteurs, tels que le bruit et l'écho.

### 4.1.9. La dynamique de frappe au clavier

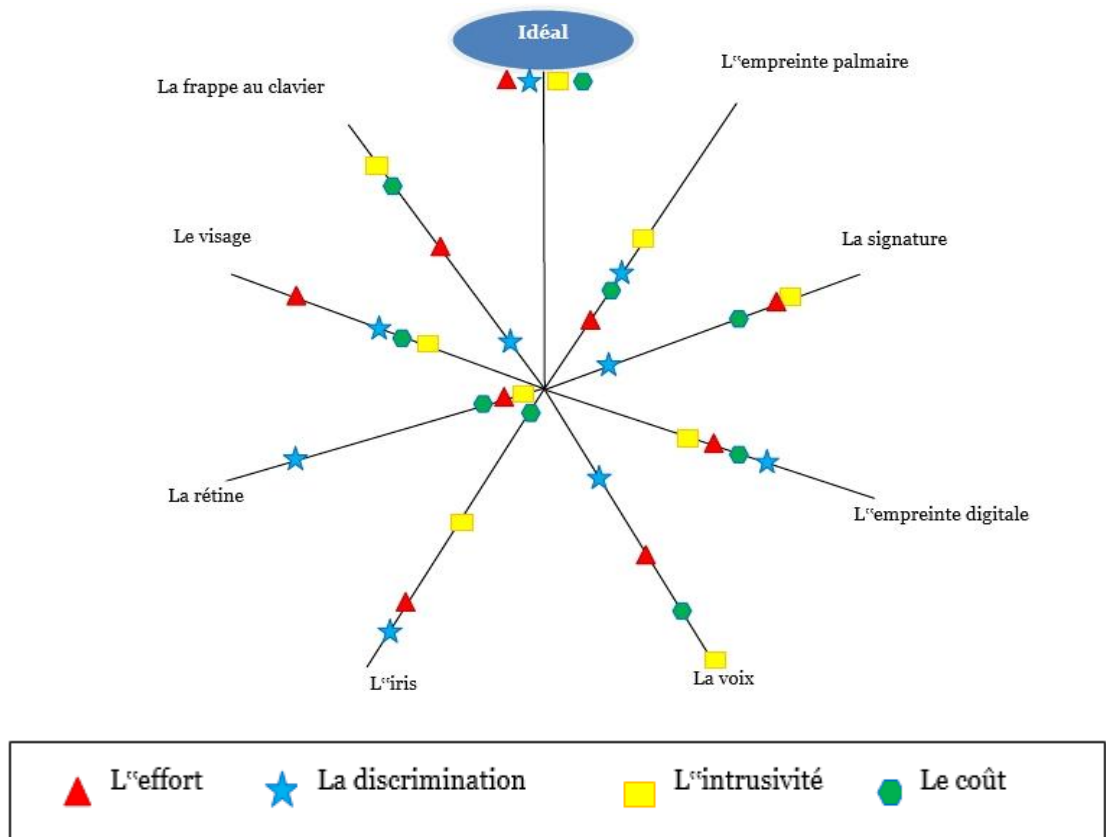
La reconnaissance de la dynamique de frappe au clavier est une nouvelle modalité biométrique émergente [1]. En effet, elle est inspirée à partir de la longue tradition de reconnaissance des opérateurs du code Morse [14]. Cette modalité est basée sur la supposition que chaque personne tape sur le clavier d'une manière particulière. Cependant, elle est fortement affectée par les changements de l'état moral de la personne, sa position, et le type de clavier utilisé [2].

### 4.2. Comparaison des modalités biométriques

Malgré l'existence de plusieurs modalités biométriques, il n'y a pas de système biométrique parfait. D'une part, le Groupe International de la Biométrie IBG (International Biometric Group) a procédé à une comparaison des différentes technologies biométriques appelée Analyse Zéphyr. Les résultats de cette comparaison sont illustrés sur la Figure 1.3- Cette comparaison est basée sur quatre (04) critères principaux :

- ✓ L'intrusivité décrit l'acceptabilité des individus à donner cette information intrinsèque pour qu'ils s'authentifient.
- ✓ La discrimination décrit le niveau de précision de la reconnaissance.
- ✓ Le coût basé, principalement, sur la valeur du capteur de trait.
- ✓ L'effort décrit le niveau de confort des utilisateurs de la modalité.

D'autre part, le CLUSIF (CLUB de la Sécurité des systèmes d'Information Français) a également proposé une autre comparaison des différentes modalités biométriques basée sur les avantages et les inconvénients de chacune. Le Table 1.1- montre le résultat global de cette comparaison.



**Figure 1.3-** Analyse Zéphyr : évaluation de différentes modalités biométriques selon quatre critères principaux : l'intrusivité, la discrimination, le coût et l'effort. Adaptée de [18]

Ces deux comparaisons permettent de choisir une technologie appropriée en fonction des contraintes liées à l'application demandée. Par exemple, on remarque que l'iris est la modalité la plus discriminante. Cela est utile pour les systèmes d'identification à grande-échelle nécessitant un haut niveau de sécurité. Cependant, cette modalité est très coûteuse et moyennement intrusive.



<b>La technique</b>	<b>Les avantages</b>	<b>Les inconvénients</b>
Empreinte palmaire	Peu coûteuse ; Facilité d'utilisation ; Taille du capteur.  Très ergonomique ; Bonne acceptabilité.	Qualité optimale des appareils de mesure (fiabilité) ; Acceptabilité moyenne ; Possibilité d'attaques.  Système encombrant ;  Perturbation possible par des blessures.
Visage	Peu Coûteuse ; Peu encombrant ; Bonne acceptabilité.	Jumeaux identiques; Psychologie ; Religion et Déguisement ; Vulnérabilité aux attaques.
Rétine de l'œil	Fiabilité ; Durabilité.	Coûteuse ; Acceptabilité faible ;
Iris de l'œil	Fiabilité. Durabilité.	Coûteuse ; Acceptabilité faible ; Contraintes d'acquisition.
Voix	Facilité.	Vulnérabilité aux attaques.
Signature	Ergonomie.	Psychologie ; Dépend de la fiabilité de la signature.
Frappe au clavier	Ergonomie.	Etat physique et psychique.

**Table 1.1–** Avantages et inconvénients des différentes technologies biométriques.

## **5. Système biométrique**

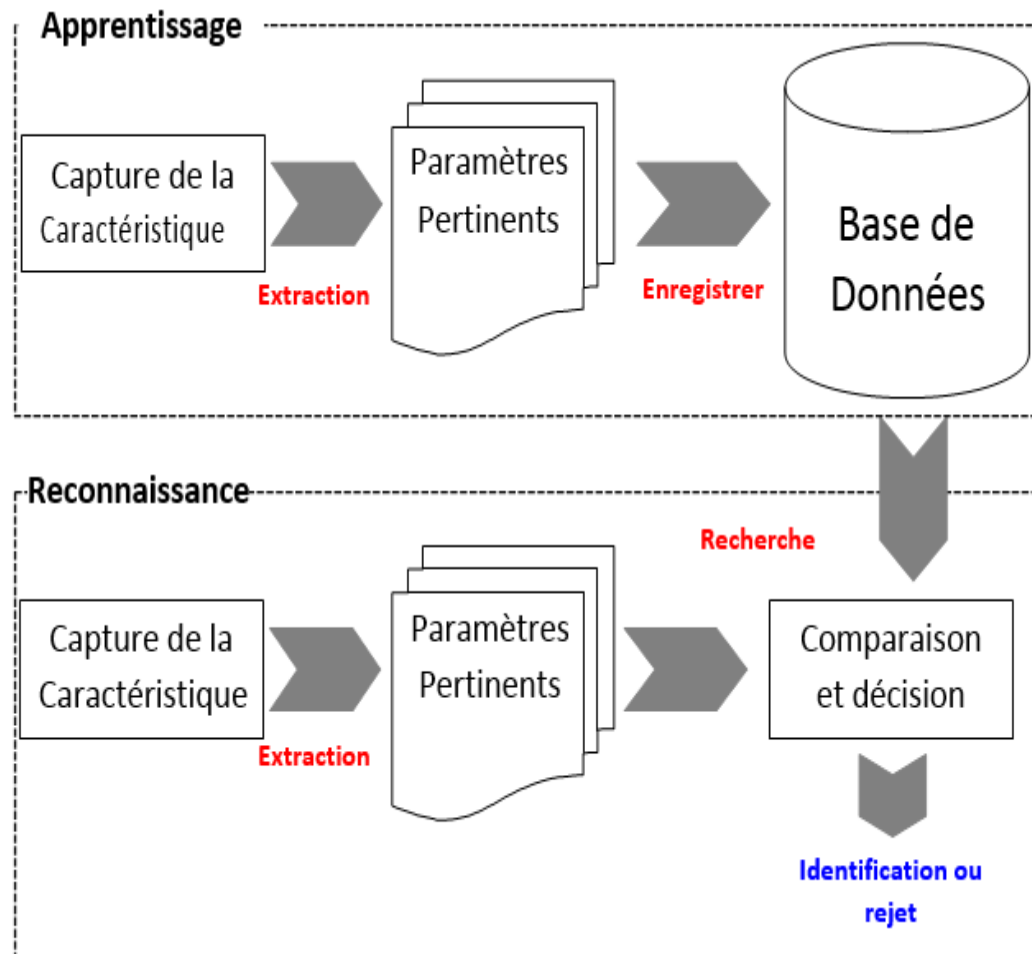
Un système biométrique est essentiellement un système qui acquiert des données biométriques d'un individu, extrait un ensemble de caractéristiques à partir de ces données, puis le compare à un ensemble de données stocké au préalable dans une base de données pour pouvoir enfin exécuter une action ou prendre une décision à partir du résultat de cette comparaison. [3]

## **6. Architecture d'un système biométrique**

Généralement, les systèmes biométriques partagent la même architecture. Cette dernière se compose de deux phases principales : une phase d'apprentissage et une phase de reconnaissance (Figure 1.4).

Tout d'abord, la caractéristique biométrique (l'empreinte digitale, l'iris, ou la signature, etc.) est enregistrée à l'aide d'un capteur spécifique. Dans les systèmes basés

sur une caractéristique morphologique, le format des données biométriques capturées est une image qui se représente par des signaux bidimensionnels [15]. Généralement, on ne procède pas directement sur ces données brutes car elles contiennent des informations inutiles pour la reconnaissance. En effet, on n'en extrait que les paramètres dit pertinents, ce qui permet de réduire significativement la taille des données à sauvegarder et aussi de simplifier le processus de reconnaissance. De plus, à partir de ces paramètres, il est impossible de revenir au signal original [9].



**Figure 1.4-**Architecture d'un système biométrique.

La phase d'apprentissage permet de constituer un modèle pour chaque personne (utilisateurs de système) à partir d'un ou plusieurs enregistrements de la caractéristique biométrique considérée.

Ces modèles sont ensuite enregistrés dans une base de données ou sur une carte à puce.

Au cours de la phase de reconnaissance, la caractéristique biométrique est capturée et les paramètres pertinents sont extraits de la même manière que dans la phase

d'apprentissage.

La suite de la reconnaissance dépend du mode opératoire du système. Si on est en mode identification, le système va comparer le signal capturé avec tous les modèles contenus dans la base de données. Puis, il va tirer le modèle le plus proche du signal pour répondre à la question : «*Qui suis-je?*». Cette tâche est difficile et très coûteuse, car la base de données peut contenir des milliers d'individus ce qui nécessite beaucoup de temps pour effectuer toutes les comparaisons possibles.

Par contre, en mode vérification, le système va comparer ce signal avec un seul modèle enregistré dans la base de données tel que la carte à puce, pour répondre à la question : «*Suis-je bien la personne que je prétends être?* ».

L'extraction de caractéristiques conduit à une représentation statistique des données. Son objectif consiste à caractériser des données grâce à plusieurs mesures qui devraient être invariantes aux transformations de données d'entrée engendrées par des conditions de capture dynamiques [2] (par exemple les changements des conditions d'éclairage). Autrement, Il est nécessaire d'identifier et de surmonter toutes les transformations de données d'entrées, comme la translation, la rotation, les changements d'échelle, les décalages, et les déformations, dans le cas où les données d'entrées sont des images. En raison de sa complexité, l'étape d'extraction des paramètres pertinents est généralement subdivisée en plusieurs modules, parmi lesquels on trouve la segmentation dans le cas où les données capturées sont des images. Elle consiste à isoler des sections ou régions de l'image capturée et localiser chaque donnée utile pour le reste du processus de la reconnaissance.

L'étape de la reconnaissance d'un système de reconnaissance biométrique consiste à recevoir les caractéristiques extraites (le vecteur de caractéristiques) et renvoyées des informations personnelles concernant l'utilisateur s'il y a une correspondance entre cette empreinte et une empreinte dans la base de données du système, et signalé que l'utilisateur n'est pas inscrit dans la base de données en cas d'échec.

L'approche traditionnelle la plus populaire pour identifier les individus par les empreintes palmaire se base sur la comparaison entre l'empreinte à identifier et toutes les empreintes et toute les empreintes de la base de données .Cette technique peut prendre beaucoup de temps si la base de données est très grande, pour cela plusieurs approches se basent sur les méthodes d'apprentissage automatique ont été proposées,

parmi ces techniques, les réseaux de neurones et les supports vecteurs machines(SVM).

### 7. Applications de la biométrie

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 machine 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).

### **8. Conclusion**

Nous avons passé en revue quelques techniques biométriques ainsi que l'architecture d'un système biométrique dans ce chapitre. Nous avons aussi relaté les applications de la biométrie, dans le but d'obtenir plus de performances. Dans le chapitre suivant, nous verrons étudiées la reconnaissance de l'empreinte palmaire.