République **A**lgérienne **D**émocratique et **P**opulaire

Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

Université des **S**ciences et de la **T**echnologie d'**O**ran **M**ohamed **B**oudiaf

Faculté de Génie Electrique **D**épartement d'Electronique

THÈSE

En vue de l'obtention du

Diplôme de Doctorat en Sciences

Présenté et Soutenu par :
BENCHENNANE Ibtissam

Intitulé

Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus

---

Spécialité : **Electronique**
Option : **Communication**

Le jury est composé de :

Professeur BOUGHANMI Nabil	**Président**	**USTO**
Professeur BENYETTOU Abdelkader	**Rapporteur**	**USTO**
Professeur BELDJILALI Bouziane	**Examinateur**	**U. Sénia**
Professeur BESSAID Abdelhafid	**Examinateur**	**U.Tlemcen**
Professeur LEHIRECHE Ahmed	**Examinateur**	**U.SBA**
Professeur OUSLIM Mohamed	**Examinateur**	**USTO**

Année Universitaire
2015 / 2016

Remerciements

Qu'il me soit permis d'exprimer ma profonde reconnaissance à ***Monsieur BENYETTOU Abdelkader***, qui m'a encouragée dans ce travail, m'a aidée et dirigée dans mes recherches .

Je tiens aussi à exprimer toute gratitude à ***Monsieur BOUGHANMI Nabil*** de m'avoir fait l'honneur d'accepter la présidence de ce jury.

Mes remerciements vont aussi à ***Monsieur BELDJILALI Bouziane*** et ***Monsieur LEHIRECHE Ahmed*** pour l'honneur qu'ils me font en acceptant d'examiner cette thèse.

J'adresse mes sincères remerciements à ***Monsieur OUSLIM Mohamed*** et ***Monsieur BENSAID Abdelhafid*** pour leur disponibilité à examiner ce travail malgré leurs multiples tâches

Je n'oublierai pas remercier l'ensemble des collègues du laboratoire SIMPA et à tous ceux qui ont contribué, de près ou de loin, par leur aide et leur soutien à la réalisation de ce travail.

Résumé :

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques.
Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance de la personne dans un grand nombre d'applications diverses. Bien que les techniques de reconnaissance biométrique promettent d'être très performantes, on ne peut garantir actuellement un excellent taux de reconnaissance avec des systèmes biométriques unimodaux, basés sur une unique signature biométrique. De plus, ces systèmes sont souvent affectés par les problèmes tels que le bruit introduit par le capteur ; la non-universalité ; le manque d'individualité et de représentation invariante ainsi que la sensibilité aux attaques. Ainsi, à cause de tous ces problèmes pratiques, les taux d'erreur associés à des systèmes biométriques unimodaux sont relativement élevés, ce qui les rend inacceptables pour un déploiement d'applications critiques de sécurité. Pour pallier à ces inconvénients, une solution est l'utilisation de plusieurs modalités biométriques au sein d'un même système, on parle alors de système biométrique multimodal. Dans cette thèse ; nous avons présenté un système d'identification multimodal combinant les informations issues de l'iris et de l'empreinte digitale. Les résultats obtenus améliorent l'identification des individus.
Mots clés : biométrie, reconnaissance des individus, bimodalité, optimisation, I.A.

Abstract:

Biometrics is a measure of the biological characteristics for identification or authentication of an individual from some of its features. This technique is used more and more today for establishing a person's recognition in many diverse applications. Although biometric techniques promise to be very efficient , it cannot currently guarantee an excellent recognition rate with unimodal biometric systems based on a unique biometric signature Furthermore, these systems are often affected by the problems such as the noise introduced by the sensor ; non- universality ; lack of individuality and representation invariant and the sensitivity to attacks. Thus, due to these practical problems, the error rate associated with unimodal biometric systems are relatively high, which makes them unacceptable for deployment of safety critical applications.
To overcome these drawbacks, a solution is the use of multiple biometric modalities in one system; it is called multimodal biometric system. In this thesis; we presented a multimodal identification system combining the information from the iris and fingerprint. The results improve the identification of individuals.
Keywords: biometric, individual recognition, bimodality, optimization, A.I.

Table des matières

LISTE DES FIGURES

Chapitre I

Chapitre II

Chapitre III

Chapitre IV

Chapitre V

LISTE DES TABLEAUX

GLOSSAIRES

Biométrie : La biométrie est la mesure ou l'analyse d'une ou plusieurs caractéristiques d'une personne à des fins d'identification.

Multimodale (biométrie) : La biométrie multimodale est une des pistes de recherche des futures applications biométriques. Elle consiste à combiner plusieurs techniques biométriques au sein d'un même système informatique, l'objectif étant de renforcer les performances et la fiabilité.

Authentification (1:1) ou 1 contre 1 :
Le lecteur biométrique compare une donnée préenregistrée à une donnée lue. Concrètement l'utilisateur saisie un code personnel (ou un badge), le lecteur recherche dans sa mémoire la donnée biométrique correspondante et la compare à la lecture faite de l'utilisateur. Les avantages de l'**authentification** (1 contre 1) sont la **rapidité** de la reconnaissance et la **certitude** de l'identité.

Identification (1 : N) ou 1 contre N : Le lecteur biométrique compare la donnée lue (l'utilisateur) à toutes les données enregistrées par le lecteur.

Le code PIN : (Personnal Identification Number) ou NIP en Français (Numéro d'Identification Personnel) est un nombre permettant d'identifier une personne.

Analyse comportementale :
Ce dit des technologies biométriques qui analysent le comportement des utilisateurs.
Les applications biométriques comportementales les plus courantes sont :
- Analyse biométrique dynamique de la frappes au clavier,
- La Reconnaissance vocale,
- Analyse biométrique dynamique des signatures.

Morphologie : Dans le milieu de la biométrie, la **morphologie** est la mesure d'une forme d'une partie d'une personne pour en créer un gabarit biométrique. Le lecteur biométrique de morphologie le plus connu est la biométrie de la forme de la main.

Enrôlement : Processus par lequel, à l'aide d'un terminal biométrique, l'identité d'une personne et son image biométrique (par exemple une image de l'empreinte digitale, ou de la forme des doigts de la main...) sont utilisés pour constituer une base de données. En général, un gabarit (en anglais : template) occupant un petit nombre d'octets est extrait de chaque image biométrique, puis stocké dans la base de données. (*Eurexem*)

Critère de performance : critère prédéterminé établi pour évaluer la performance d'un système biométrique

Degrés de liberté : Nombre de caractéristiques statistiquement indépendantes d'une donnée biométrique.

Taux d'égal erreur (TEE) ou point d'équivalence des erreurs (ou taux d'exactitude croisée), correspond à l'intersection des deux courbes précédentes. Plus ce taux est faible, plus le système est considéré comme performant.

Taux de fausse acceptation (TFA) : représente le pourcentage d'individus acceptés par erreur (fraude ou défaillance du système).

Taux de faux rejet (TFR) : représente le pourcentage d'individus rejetés par erreur.(voir Évaluation de la performance) .

Données biométriques :
Les informations extraites d'une mesure biométrique seront enregistrées en données biométriques. Cet ensemble de données biométriques est aussi appelé gabarit ou template. Ces données serviront de référence pour identifier l'utilisateur lors de la lecture.
Eigenface: L'eigenface est un ensemble de vecteurs utilisés dans les problèmes informatiques de reconnaissance faciale.

Appariement : vérification de la similarité entre deux empreintes

INTRODUCTION GENERALE

Introduction Générale

La sécurité des systèmes d'information est devenue un domaine de recherche d'une très grande importance. La conception d'un système d'identification fiable, efficace et robuste est une tâche prioritaire. L'identification de l'individu est essentielle pour assurer la sécurité des systèmes et des organisations. Elle correspond à la recherche de l'identité de la personne qui se présente dans une base de données et peut servir à autoriser l'utilisation des services. L'exemple de contrôle d'accès à une zone très sécurisée pour laquelle seul un nombre restreint de personnes (enregistrée dans une base de données) y ont accès. Elle peut être également utilisée par la police judiciaire .

De nos jours, peut être mise à contribution pour reconnaître des individus, grâce à des appareils couplés à des programmes informatiques complexes.

Pour répondre à ces besoins, la biométrie semble être une solution pratique, efficace et dont le coût en effort et en argent est en constante diminution. En effet, cette technique connaît un développement fulgurant. Cet engouement entraîne le développement de méthodes biométriques très variées : des plus classiques, comme l'étude des empreintes digitales [Jai97] ou de l'iris [Tis03], aux plus exotiques comme la reconnaissance de la démarche [Yam02], la reconnaissance de la forme de l'oreille [Yan05]. Les industriels proposent de plus en plus, pour les problèmes exigeant énormément de sécurité, de ne plus utiliser une seule caractéristique mais de mettre en place un système basé sur des combinaisons de différents moyens biométriques afin d'accroître encore la sécurité.

Grace à la puissance de calcul grandissante des ordinateurs, les applications biométriques sont devenues de plus en plus nombreuses et efficaces. Elles permettent d'apporter un niveau de sécurité supérieur en ce qui concerne des accès logiques (ordinateurs, comptes bancaires, données sensibles, etc.), ou des accès physiques (bâtiments sécurisés, aéroports, laboratoires, etc.)

Cependant, la biométrie comporte des points d'imperfections. En effet, actuellement, il y a encore bien souvent trop peu de réflexions avant l'implémentation d'une solution biométrique, que ce soit au niveau de la méthode choisie, des contraintes imposées aux usagers ou du niveau de sécurité choisi.

L'autre point critique des systèmes biométriques concerne leur fiabilité et les mécanismes de reconnaissance ou d'authentification à mettre en œuvre.

Dans ce travail de thèse, nous développons un procédé d'identification biométrique multimodal combinant l'iris et les empreintes digitales. Notre étude se base sur la classification en utilisant une méthode intelligente d'apprentissage supervisée, c'est l'un des algorithmes des systèmes immunitaires artificiels (AIRS : *A*rtificial *I*mmune *R*ecognition *S*ystem).

Cette thèse est organisée comme suit :

Les deux premiers chapitres sont consacrés à une introduction aux systèmes de reconnaissance biométrique et un aperçu sur la multimodalité et leurs différentes architectures. Nous présentons à la fin du second chapitre, les différents niveaux de fusion possibles et les techniques associées.

Un état de l'art des reconnaissances par l'iris et par l'empreinte digitale et les étapes typiques de la conception de chaque système sont présentés dans le troisième chapitre.

Le quatrième chapitre est consacré à la présentation du système immunitaire naturel, les systèmes immunitaires artificiels et les différents algorithmes inspirés du système immunitaire naturel, nous présentons en détail l'algorithme AIRS qui sera implémenté dans la classification des pièces des deux modalités utilisées dans notre étude.

Le cinquième chapitre est consacré à l'implémentation et à la fusion des systèmes d'identification multimodaux.

Enfin, la conclusion générale donnera les résultats obtenus et quelques perspectives.

CHAPITRE I :

LA BIOMETRIE

LA BIOMETRIE

I-1Définition :

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques: comportementales (exemple de la dynamique de frappe au clavier), physiques ou physiologiques (exemple de l'ADN)

Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance des personnes dans un grand nombre d'applications diverses.

Le mot biométrie est une traduction du mot anglais « biométrics » qui correspond en français à l'anthropométrie. Il désigne dans un sens très large l'étude quantitative des êtres vivants, mais dans le contexte de la reconnaissance d'individus il est défini par :

1. Selon le CLUSIF (Club de la Sécurité des systèmes d'Information Français) La biométrie est la science qui étudie à l'aide des mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé.
2. Selon la RAND (Public Safety and Justice), la biométrie est définie comme toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier son identité.
3.

Pour reconnaître un individu, on extrait des paramètres de l'image photographiée (empreinte, face, iris...) puis on compare le gabarit obtenu avec tous les paramètres précédemment extraits et sauvegardés.

Les techniques biométriques permettent la mesure et la reconnaissance de **ce que l'on est**, à la différence d'autres techniques de même finalités, mais permettant de mesurer ou vérifier **ce que l'on possède** (cadre, 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.

I-2 Un bref historique de la biométrie :

Dans la Chine des dynasties, les documents étaient signés à l'aide d'empreintes digitales. Selon le rapport de l'explorateur Joao de Barros. Il a écrit que les marchands chinois relevaient les empreintes des mains et des pieds des enfants de jeune âge sur du papier en utilisant de l'encre afin de les distinguer les uns des autres. C'est une des méthodes les plus anciennes de la biométrie en pratique et elle est toujours utilisée de nos jours. Dans les échanges commerciaux de Babylone, 3000 ans avant-J.-C., le même système était utilisé. En Amérique précolombienne, nombre d'architectes laissèrent également la trace de leurs mains colorées sur les parois de grottes aménagées. [Cha09].

Mais ce n'est qu'au début du XVIIIème siècle que le Docteur Henri Faulds développe l'utilisation de traces de doigt pour l'identification des personnes. A la même époque, l'anglais Francis Galton réalise des travaux de mesures de corps humains et crée une table de statistiques basée sur les tailles et les poids des personnes. Il met au point la méthode "Fingerprints" qui établit l'unicité et la permanence des figures cutanées. En 1881, le médecin italien Cesare Lombroso tente de prouver que l'humain criminel présente des caractéristiques repérables et stables. Ainsi, le poids du cerveau des honnêtes gens pèserait entre 1475 et 1550 grammes tandis que celui des criminels serait d'à peu près 1455 grammes. Ces théories, non fondées scientifiquement, sont vite abandonnées. En 1885, Alphonse Bertillon ne laisse cependant pas de côté cette hypothèse, responsable de l'identité

judiciaire en France, il construit "le Bertillonage" qui s'appuie sur les mensurations des criminels. Le principe connaît un vif succès jusqu'au jour où une erreur judiciaire grave vient détruire le rêve de ségrégation.

Après l'échec du Bertillonage, la police a commencé à utiliser la technique des empreintes digitales, qui a été développée par Richard Edward Henry de Scotland Yard, ressemblant essentiellement aux mêmes méthodes employées par les Chinois durant des années. Au XIXème siècle, la police criminelle fait considérablement avancer la recherche du fait de la multiplication des Analyses d'Indices Biologiques (ADN) [Mor 09]

Dans les trois dernières décennies, la biométrie a évolué d'une seule méthode simple (empreintes digitales) vers plus de dix méthodes discrètes. Les sociétés de biométrie comptent des centaines de nouvelles méthodes appliquées et continuent à améliorer leurs méthodes de sécurité tant que la technologie répond à leurs exigences. Les prix du hardware requis continuent à baisser rendant des systèmes faisables pour de faibles et moyens budgets.

Cependant le développement de l'industrie, fait ainsi le souci du public concernant les libertés et l'intimité. Des lois et des règlements continuent à être rédigés et des normes commencent à être mises en place. Tandis qu'aucune autre technique biométrique n'a encore atteint le succès de l'utilisation de l'empreinte digitale, certaines commencent à être employées dans des secteurs d'activité judiciaire et commerciale.

Aujourd'hui, la biométrie est une technologie à part entière qui utilise des critères permanents, uniques et infalsifiables. Elle permet de garantir la sécurité des accès aux environnements physiques et numériques et révolutionne du même coup le e-business et le e-commerce.

I-3 Les Systèmes biométriques et leurs modes de fonctionnements :

En général un système biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à un individu : physique ou comportementale. Il est basé sur l'analyse de données liées à l'individu qui peuvent être classées en trois grandes catégories : analyse basée sur la morphologie, analyse de traces biologiques, l'analyse comportementale.

Il peut être représenté par quatre modules principaux :

1. **Le module de capture** est 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, etc.,)

2. Le module d'extraction de caractéristiques 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. Généralement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classes,

4. **Le module de correspondance** 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.

4. Le 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).

I.4. Les différentes techniques de la biométrie :

Les techniques biométriques se divisent en deux groupes selon la coopération ou non de l'individu :

1. **Techniques intrusives :** Ces techniques requièrent un contact physique avec l'individu pour l'identifier, tel que les empreintes digitales, la rétine, l'ris ou la forme de la main. Leur usage est généralement mal accepté.

2. **Techniques non intrusives :** Ces techniques ne requièrent pas la coopération de l'individu en question. Leur application peut se faire à distance en utilisant des capteurs qui ne nécessitent pas de contact directe avec l'utilisateur (visage, démarche,…).

La biométrie permet l'identification ou l'authentification d'une personne sur les bases de données reconnaissables et vérifiables qui lui sont propres.

Figure I.1 : Différentes modalités biométriques

On peut classer les techniques biométriques en trois catégories :

1- **Celles basées sur l'analyse de traces biologiques** : ce type de biométrie se fait à l'aide de l'ADN d'une personne, de son sang, ou de sa salive…

2- **Celles basées sur l'analyse comportementale :** se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, l'empreinte de sa voix, sa démarche et sa façon de taper sur le clavier.

3- **Celles basées sur l'analyse morphologique** : est basée sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance de la forme du visage, de la forme de la main, des empreintes digitales, de la rétine et de l'iris de l'œil.

Ces éléments ont l'avantage d'être stables dans la vie d'un individu et ne subissent pas autant les effets du stress par exemple, que l'on retrouve dans l'identification comportementale

Toutefois, dans un système biométrique pratique (à savoir, un système qui utilise la biométrie à des fins personnelles de reconnaissance), il y a un certain nombre d'autres questions qui devraient être considérées, y compris:

- **La performance,** qui se réfère à la précision de la reconnaissance et de la vitesse possible ainsi que les ressources nécessaires pour obtenir cette précision de la reconnaissance et de la vitesse désirées. La performance se réfère également au fonctionnement et aux facteurs environnementaux qui influent sur la précision et la vitesse;
- **L'Acceptabilité,** qui indique la mesure dans laquelle les gens sont prêts à accepter l'utilisation notamment d'un identifiant biométrique (caractéristique) dans leur vie quotidienne;
- **Le contournement,** ce qui reflète la façon dont le système peut facilement être dupe en utilisant des méthodes frauduleuses.

Les technologies les plus fréquemment utilisées sont les suivantes :

I.4.1. Analyses biologiques :

I. 4.1. 1. L'odeur corporelle :

Chaque personne dégage une odeur qui lui est particulière. Les systèmes biométriques qui exploitent cette technologie analysent les composantes chimiques contenues dans l'odeur pour ensuite les transformer en données comparatives.

I. 4.1. 2. L'A.D.N. (Support matériel de l'hérédité):

Présent dans les cellules du corps, il est spécifique d'un individu à un autre et permet de l'identifier de manière certaine à partir d'un simple fragment de peau, d'une trace de sang ou d'une goutte de salive.
Actuellement, le temps requis pour une analyse et le coût associé à celle-ci restreignent son utilisation dans des domaines autres que celui de l'identification judiciaire. Cependant, ce procédé biométrique fait l'objet de recherche intensive puisqu'il représente la technologie d'identification par excellence avec une marge d'erreur bien en dessous des autres moyens biométriques.

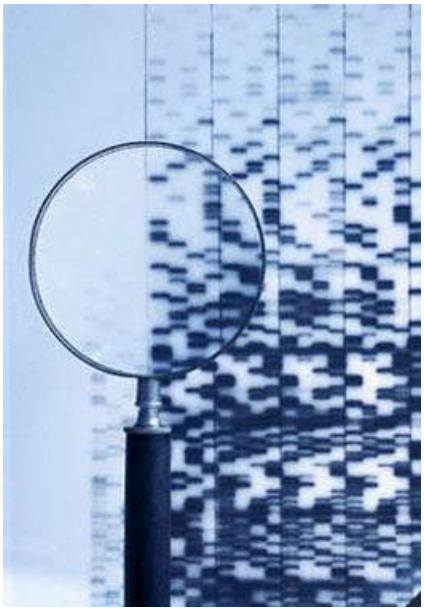


Figure I.2 : L'ADN [Cha09].

I. 4.1. 3. La reconnaissance de la thermographie faciale :

Une caméra infrarouge capte la chaleur émise par la peau. Contrairement à la reconnaissance faciale, on peut donc l'utiliser même dans l'obscurité ou de mauvaises conditions de visibilité. Mais les conditions de prise de vue peuvent conduire à des erreurs

I. 4.2. Analyses morphologiques :

I. 4.2. 1. Les empreintes digitales :

Un système biométrique utilisant l'empreinte digitale comme moyen d'identification ou de vérification ne procède pas de la même façon, ce n'est pas l'image de l'empreinte digitale qui sert de point de comparaison, mais l'ensemble des données biométriques qui est tiré à partir des minuties de l'empreinte digitale. Les minuties représentent les fins de crêtes, les bifurcations,

les lacs, les Lots et les points qui composent l'empreinte digitale. La combinaison des minuties est quasi infinie. L'acquisition des données est faite par un capteur électronique de type optique, thermique, capacitif ou à ultrasons. Cette dernière est considérée comme la plus fiable, mais aussi la plus coûteuse (voir figure I.3).

Le recours à l'empreinte digitale compte pour plus du tiers du marché des procédés biométriques. Elle représente nettement la solution préférée des entreprises œuvrant dans ce domaine. La force de ce procédé tient au fait que l'utilisation de l'empreinte digitale est plus facile à accepter par la communauté et qu'elle est une des plus efficaces et des moins coûteuses. La qualité d'image de l'empreinte digitale peut varier selon que la peau du doigt est sale, trop humide ou trop sèche, huileuse ou affligée d'une coupure.

Figure I.3 : La reconnaissance de l'empreinte digitale

I.4.2. 2. La Géométrie de la main :

La reconnaissance de la forme de la main est considérée comme l'ancêtre des technologies biométriques. A la fin des années soixante, Robert P. Miller déposa un brevet pour un appareil permettant de mesurer des caractéristiques de la main et de les enregistrer pour comparaison ultérieure, l'utilisateur place sa main sur un gabarit. Le tout est éclairé par une lumière infrarouge et l'image est captée par une caméra digitale. Prés d'une centaine de caractéristiques sont extirpées de l'image et converties en données stockées en mémoire, lors de la phase d'enrôlement ou comparées lors de la phase d'identification. Ces données concernent la longueur, la largeur et l'épaisseur de la main, de même que la forme des articulations et la longueur inter articulations.

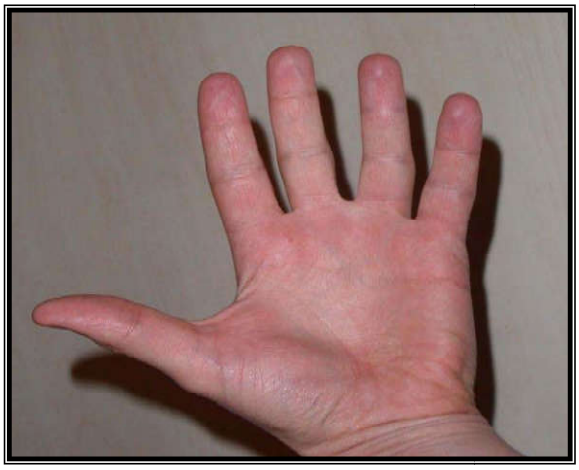


Figure I.4 : La reconnaissance de la main

I. 4.2.3 La reconnaissance de la rétine :

La rétine est la « pellicule photographique » de l'œil. Elle est constituée de 4 couches de cellules et est située au fond de l'œil.

Les éléments qui permettent de distinguer deux rétines sont les veines qui les tapissent. La disposition de ces veines est stable et unique.

La biométrie par la rétine procure également, un haut niveau en matière de reconnaissance. Cette technologie est bien adaptée pour des applications de haute sécurité (sites militaires et nucléaires, salles de coffres forts, etc.). La disposition des veines de la rétine assure une bonne fiabilité et une haute barrière contre la fraude.

L'utilisateur doit placer son œil à quelques centimètres d'un orifice de capture situé sur le lecteur de rétine. Il ne doit pas bouger et doit fixer un point vert lumineux qui effectue des rotations. A ce moment, un faisceau lumineux traverse l'œil jusqu' aux vaisseaux sanguins capillaires de la rétine. Le système localise et capture ainsi environ 400 points de référence. Après la capture d'une image de la rétine, le logiciel du dispositif de lecture découpe un anneau autour de la fovéa. Il repère l'emplacement des veines et leur orientation. Puis il les codifie dans un gabarit. Les algorithmes de l'opération restent relativement complexes.

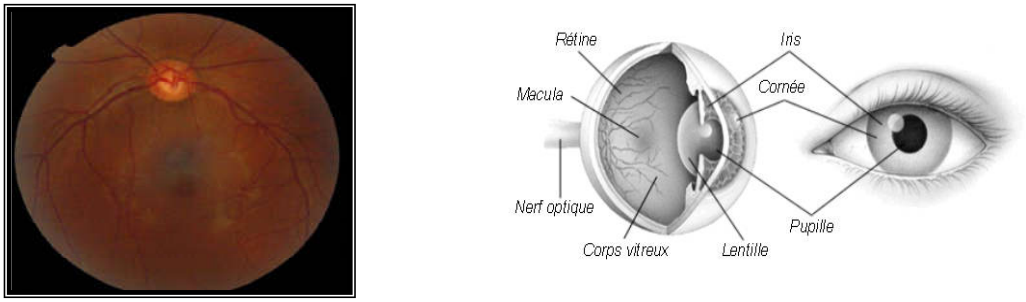


Figure I.5 : la reconnaissance de la rétine

I. 4.2.4 La reconnaissance de l'iris :

C'est une technologie fiable ; et semble être beaucoup plus précise que certains autres moyens biométriques. Ceci s'explique par le fait que notre iris comporte énormément de caractéristiques pouvant varier d'un individu à l'autre. L'iris se compose de vaisseaux sanguins et ceux-ci sont disposés différemment d'un individu à un autre. Chaque œil est unique. Il est prouvé que la probabilité de trouver deux iris identiques est inférieure à l'inverse du nombre d'humains ayant vécu sur terre.

Une fois que l'image de la configuration des vaisseaux sanguins est obtenue par le système biométrique, le fonctionnement est quasi identique à celui du système analysant l'empreinte digitale. La grosseur des vaisseaux, leur positionnement et les bifurcations qui les caractérisent font partie des éléments, les minuties, qui seront étudiés par le système dans le but d'en dégager un algorithme particulier. La comparaison avec le fichier référence pourra s'ensuivre.

Le point faible de ce type de système utilisant l'œil à des fins d'identification ou de vérification est qu'il éprouve beaucoup de difficultés à lire l'image de l'œil d'une personne aveugle ou d'un individu ayant un problème de cataracte.

Figure I.6: la reconnaissance de l'iris

I. 4.2.5 La reconnaissance de visage :

Le développement de systèmes biométriques basés sur la reconnaissance de la forme du visage est des plus récents. En 1982, deux chercheurs Hay et Young affirment que l'humain, pour reconnaître un visage, utilise les caractéristiques globales et locales qui le composent.

Des recherches plus avancées furent effectuées afin de voir si cette capacité de reconnaissance pouvait être reproduite informatiquement.

C'est à partir des travaux du professeur Teuvo Kohonen (1989), chercheur en réseaux neuronaux de l'Université d'Helsinki, et des travaux de Kirby et Sirovich (1989) de l'Université Brown du Rhode Island, que fut mis au point par le MIT un système de reconnaissance du visage nommé : EIGENFACE.

L'image du visage est captée par une caméra. Le sujet peut se présenter volontairement devant celle-ci ou encore, son image peut être capturée à son insu pour en dégager certaines particularités.

Selon le système utilisé, l'individu doit être positionné devant l'appareil ou peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier référence.

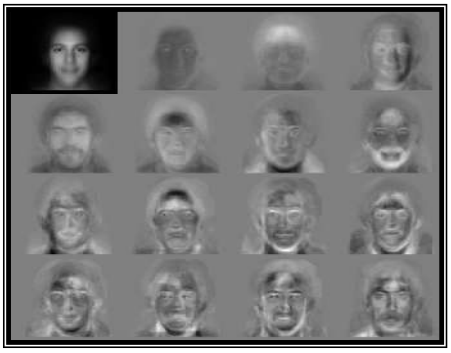


Figure I.7 : la reconnaissance de visage

I. 4.2.6 La reconnaissance vocale :

C'est en 1962 que Lawrence Kersta, un ingénieur du bel Laboratories, établit que la voix de chaque personne est unique et qu'il est possible de la représenter graphiquement. La voix est constituée de composantes physiologiques et comportementales.

Dans les années 80, plusieurs entreprises développèrent des systèmes de reconnaissance de la voix pour les corps policiers et les agences d'espionnage. Au début des années 90, le gouvernement américain demanda à ces entreprises de mettre au point un système pour le marché commercial. **[WEB 15]**

Initialement, une table de référence de la voix d'une personne doit être construite. Pour ce faire, celle-ci doit lire une série de phrases ou de mots à plusieurs reprises. Plusieurs caractéristiques de la voix sont alors extraites comme le débit, la force, la dynamique et la forme des ondes produites.

Un individu ne parle pas toujours de la même manière, ce qui nécessite l'application d'une méthode permettant d'éliminer certaines de ces variations. Ses caractéristiques formant une empreinte unique sont ensuite traitées par un algorithme et conservées pour une comparaison ultérieure. Il existe cinq principales méthodes de traitement de la voix : dépendante du sujet, indépendante du sujet, discours discontinu, discours continu et discours naturel.

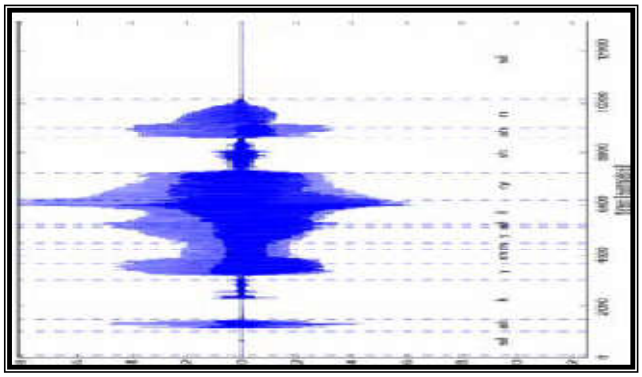


Figure I.8: la reconnaissance de la parole

I. 4.2.7 La reconnaissance de la dynamique de la frappe au clavier :

Le système est basé sur la dynamique de frappe au clavier, il ne nécessite aucun équipement particulier, chaque ordinateur disposant d'un clavier.

Il s'agit d'un dispositif logiciel qui calcule le temps ou un doigt effectue une pression sur une touche et le temps où un doigt est dans les airs (entre les frappes).

Cette mesure est capturée environ 1000 fois par seconde. La séquence de frappe est prédéterminée sous la forme d'un mot de passe. Initialement l'utilisateur doit composer son mot de passe à quelques reprises afin que soit constitué un gabarit de référence.

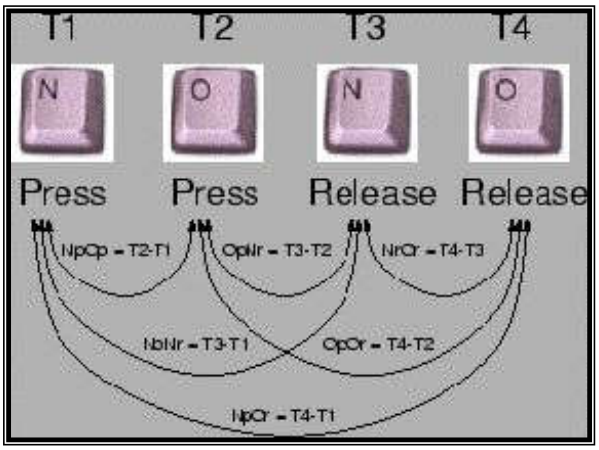


Figure I.9 : la reconnaissance de la frappe au clavier

Remarque :

Aux Etats-Unis, 82% des personnes interrogées ont fait l'expérience de la reconnaissance des empreintes digitales, contre 46% pour la signature dynamique, 27% pour la voix, 22% pour le visage, 20% pour les yeux, 19% pour la géométrie de la main et 7% pour la dynamique de la frappe au clavier.

I. 4.2.8 La reconnaissance de l'oreille :

A priori, la technique serait efficace, car il n'existe pas deux formes d'oreilles identiques. Mais il n'existe encore aucune application commerciale.

*Figure I.10. La reconnaissance de l'**oreille***

I. 4.2.9 La reconnaissance des ongles :

La technique est basée sur les stries longitudinales des ongles, qui dépendent de la structure de l'épiderme sous-jacent. On peut révéler le relief de l'ongle grâce à un interféromètre, et le cartographier.

I. 4.2.10 La reconnaissance du réseau veineux :

Prometteuse, cette dernière technique sonde par infrarouge le dessin du réseau de veines soit du doigt soit de la main. C'est un procédé déjà très répandu au Japon. Il est notamment développé par Hitachi pour les établissements bancaires.

Le motif des veines du doigt ou de la paume de la main sert de critère d'authentification des personnes.

La biométrie par la reconnaissance des veines fonctionne assez simplement. Des diodes émettent une lumière proche de l'infrarouge (IR) qui pénètre dans le revers de la main ou les doigts (ce sont les deux endroits les plus couramment utilisés pour la reconnaissance par les veines). Cette lumière est absorbée par les tissus de la peau et les vaisseaux sanguins: certains tissus vont en absorber plus que d'autres et certains tissus vont refléter la lumière IR plus que d'autres. Pour la reconnaissance par les veines du revers de la main, c'est la lumière réfléchie qui est captée par les capteurs tandis que pour les doigts, c'est la lumière absorbée qui l'est (les tissus qui absorbent cette lumière apparaîtront comme noirs). L'image résultante est

numérisée et traitée pour en extraire le motif des veines, mais aussi leurs épaisseurs, leurs branchements, leurs interconnexions et autres caractéristiques pertinentes.

Ce type de moyen biométrique est bien entendu utilisé pour gérer des accès dans des lieux protégés et pour remplacer les mots de passe permettant de se connecter à un réseau ou d'autoriser une imprimante à sortir les documents uniquement en présence de celui qui en a lancé l'impression. Ce sont là des applications basiques. Mais les fabricants ne s'arrêtent pas ici: des lecteurs d'image vasculaire, ils en mettent aussi sur les distributeurs automatiques de boissons ou les casiers pour les personnels d'entreprise et les consignes publiques.

Figure I.11: La reconnaissance du réseau veineux

I.4.2.11 Rythme cardiaque

Comme les empreintes digitales, le rythme cardiaque est propre à chaque personne et doit donc permettre de l'identifier. En effet, des chercheurs ont découvert que le rythme cardiaque, et plus précisément la forme des pics d'un électrocardiogramme, sont propres à chaque individu. Une chercheuse a mis au point un capteur cardiaque, HeartID, identifiant en 1,2 seconde et qui peut être intégré dans tout type d'appareil électronique pour servir de système d'authentification biométrique. On pourrait le voir arriver sur les Smartphones, tablettes et consoles de jeu dans un avenir proche.

Différents laboratoires de recherche situés en Europe et en Amérique du Nord travaillant sur ce sujet confirment que ce profil cardiaque ne varie pas avec l'âge ni même si le rythme du cœur s'emballe suite à un effort ou une émotion. Par ailleurs, les progrès techniques récents sur les électrocardiogrammes ont permis de mettre au point des capteurs miniaturisés et bon marché qui fonctionnent à partir du bout des doigts. L'idée d'utiliser le rythme cardiaque comme outil biométrique a donc rapidement fait son chemin.

Figure I.12: *Aperçu de l'interface du système d'identification HeartID. Lorsque l'utilisateur place ses doigts sur les capteurs de rythme cardiaque, un algorithme de reconnaissance traite le signal et le compare avec l'électrocardiogramme de la personne préalablement enregistré.* [Adj11].

I.4.3. Analyse comportementale:

I.4.3.1 La reconnaissance de la signature:

Des 1929, Osborn établit que l'écriture dépend de plusieurs facteurs caractéristiques. Pour imiter une signature, il faut donc non seulement limiter la forme de l'écriture mais aussi tenir compte de ces facteurs liés notamment à la vitesse, aux conditions environnantes et à la dextérité musculaire.

Par la suite, diverses techniques de reconnaissance de la signature furent mises au moins au bénéfice notamment des banques et des corps policiers.

Les systèmes de reconnaissance de l'écriture, analysent les caractéristiques spécifiques d'une signature comme la vitesse, la pression sur le crayon, le mouvement, les points et les intervalles de temps où le crayon est levé.

L'utilisateur de cette technologie signe généralement avec un stylo électronique sur une tablette graphique. Ces données sont enregistrées pour comparaison ultérieure. Certains systèmes ne font qu'enregistrer l'image statique de la signature pour comparaison.

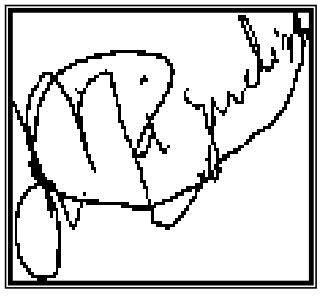


Figure I.13 : une signature scannée

I.4.3.2 La reconnaissance de la démarche :

Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvements du corps…), en analysant des séquences d'images. La démarche serait en effet étroitement associée à la musculature naturelle et donc très personnelle. Mais des vêtements amples, par exemple, peuvent compromettre une bonne identification.

I-5. Architecture d'un système biométrique :

Le système biométrique repose sur deux processus : celui dit d'enrôlement biométrique et celui de recherche et de vérification (contrôle).

L'enrôlement : cette étape sert à créer la base de données de référence. Ses étapes sont multiples et ordonnées : capture de l'échantillon biométrique, extraction des données décrivant les caractéristiques de cet échantillon, création d'un gabarit reproduisant l'ensemble des données de l'échantillon original, mise en mémoire de celui-ci sur une base de données centralisée ou dans un dispositif tel que disque dur, carte à puce, code barre.

Le processus de vérification (contrôle) : cette étape permet de comparer une donnée d'utilisateur à une donnée de référence. Il se décompose de la façon suivante : utilisation du dispositif biométrique pour la capture d'un échantillon, extraction des données numériques, création d'un candidat gabarit reproduisant l'ensemble des données caractéristiques de l'échantillon original qui servira à effectuer la recherche et la vérification, placement du candidat gabarit dans le moteur de vérification biométrique pour qu'il puisse être comparé avec le gabarit biométrique original.

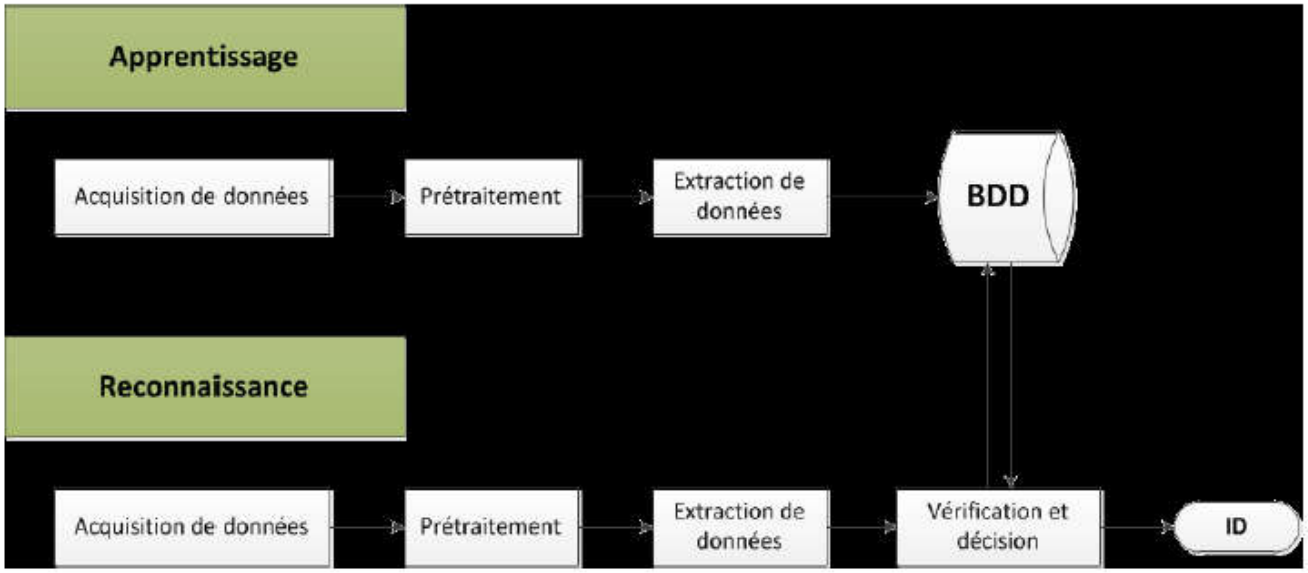


Figure I.14: Architecture d'un système biométrique [Akr11].

I. 6. Les performances des systèmes biométriques :

Les performances d'un système biométrique sont données par la mesure de deux taux d'erreurs : le **FRR** (False Rejet Rate ou Taux de Faux Rejet) et le **FAR** (False Acceptation Rate ou Taux de Fausse Acceptation). **Le FRR ou le TFR** (Taux de Faux Rejets) : estime le pourcentage d'utilisateurs valides qui ne seront pas reconnus par le système. **Le FAR ou le TFA** (taux de fausse acceptation) : estime le pourcentage d'utilisateurs non connus qui seront faussement reconnus par le système.

Le paramétrage d'un système consiste à trouver le bon équilibre entre ces deux taux, le FAR augmentant lorsque le FRR diminue, et inversement. Un contrôle d'accès très sécurisé aura un FAR très bas, pour garantir qu'aucune personne non autorisée n'accède au site, mais, en contrepartie le FRR sera élevé, ce qui signifie que des utilisateurs valides se verront refuser l'accès. Les

autres mesures de performance sont les temps d'encodage de l'empreinte et de mise en correspondance. Là encore, ces valeurs peuvent varier considérablement d'une application à une autre. Un troisième paramètre FER ***(False Equal Rate)*** mesure le taux d'échec à l'enrôlement. Il traduit la probabilité d'absence d'une caractéristique biométrique pour un individu dans une population, donne un point sur lequel le T.F.A. est égal au T.F.R.
La figure I.5 illustre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs

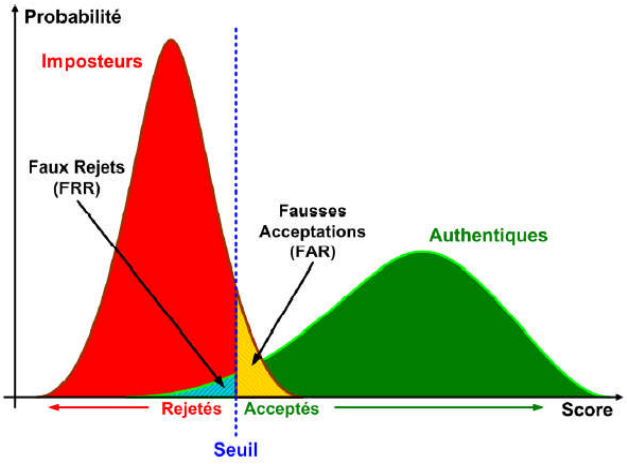


Figure I.15 : Illustration du FRR et du FAR. [Akr11].

I.7 Les applications de la biométrie :

Aujourd'hui, les principales applications sont la production de titres d'identité, le contrôle d'accès à des sites sécurisés, le contrôle des frontières, l'accès aux réseaux, systèmes d'information et stations de travail, le paiement électronique, la signature électronique et même le chiffrement de données. Cette liste n'est pas exhaustive, et de nouvelles applications vont très certainement voir rapidement le jour.
Les techniques biométriques sont appliquées dans plusieurs domaines et leur champ d'application couvre potentiellement tous les domaines de la sécurité où il est nécessaire de connaître l'identité des personnes. Les applications peuvent être divisées en trois groupes principaux :

- **Application commerciales :** telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, l'accès d'internet, l'ATM, la carte de crédit, le contrôle d'accès physique, le téléphone portable, le PDA, la gestion des registres médicales, l'étude de distances, etc.…
- **Applications de gouvernement :** telles que la carte nationale d'identifications, le permis de conduite, la sécurité sociale, le contrôle de passeport, etc.…
- **Applications juridiques :** telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc.

Figure I.16. : Applications biométriques.

Les applications de la biométrie :

Contrôle d'accès aux locaux:

- Salles informatiques.
- Sites sensibles (service de recherche, site nucléaire).

Equipements de communication:

- Terminaux d'accès.
- Téléphones portables.

Systèmes d'informations:

- Lancement du système d'exploitation,
- Accès au réseau.
- Transaction (financière pour les banques, données entre entreprises).

Machines & Equipements divers:

- Distributeur automatique de billets.
- Lieu sensible (club de tir, police).
- Contrôle des adhérents dans les clubs privés.
- Contrôle des temps de présence.

Etat/Administration:

- Fichier judiciaire.
- Services sociaux (sécurisation des règlements).
- Système de vote électronique.

I. 8. Les avantages et les limites de la biométrie:

I.8.1 Les avantages de la biométrie :

La biométrie est une technologie récente et commence à être adoptée par de grands constructeurs de matériel informatique. L'usage de la biométrie est un complément de l'utilisation des méthodes d'authentification comme des mots de passe, des badges, des cartes à puce.

- **Suppression des mots de passe, Suppressions des clés :**

Au lieu de retaper son mot de passe dès que le PC se met en veille, une simple pression de l'empreinte digitale sur le capteur suffit et permet facilement de changer la session d'utilisateur.

- **Utilisation d'une signature biométrique:**

Grande sécurité, intransmissible à une autre personne.
Une identité vérifiée (Le destinataire est bien la personne autorisée à visualiser ou à utiliser les données).
Lors de transactions financières, il est capital de savoir quel moyen de paiement du consommateur est le plus sûr.
La biométrie offre le chaînon manquant dans la triade du problème de sécurité:

- Diminution de la fraude.
- Rehaussement de l'intégrité des informations et la sécurité.
- Réduction des attaques à l'égard des programmes gouvernementaux.
- Croissance de la confiance envers les systèmes de sécurité.

- Diminution des frais administratifs.
- Accélération des services.

I.8.2 Les limites de la biométrie: La biométrie présente malheureusement un certain nombre d'inconvénients parmi eux : le problème de la qualité de l'authentification. Ces méthodes ne sont en effet pas toujours fiables à 100%, ce qui empêche des utilisateurs de bonne foi d'accéder à leur système. Car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant : on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, bref on évolue et les mesures changent. [Adj06]:

Prenons le cas le plus simple, celui des empreintes digitales (mais la même chose s'applique à toute donnée physique). Suivant les cas, nous présentons plus ou moins de transpiration, la température des doigts n'est pas régulière. Il suffit de se couper pour présenter une anomalie dans le dessin de ses empreintes. Dans la majorité des cas, les mesures du capteur et du logiciel associé retourneront un résultat différent de la mesure initiale de référence. Or, il faut pourtant bien réussir à se faire reconnaître. En pratique, cela sera réalisé dans la plupart des cas car le système est amené à autoriser une marge d'erreur entre la mesure et la référence.

De manière générale, les faiblesses de ces systèmes ne se situent pas au niveau de la particularité physique sur laquelle ils reposent, mais bien sur la façon avec laquelle ils la mesurent, et la marge d'erreur qu'ils autorisent. Là encore, il convient de ne pas se laisser impressionner par une image illusoire de haute technologie - produit miracle.

De plus, les experts techniques mettent au passif de cette technologie, d'une part, son coût, d'autre part, la question de sa révocation. En effet, confronté à une personne qui a subtilisé un mot de passe ou une signature manuscrite, le titulaire du mot de passe ou de la signature peut facilement les remplacer ou les révoquer. La chose semble plus complexe pour une empreinte digitale ou rétinienne. Si un tiers s'approprie une identité biométrique du type empreintes digitales ou identité visuelle, il peut au moyen de ces identités biométriques passer tout type d'actes au nom de la victime. Comment la victime pourrait-elle alors révoquer sa propre empreinte digitale ou identité visuelle ? Les experts en sécurité sont partagés sur la question, même si, en majorité, ils semblent considérer que cette révocation est possible. Tous reconnaissent cependant la difficulté à mettre au passif cette protection technique.

Les données biométriques sont comparables à tout autre système de contrôle d'accès comme des mots de passe, …etc. Car du point de vue du système informatique, ce ne sont rien d'autres que des séries de bits comme toute donnée. Autrement dit, la difficulté réside dans la contrefaçon de la caractéristique physique et biologique que l'on mesure.
Si la biométrie se généralise dans notre environnement, il est dangereux de penser qu'il s'agit de la réponse à tous les problèmes de sécurité. La biométrie, de par ses limites fonctionnelles, techniques et juridiques n'est en aucun cas synonyme de technologie miracle et de sécurité absolue.

- **Les limites fonctionnelles:**

Les systèmes d'authentification biométrique représentent une grande partie des limites fonctionnelles. En effet, les systèmes biométriques laissent la place à un certain nombre de faux rejets et de fausses acceptations. Ils ne peuvent à eux seuls garantir à 100% que seules les personnes autorisées pourront passer le contrôle. Ils ne peuvent même pas garantir qu'une personne autorisée ne sera pas rejetée par le système. Il y aura toujours une marge d'erreur à prendre en compte, ce qui n'est pas forcément très rassurant.

- **Les limites techniques :**

Bien que cela représente un travail assez conséquent, les données biométriques peuvent être imitées, notamment celles qui laissent des traces sur le passage de l'individu telles que les empreintes digitales. Un individu mal intentionné peut récupérer les empreintes digitales sur un objet tenu par la victime, les imiter et tenter de passer le contrôle biométrique à l'aide de ces empreintes. De plus, les données biométriques sont dans la majeure partie des cas numérisées sur un support, de préférence individuel. Si ce support n'est pas protégé contre les intrusions et le piratage, tout le système biométrique tombe à l'eau.

I.8.3 Tableaux de comparaison:

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Tableau I.1: Comparaison entre les techniques biométriques

Remarque :

L'étude d'un produit biométrique se base principalement sur quatre points : la technologie et le coût associé, la simplicité d'usage, l'efficacité quantitative et juridique.

Plutôt que de comparer uniquement les performances de ces systèmes, il est nécessaire de tenir compte de l'environnement, de l'usage, de la facilité aussi bien de saisie que d'analyse, de stockage ou de vérification. En effet, chaque technologie possède des avantages et des inconvénients, acceptables ou inacceptables suivant les applications. Toutes les solutions ne sont donc pas concurrentes, elles n'offrent ni les mêmes niveaux de sécurité ni les mêmes facilités d'emploi.

Nous dressons dans le tableau suivant les avantages et inconvénients des différentes technologies biométriques :

Modalité	**Avantages**	**Inconvénients**
L'iris	-L'iris n'est pas modifiable même par intervention chirurgicale. -Les iris sont uniques et différant même pour les vrai jumeaux. -Grande quantité d'information contenue dans l'iris - Iris très difficilement falsifiable. - Dessin de l'iris indépendant du code génétique. - L'iris ne varie presque pas au cours d'une vie.	-L'iris est aisément visible et peut être photographié. Le problème de sécurité est alors lié aux vérifications effectuées lors de la prise de vue. (Problème identique pour les empreintes, la voix, l'oreille,... Mais moins pour la rétine). -Aspect psychologiquement invasif de la méthode - Des problèmes peuvent survenir lors de la mesure (reflet, variation de la taille de la pupille, etc.). Une photo ou une lentille de contact reproduisant l'image de l'iris peut affecter la fiabilité.
La rétine	-L'empreinte rétinienne est peu exposée aux blessures (coupure, brûlure), -Les taux de faux rejet et de fausse acceptation sont faibles, -Très difficile, voie impossible, à imiter, -La rétine est différente chez les vrais jumeaux, -La rétine est stable durant la vie d'un individu - très efficace. Carte vasculaire propre à chaque individu et différente, même entre jumeaux. - Haute sécurité.	-Système intrusif, il faut placer l'œil près du capteur, -Mauvaise acceptation du public (l'œil est un organe sensible), -Coût plus important que d'autres technologies, -Pas adapté pour un flux de passage important -Technique contraignante pour les participants (mesure à courte distance [quelques centimètres] du capteur). -Technique invasive et peu acceptée par le public. -L'aspect des vaisseaux sanguins peut être modifié par la maladie ou l'âge
Le visage	- Le facial-scan fait par caméra photo est réputé pour être la technique la plus simple et la moins contraignante. Son principal avantage est son côté peu intrusif. -Comparable à se faire prendre en photo, il est relativement mieux accepté socialement - Seule une opération chirurgicale modifiant la forme du visage (ajout de prothèses, transformation du cartilage, etc.) peut affecter la fiabilité. Seule technique utilisable sans le consentement de la personne. - utilisation facile.	-La reconnaissance des visages ne fonctionne pas bien incluent l'éclairage pauvre, les lunettes de soleil, les longs cheveux, ou d'autres objets couvrant partiellement le visage du sujet, et des images à basse résolution. -la distance pour la capture de l'image du visage n'est pas inconfortable. -Un autre inconvénient sérieux est que beaucoup de systèmes sont moins efficaces si les expressions du visage varient. Même un grand sourire peut rendre le système moins efficace. Par exemple : Le Canada permet maintenant seulement des expressions du visage neutres en photos de passeport - Technique qui ne permet pas d'identifier des personnes en mouvement.

		-Impossibilité de différencier des jumeaux. - Peu d'efficacité. - Sensibilité à la variation de l'éclairage et au changement de la position du visage.
Les empreintes digitales	-La technologie la plus éprouvée techniquement et la plus connue du grand public. -Petite taille du lecteur facilitant son intégration dans la majorité des applications (téléphones portables, PC). -Faible coût des lecteurs grâce aux nouveaux capteurs de type "Chip silicium". -Traitement rapide -Bon compromis entre le taux de faux rejet et le taux de fausse acceptation.	-Image "policière" des empreintes digitales. Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur). -Certains systèmes peuvent accepter un moulage de doigt ou un doigt coupé (la détection du doigt vivant permet d'éviter ce type d'usurpation). -Difficulté de lecture : sensibilité aux altérations pouvant survenir au cours de la vie (égratignure, cicatrice, vieillissement ou autres) et à certaines variations (température, humidité, saleté)
Forme de la main	-Bonne acceptation des usagés, -Très simple à utiliser, -Le résultat est indépendant de l'humidité et de l'état de propreté des doigts, -Fichier "gabarit" de petite taille. -Technique moins coûteuse que la reconnaissance des empreintes digitales : insensibilité à la poussière, aux coupures au doigt, etc. -D'utilisation très simple	-Trop encombrant pour un usage sur le bureau, dans une voiture ou un téléphone, -Risque de fausse acceptation pour des jumeaux ou des membres d'une même famille - La forme de la main ou des doigts se modifie avec le vieillissement, ce qui nuit à la mesure à long terme.
La voix	-Technologie biométrique facile à mettre en œuvre. -Permet de sécuriser une conversation téléphonique. -Généralement très bien acceptée car la voix est un signal naturel a produire [F.Per, J.Dug02]. - Une des seules techniques permettant de reconnaître quelqu'un à distance et la seule - utilisée pour la reconnaissance par téléphone.	-La voix n'est pas un attribut permanent (elle change bien entendu avec l'âge). -Technologie biométrique vulnérable aux attaques [F.Per, J.Dug, 02]. - Il est très facile d'enregistrer ou de reproduire la voix. - Nécessite une excellente qualité audio. -Sensible aux bruits ambiants. -La voix change dans le temps et peut être altérée (rhume, fatigue, forte émotion, etc.). -Faible niveau de différenciation entre deux voix. - Taux élevés de faux rejets et de fausses acceptations
Frappe du clavier	-Non intrusif, geste naturel pour un individu, -Pas de matériel supplémentaire, un simple logiciel suffit, -Mise en œuvre rapide pour un grand nombre d'utilisateur, -Réduit sensiblement la nécessité de changement de mot de passe et la sollicitation des services informatique **[Oud09],** - Permet d'identifier une personne à distance, à partir de son ordinateur.	-L'utilisation d'un clavier d'un format différent AZERTY, QWERTY …, provoque un refus de son propre mot de passe [Oud 09]. -L'état de santé et la fatigue peuvent altérer la façon de frapper les touches. - Sensibilité à la différence entre les claviers.
signature	-La signature écrite sur un document peut être conservée des certains documents, -Action qui implique (responsabilité) le	-Besoin d'une tablette graphique, -Sensible aux émotions de l'individu, -Pas utilisable pour du contrôle d'accès en

	demandeur - Facile à utiliser. Très acceptée par les usagers	extérieur par exemple - Technique peu utilisée jusqu'à maintenant. La signature étant changeante, une combinaison de données (vitesse d'exécution ou autres) est nécessaire
ADN	-Une Très grande précision. -Il impossible que le système a fait des erreurs. -Il est standardisé	-Très cher
Réseau veineux	-Très haut niveau de sécurité, à ce jour aucun moyen de frauder. -biométrie dite "sans trace". -La biométrie de mesures des veines respecte les libertés individuelles C.F. CNIL AU N°009. -TFA - taux de fausses acceptations (personnes authentifiées comme quelqu'un d'autre) est inférieure à 0,0001%. -Biométrie sans badges et sans code.	-Utilisation uniquement en intérieur, -Capteur sensible à la lumière, toutefois les constructeurs ont apporté des protections limitant le problème. -La CNIL n'autorise pas dans l'AUN°019 la mise sous réseau des lecteurs pour le transfert des données biométriques, -La bonne identification de l'utilisateur implique de poser correctement le doigt sur le capteur. L'utilisateur doit être volontaire pour appliquer son doigt correctement.

Tableau I.2 : Avantages et inconvénients des différentes technologies biométriques.

Ces deux comparaisons nous permettent de choisir une technologie appropriée en fonction des contraintes liées à l'application demandée. Par exemple, on remarque que l'iris et l'empreinte digitale sont les modalités les plus discriminantes. Cela est utile pour les systèmes d'identification à grande-échelle nécessitant un haut niveau de sécurité.

Une brève comparaison des techniques biométriques les plus utilisées ci-dessus basées sur sept facteurs est fournie dans le tableau. L'applicabilité d'une technique biométrique spécifique dépend fortement des conditions du domaine d'application. Par exemple, il est bien connu que la technique basée sur l'empreinte digitale est plus précise que la technique basée sur la voix. Cependant, dans une application de transaction bancaire à distance, la technique basée sur la voix peut être préférée puisqu'elle peut être intégrée dans le système de téléphone existant.

Avantages et Inconvénients des Techniques biométriques : voir tableau I.2

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)[1] a procédé à une comparaison des différentes technologies biométriques appelée Analyse Zéphyr. Les résultats de cette comparaison sont illustrés sur la figure I.8. Cette comparaison est basée sur quatre (04) critères principaux [Hoc 07] :

- **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).

[1]Site officielle d'IBG, URL : http://www.ibgweb.com/
[1]Site officielle du CLUSIF, URL : http://www.ibgweb.com/

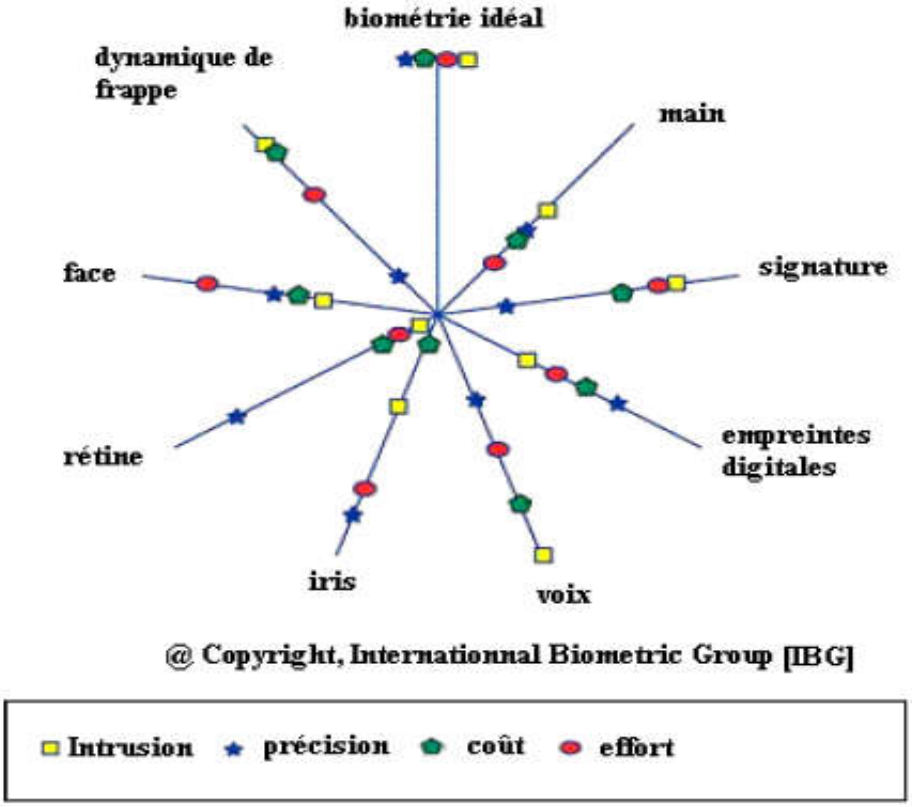


Figure I.17. Analyse Zephyr : comparaison de différentes modalités selon quatre critères principaux: l'intrusivité, le pouvoir discriminant, le coût et l'effort.

I-9 Le marché de la biométrie :

I.9.1-Présentation du marché :

La biométrie connaît un engouement sans précédent. La croissance mondiale de la biométrie depuis quelques années est incontestable, tant le nombre d'intervenants est grand, même s'il existe peu d'informations publiques concernant ce marché. On peut toutefois considérer certaines données et certains chiffres sur son évolution au fil des années, tant à l'échelle mondiale, qu'américaine ou européenne.

Le marché de la sécurité informatique est encore atomisé, peu de fournisseurs peuvent prétendre offrir une gamme complète de produits. Les spécialistes estiment que ce marché est en pleine croissance et qu'il va également se concentrer. L'Internet et le commerce électronique sont des marchés porteurs pour la sécurité, mais ils ne sont pas les seuls. Le télétravail, la mise à dispositions d'informations aux clients et sous traitants sont également des facteurs de risque pour les entreprises qui ouvrent leur système d'informations.

Le besoin grandissant de sécurité sur les terminaux mobiles a été mis en exergue par une enquête récente, publiée par Toshiba. Celle-ci soutient que 90% des cadres dirigeants et chefs d'entreprise européens stockent des données sensibles, voire confidentielles sur leur outil de communication et parmi eux, 22% admettent avoir pourtant déjà perdu cet outil.

I.9.2-Le marché mondial de la biométrie :

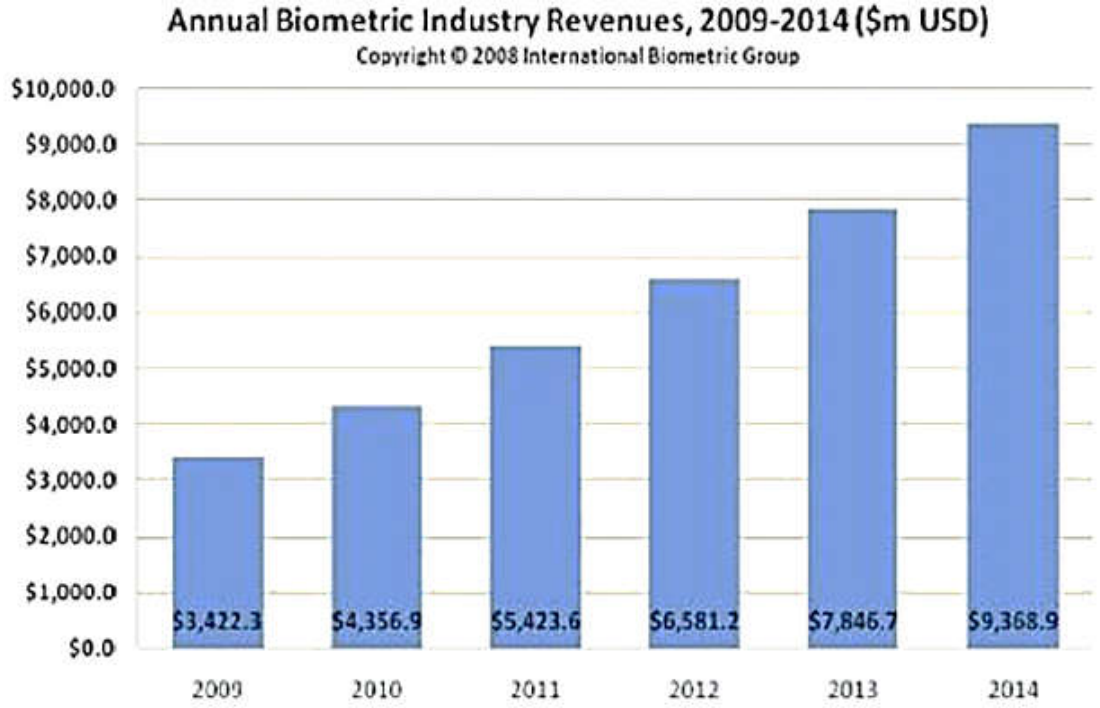


Figure I.18 : La croissance de la biométrie

IBG (International Biometric Group) édite régulièrement un rapport sur le marché de la biométrie. Cette étude est une analyse complète des chiffres d'affaires, des tendances de croissance, et des développements industriels pour le marché de la biométrie actuel et futur. La lecture de ce rapport est essentielle pour des établissements déployant la technologie biométrique, les investisseurs dans les entreprises biométriques, ou les développeurs de solutions biométriques. Independent Biometrics Expertise [Alo12].

On s'attend à ce que le chiffre d'affaires de l'industrie biométrique incluant les applications judiciaires et celles du secteur public, se développe rapidement. Une grande partie de la croissance sera attribuable au contrôle d'accès aux systèmes d'information (ordinateur / réseau) et au commerce électronique, bien que les applications du secteur public continuent à être une partie essentielle de l'industrie.

On prévoit que le chiffre d'affaires des marchés émergents (accès aux systèmes d'information, commerce électronique et téléphonie, accès physique, et surveillance) dépasse le chiffre d'affaires des secteurs plus matures (identification criminelle et identification des citoyens).

- On s'attend à ce que l'empreinte digitale gagne 43,6% du marché de biométrie, suivi de l'identification de visage à 19,0%.
- On projette que les revenus annuels de l'identification de l'iris excèdent $250m d'ici.
- On s'attend à ce que l'Asie et l'Amérique du Nord soient les plus grands marchés globaux pour les produits biométriques et les services.
- Les systèmes Multi biométriques émergeront pour comporter approximativement 5% de tout le marché de la biométrie.
- Les empreintes digitales continuent à être la principale technologie biométrique en termes de part de marché, près de 50% du chiffre d'affaires total (hors applications judiciaires). La reconnaissance du visage, avec 12% du marché (hors applications judiciaires), dépasse la reconnaissance de la main, qui avait avant la deuxième place en termes de source de revenus après les empreintes digitales [Alo12].

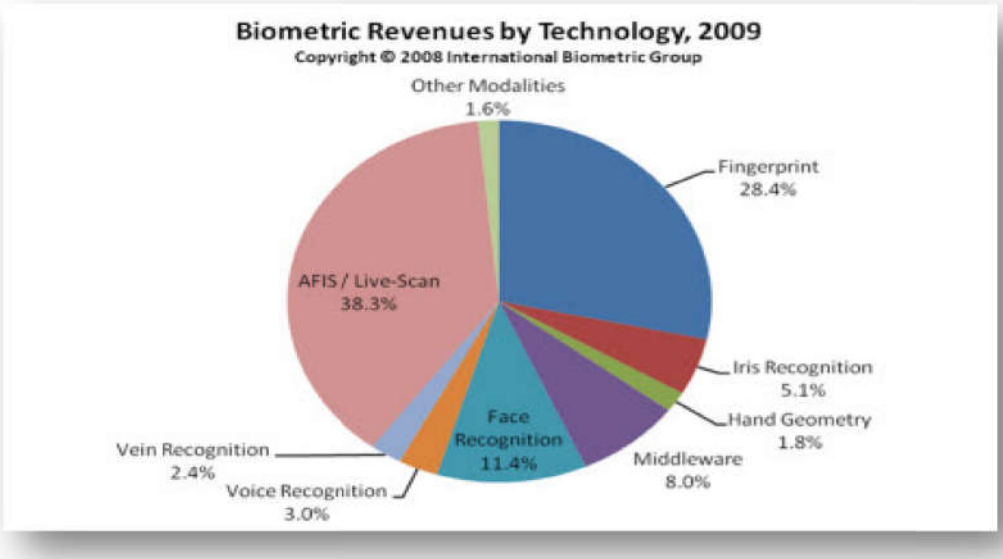


Figure I.19. : Les parts de marché par technologie [Alo12].

I-10. Conclusion :

Dans ce chapitre nous avons décrit les technologies utilisées dans les systèmes biométriques pour l'identification des personnes , leurs architectures et leurs différentes applications, ainsi nous avons donné un aperçu sur les techniques de mesure des performances des systèmes biométriques et montré les différentes modalités biométriques tout en soulignant les avantages et les inconvénients de chacune. Nous avons constaté aussi que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre.

Parmi les modalités utilisées dans la reconnaissance biométrique, nous avons trouvé que la texture de l'iris et les minuties de l'empreinte digitale sont les traits les plus intéressants à cause de leurs précisions et leurs stabilités. De même, l'utilisation de l'iris et de l'empreinte digitale suscite de plus en plus l'intérêt de la communauté scientifique car elle présente plusieurs challenges et verrous technologiques.

CHAPITRE II :

LA MULTIMODALITE

II.1 La multimodalité :

Face aux nombreuses limitations imposées par l'utilisation des systèmes biométriques unimodaux, la biométrie multimodale s'impose de manière indéniable comme une alternative d'avenir dans le domaine de la sécurité des personnes et leurs biens. Bien que le couplage des systèmes biométriques peut être effectué à différents niveaux, la fusion au niveau des scores est la plus courante puisqu'elle a été généralement prouvée plus efficace que le reste des niveaux de fusion. Dans cette thèse, nous nous intéressons tout particulièrement à la fusion au niveau des scores de données biométriques.

La biométrie multimodale, consiste à combiner plusieurs systèmes biométriques. Elle permet de réduire certaines limitations des systèmes biométriques, comme l'impossibilité d'acquérir les données de certaines personnes ou la fraude intentionnelle, tout en améliorant les performances de reconnaissance. Ces avantages apportés par la multi modalité aux systèmes biométriques "monomodaux" sont obtenus en fusionnant plusieurs systèmes biométriques.

Pourquoi la multimodalité ?

Bien que les techniques de reconnaissance biométrique promettent d'être très performantes, on ne peut garantir actuellement un excellent taux de reconnaissance avec des systèmes biométriques unimodaux, basés sur une unique signature biométrique. De plus, ces systèmes sont souvent affectés par les problèmes suivants :

- Bruit introduit par le capteur
- Non-universalité
- Manque d'individualité
- Manque de représentation invariante
- Sensibilité aux attaques

Ainsi, à cause de tous ces problèmes pratiques, les taux d'erreur associés à des systèmes biométriques unimodaux sont relativement élevés, ce qui les rend inacceptables pour un déploiement d'applications critiques de sécurité. Pour pallier à ces inconvénients, une solution est l'utilisation de *plusieurs modalités biométriques* au sein d'un même système, on parle alors de **système biométrique multimodal**.

II.2. Différentes formes de multimodalité:

Les différentes formes de multimodalités sont les suivantes : [D.Dam, J.Ric, 2006] (Voir la figure II.1)

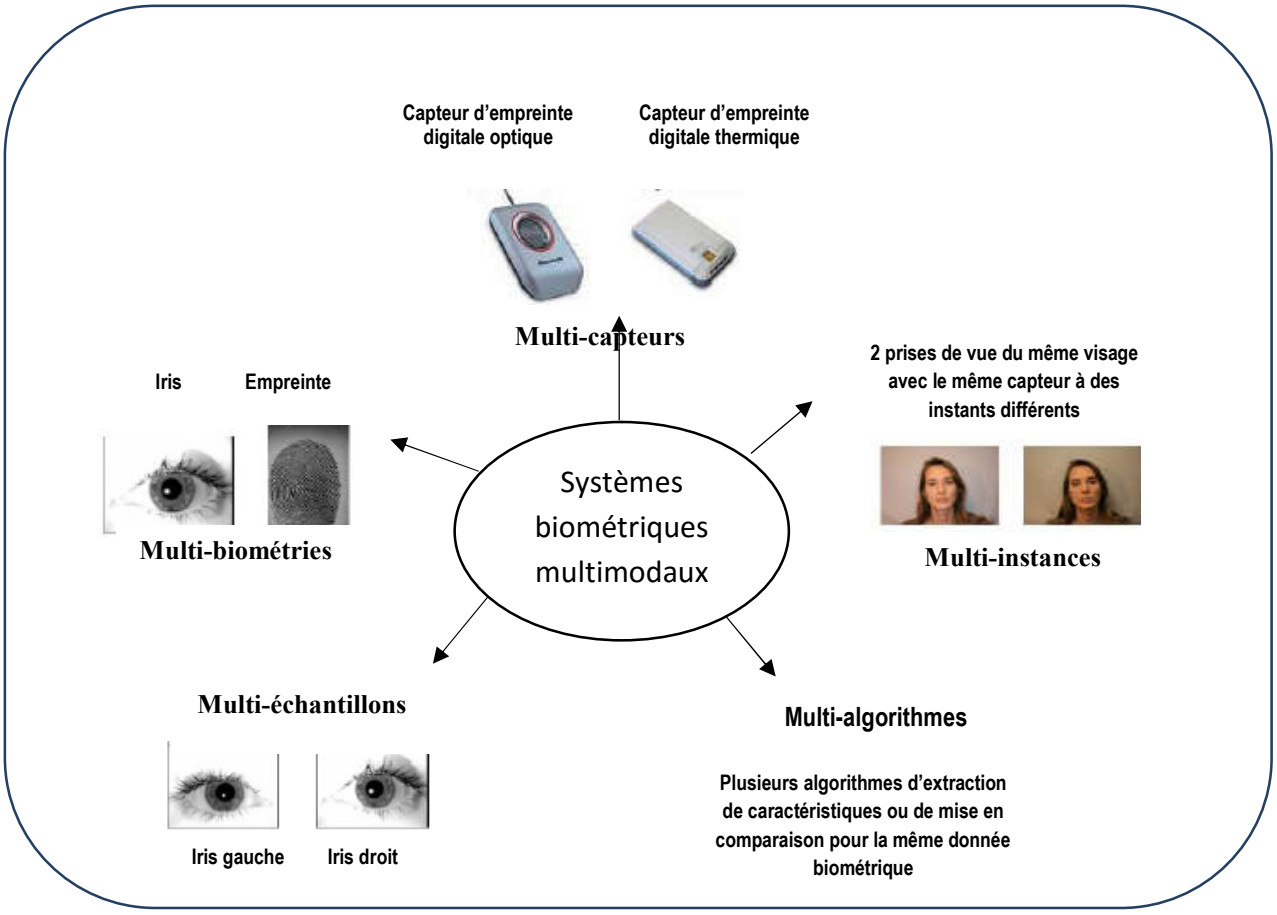


Figure II.8 : les différents systèmes multimodaux.

II.2.1 Systèmes multiples biométriques :

Lorsque l'on considère plusieurs biométries différentes, par exemple visage et empreinte digitale. C'est le sens le plus classique du terme multimodal.

II.2.2. Systèmes multiples d'acquisition

Par exemple utiliser deux scanners différents (l'un optique, l'autre thermique) pour la reconnaissance d'empreintes digitales

II.2.3. Mesures multiples d'une même unité biométrique

Lorsqu'ils associent plusieurs échantillons différents de la même modalité, par exemple deux empreintes digitales de doigts différents ou les deux iris.

II.2.4. Instances multiples d'une même mesure

Faire une capture répétée du même attribut biométrique avec le même système d'acquisition, par exemple l'acquisition de plusieurs images de visage avec des changements de pose, d'expression ou d'illumination.

II.2.5. Algorithmes multiples

Lorsque plusieurs algorithmes traitent la même image acquise, cette multiplicité des algorithmes peut intervenir dans le

module d'extraction en considérant plusieurs ensembles de caractéristiques et/ou dans le module de comparaison en utilisant plusieurs algorithmes de comparaison.

II.3. Les architectures

Il existe deux types d'architectures :

L'architecture en parallèle : correspond à l'acquisition et le traitement des données simultanément des systèmes biométriques associés pour la conception d'un système multimodal.

On parlera de l'architecture en série lorsque l'acquisition et le traitement des données de ces systèmes se font successivement. [D.Dam, J.Ric, 2006]

II.3.1. L'architecture en parallèle

C'est la plus utilisée car elle permet d'utiliser toutes les informations disponibles et donc d'améliorer les performances du système. En revanche, l'acquisition et le traitement d'un grand nombre de données biométriques est coûteux en temps et en matériel, et réduit le confort d'utilisation (voir figure II.2).

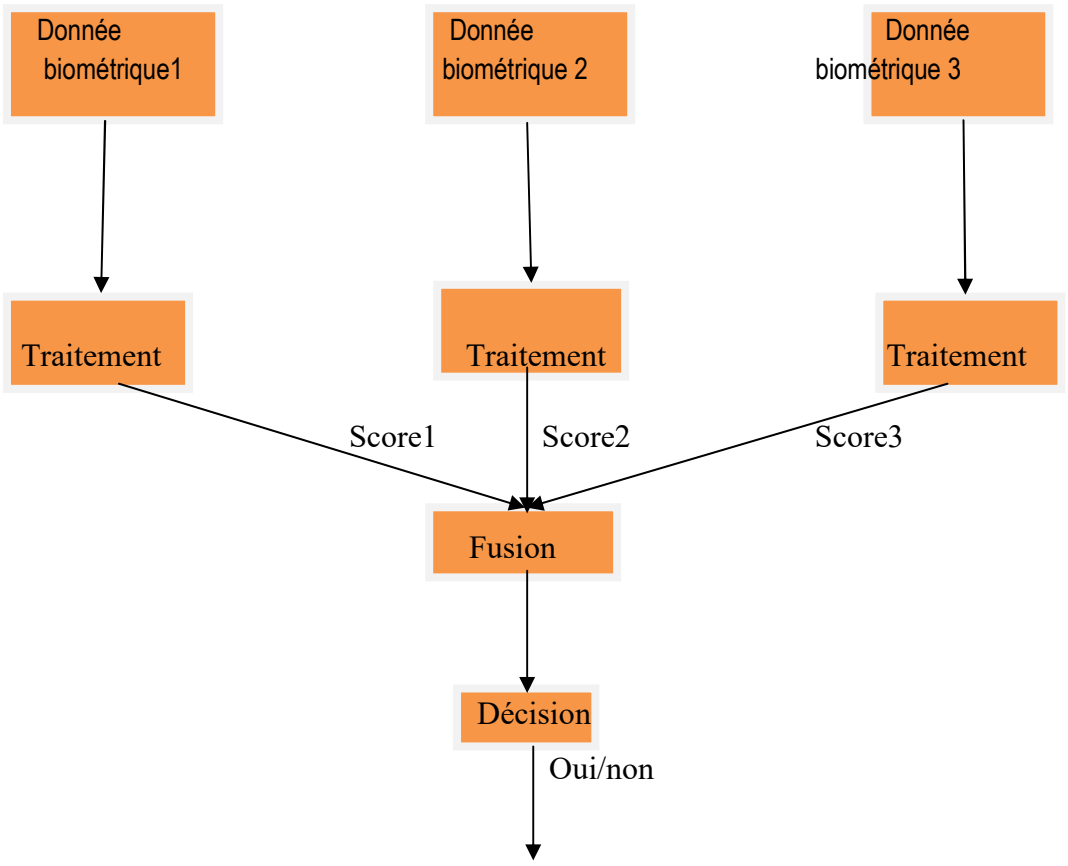


Figure II. 2: Architecture de fusion en parallèle

II.3.2. L'architecture en série

Elle peut être privilégiée dans certaines applications ; par exemple si la multimodalité est utilisée pour donner une alternative pour les personnes ne pouvant pas utiliser l'empreinte digitale. Pour la majorité des individus seule l'empreinte est acquise et traitée mais pour ceux qui ne peuvent pas être ainsi authentifiés on utilise un système à base d'iris alternativement (voir figure II.3)

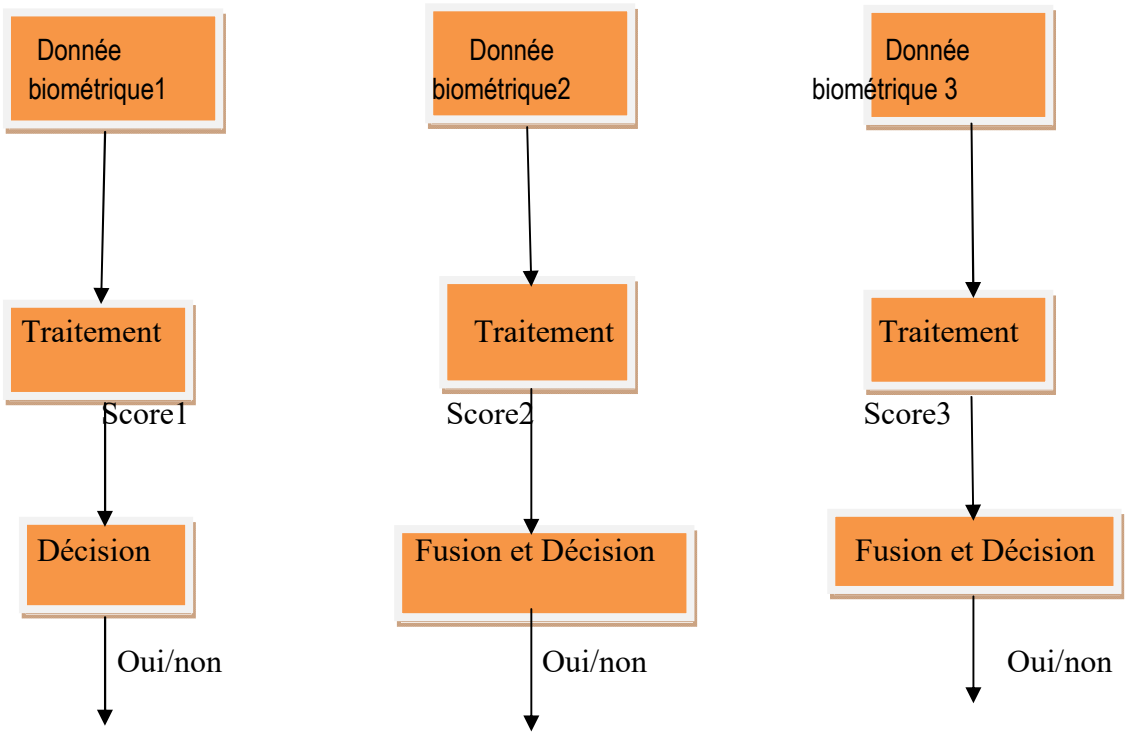


Figure II. 3: Architecture de fusion en série.

II.4. Fusion de données :

La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents : au niveau des données, au niveau des caractéristiques extraites, au niveau des scores issus du module de comparaison ou au niveau des décisions du module de décision [L.Allano, 2009]

Ces quatre niveaux de fusion peuvent être classés en deux sous-ensembles :

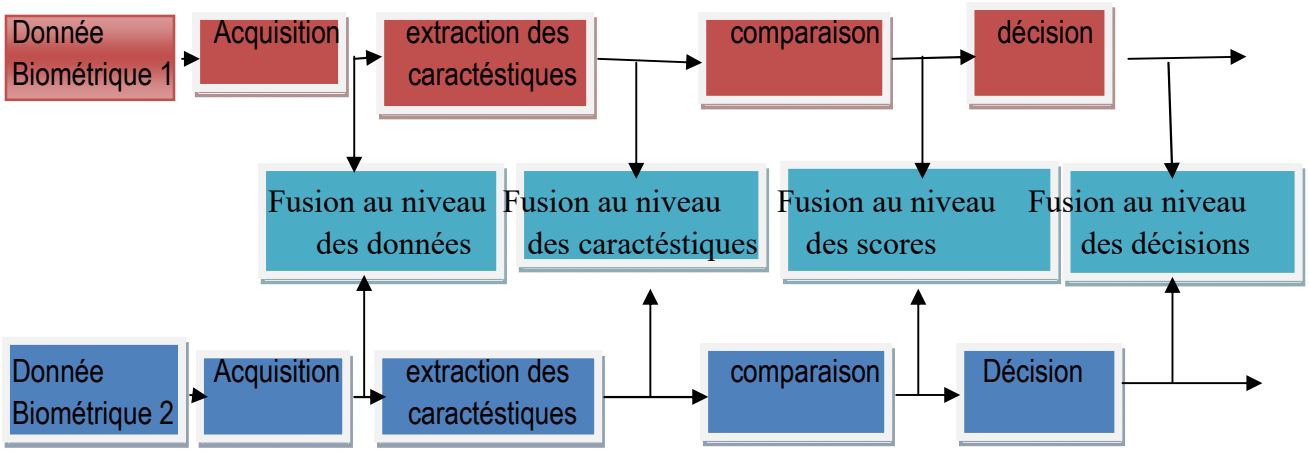


Figure II.4: les différents niveaux de fusion

II.4.1. La fusion pré-classification (avant comparaison)

Ce genre de fusion correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur (images brutes) ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques. La fusion à ces deux niveaux est limitée car elle nécessite une homogénéité entre les données. Par exemple la combinaison de plusieurs images de visages en visible et en infrarouge s'ils correspondent à la même scène (pour le premier niveau), un autre exemple qui ne nécessitent pas vraiment d'homogénéité est la concaténation de plusieurs vecteurs de caractéristiques avant le traitement par l'algorithme de comparaison (pour le deuxième niveau).

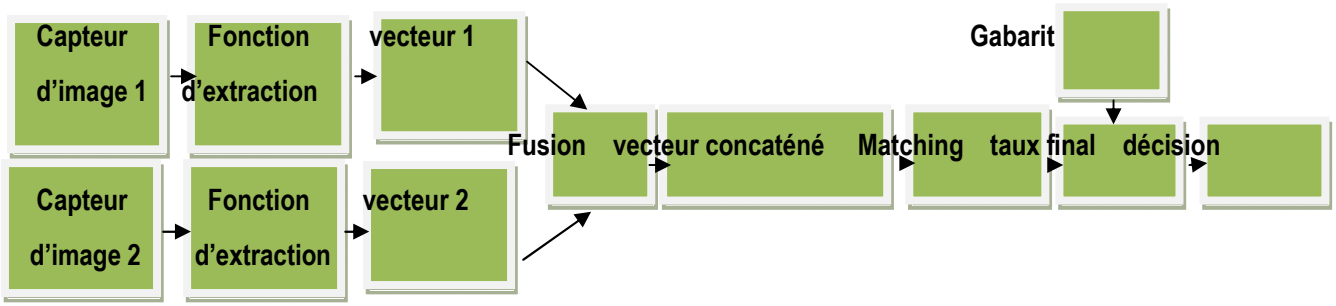


Fig. II.5 .fusion au niveau d'extraction des paramètres [2]

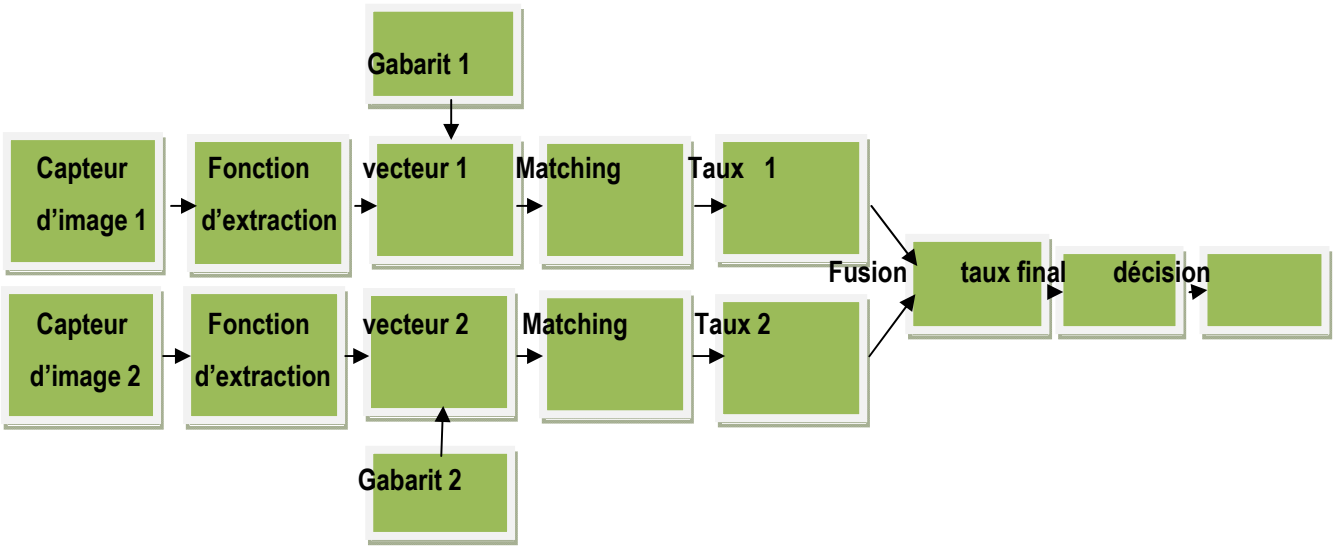


Fig. II.6.fusion au niveau du matching [2]

II.4.2. La fusion post-classification (après la comparaison) :

Elle est très étudiée par les chercheurs. Cette fusion peut se faire au niveau des scores issus des modules de comparaison ou au niveau des décisions. La fusion au niveau des décisions est souvent utilisée pour sa simplicité. En effet, chaque système fournit une décision binaire sous la forme OUI ou NON que l'on peut représenter par 0 et 1, et le système de fusion de décisions consiste à prendre une décision finale en fonction de cette série de 0 et de 1.

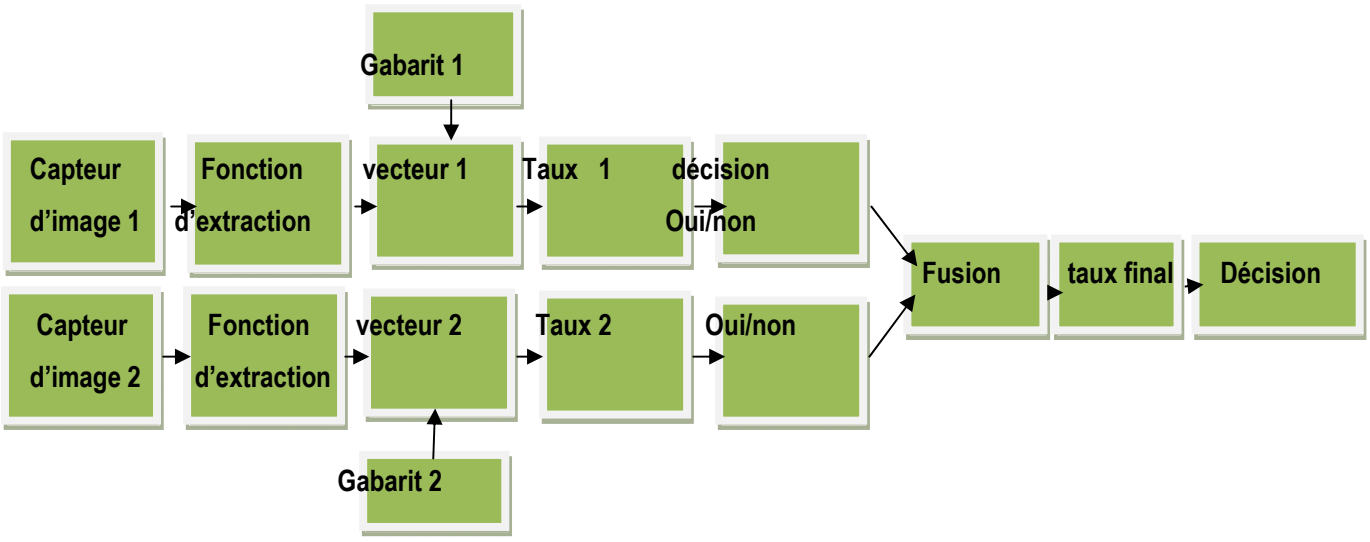


Fig. II.7. Fusion au niveau de la décision [2]

La fusion au niveau des décisions est souvent utilisée pour sa simplicité. En effet, chaque système fournit une décision binaire sous la forme OUI ou NON que l'on peut représenter par 0 et 1, et le système de fusion de décisions consiste à prendre une décision finale en fonction de cette série de 0 et de 1.

Remarque : Dans ce niveau, on traite chaque modalité a part et en prend le résultat majoritaire .C'est l'approche la plus performante car elle demande l'acceptation de l'une deux modalités donc plus de souplesse et moins complexe.

La fusion au niveau des scores est le type de fusion le plus utilisé car elle peut être appliquée à tous les types de systèmes (contrairement à la fusion préclassification), Il existe un grand nombre de méthodes de fusion de scores parmi lesquelles on cite : la moyenne des différents scores [L.Allano, 2009].

II.5. Conclusion

Dans ce second chapitre, nous avons présenté la biométrie multimodale. Après une introduction générale sur la biométrie inscrite au chapitre précédent, nous avons défini la structure des systèmes biométriques et présenté les limitations de ces systèmes lorsqu'ils n'utilisent qu'une seule modalité biométrique. Nous avons ensuite présenté une façon de réduire les limitations des systèmes biométriques monomodaux en combinant plusieurs systèmes conduisant ainsi à la biométrie multimodale. Les systèmes multimodaux peuvent être de différentes natures, nous avons donc présenté dans ce chapitre, les différents types de combinaisons de modalités possibles, mais aussi les architectures et les niveaux de fusion qui peuvent être utilisés dans un système multimodal.

CHAPITRE III :

CHOIX DES MODALITES POUR L'IDENTIFICATION

III. Choix des modalités pour l'identification :

III.1 Identification par l'iris

III.1.1. Introduction :

L'utilisation de l'iris pour l'identification d'une personne a été proposée à l'origine en 1936 par l'ophtalmologue Frank Burch. Dans les années 1980, l'idée réapparut avec les films sur James Bond, mais cela restait toujours de la science-fiction. En 1987 les ophtalmologues Aran Safir et Léonard.Floment font breveter cette idée et en 1989 ; ils ont demandé à John Daugman (Alors enseignant à l'université de Harvard), d'essayer de créer des Algorithmes pour l'identification par l'iris. Ces algorithmes (méthode Basée sur les ondes de Gabor), que Daugman a fait breveter en 1994, sont la base de tous les systèmes d'identification par l'iris.

Le choix de la signature représentée par l'iris est motivé pour les raisons suivantes :

- La reconnaissance de l'iris est caractérisée par un niveau de précision très élevé.
- Cette technique est considérée comme difficile à frauder.
- Le tissu de l'iris de l'œil gauche est différent de celui de l'œil droit pour chaque personne.
- La probabilité d'avoir le même tissu de l'iris est 10^{-72}. Entre les vrais jumeaux, il y a assez de caractéristiques dans l'iris pour que l'on puisse les distinguer.
- La simplicité de la capture d'image de l'iris.
- L'iris ne peut pas être capté à l'insu des personnes.
- L'acceptation par les utilisateurs de toutes les nationalités et des différentes cultures.
- Les résultats obtenus par J. Daugman [Dau 06] ont montré la fiabilité de cette modalité dans un système d'identification.

III.1.2. Description

L'identification par l'iris utilise plus de paramètres que les autres méthodes d'identification et la fiabilité résultante est suffisante pour ne plus faire de l'identification mais de l'authentification.

- La formation de l'iris pour un œil humain commence pendant le troisième mois de gestation.
- Les structures qui créent les éléments distinctifs sont complètes au huitième mois.
- La pigmentation continue dans les premières années après la naissance.

Cette formation est chaotique, elle génère donc des motifs possédant une forte variabilité (244 degrés de liberté).

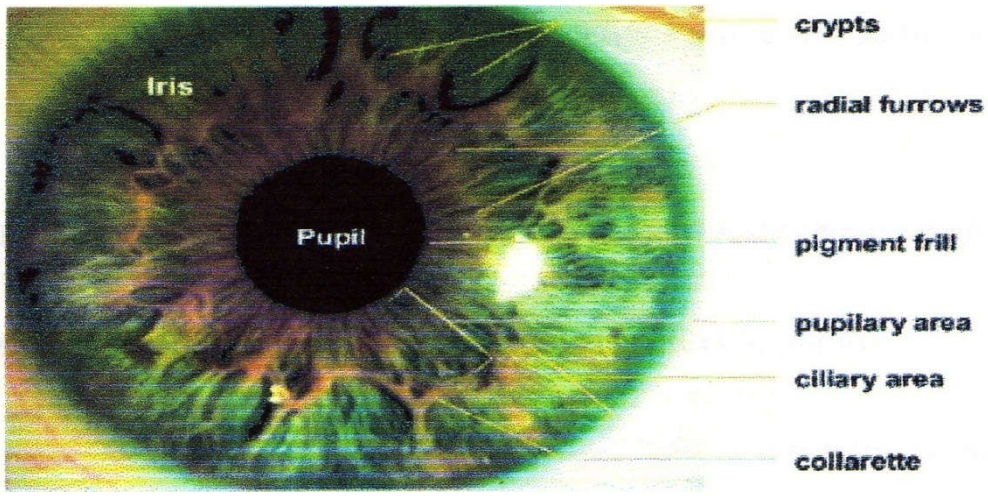


Figure III.1: L'œil humain

III.1.3. A Propos de l'Iris

L'iris est une région de l'œil "relativement stable":

- "Stable" car seules quelques maladies rares peuvent en modifier rapidement l'apparence.
- "Relativement" car, avec l'âge, l'iris change d'apparence.
- On estime à environ 5 ans la période naturelle de ces changements.

Ainsi, la grande période des changements rend possible l'actualisation des données. On considère que les images sont immuables. Chaque œil possède une texture très détaillée et unique. Même capturée avec une faible résolution, l'image d'un iris contient déjà plus d'une centaine de degrés de libertés. Ceci est dû à l'existence d'un réseau dense et très fin de minuscules tubes qui assurent l'indépendance statistique des iris observés. Les recherches menées dans les laboratoires de British Telecom montrent une indépendance statistique quasi-parfaite entre les différentes régions de l'oeil. Il est donc utile de traiter l'ensemble des surfaces de l'iris.

III.1.3.1Eclairage

- Configuration de ou des sources lumineuses.
- Son intensité.
- Configuration des filtres optiques antireflets éventuels.

Il est important de ne négliger aucune des imperfections conjuguées lors de la prise de vue de l'œil : position, reflets, taille de l'iris dans l'image ...

III.1.3.2 Traitement

Le code existant doit avoir une exécution plus fluide et plus rapide ; et ceci par l'emploi d'une ou plusieurs méthodes telles que :

- Réécriture en MATLAB
- Compilation simple
- Optimisation et adaptation du code

Il est important que les programmes ainsi produits soient simples à déplacer (taille minimale) et que l'utilisateur soit sollicité le moins possible.

Les fonctions de recherche automatique des paramètres de la pupille , de l'iris et du blanc de l'œil sont à écrire. Le principe de base du traitement (filtrage, opérations matricielles...) est conservé.

III.1.3.3. Présentation

Plusieurs images sont à afficher:

- Images en provenance de la caméra (positionnement de l'œil de l'individu testé)
- Affichage de la liste des résultats des opérations (historique)
- Affichage de la liste des individus authentifiés les plus probables (classement)

III.1.4. Reconnaissance de l'iris:

But: L'identification de l'iris est basée sur l'interprétation et la comparaison des informations entre deux iris d'un même œil (gauche ou droite) appartenant à deux individus pouvant être la même personne ou non : dans le premier cas, il doit y avoir authentification, dans le second non.

La sélection des images d'iris par la carte au travers de la caméra et de l'objectif peut donner lieu à des différences de taille et d'orientation entre plusieurs clichés: il est donc nécessaire de rendre l'information utile (l'iris uniquement) indépendante des paramètres de l'image. C'est pourquoi il faut éliminer les informations non utiles voire gênantes : la pupille, le blanc de l'œil, peut-être les reflets et les zones de la paupière dans le cas d'empiétement significatif sur l'iris. Cette opération permettra donc de rendre le traitement ultérieur plus fiable car on ne compare que les informations de l'iris seuls significatifs et en outre de gagner en occupation mémoire lors de la sauvegarde des fichiers image.

Principe: Nous avons précédemment énoncé les zones d'informations de l'image qui sont à éliminer : la pupille, le blanc de l'œil, et éventuellement les reflets : zones de dégradation absolue de l'information, et les parties de paupière qui empiètent sur l'iris. Pour les deux premières zones, le traitement sera plus simple pour des raisons géométriques simples : l'iris a toujours la même forme générale : une ellipse, dont il va falloir justement trouver les paramètres. La pupille et le blanc de l'œil peuvent donc être repérés au moyen de deux ellipses : la première, intérieure à l'iris qui contient la pupille et la seconde, extérieure qui délimite le blanc de l'œil.

Cela paraît simple au vu des 5 paramètres qui la caractérisent : son centre en abscissesX_0, en ordonnées Y_0, son grand rayon A

et son petit rayon B, et de surcroît l'angle I que fait l'ellipse par rapport à l'horizontale fig. III.2

L'opération de sélection de l'iris se décompose en deux opérations identiques de recherche d'ellipse : l'iris est ensuite localisé dans une couronne déformée définie par ces deux ellipses.

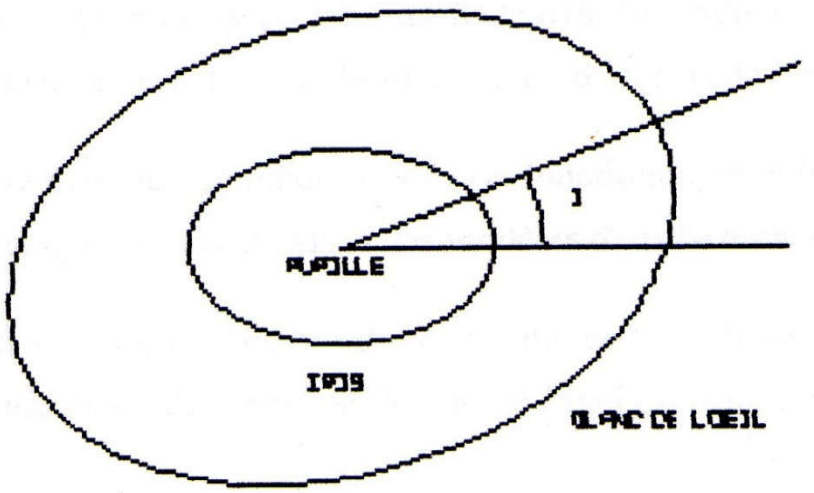


Figure III.2: le grand rayon a et le petit rayon b

Cette géométrie particulière de l'œil est un avantage et un inconvénient : l'avantage est que le contour de délimitation est mémorisable (5 paramètres seulement au lieu d'un ensemble de coordonnées de pixels) et l'inconvénient est que les ellipses n'ont pas le même angle de référence, ce qui complique la transformation polaire rectangulaire.

III.1.4.1Fonctionnement d'un système d'identification par l'iris

Une fois l'image de l'iris acquise, un système de reconnaissance d'iris est composé de plusieurs modules illustrés dans la figure III.3

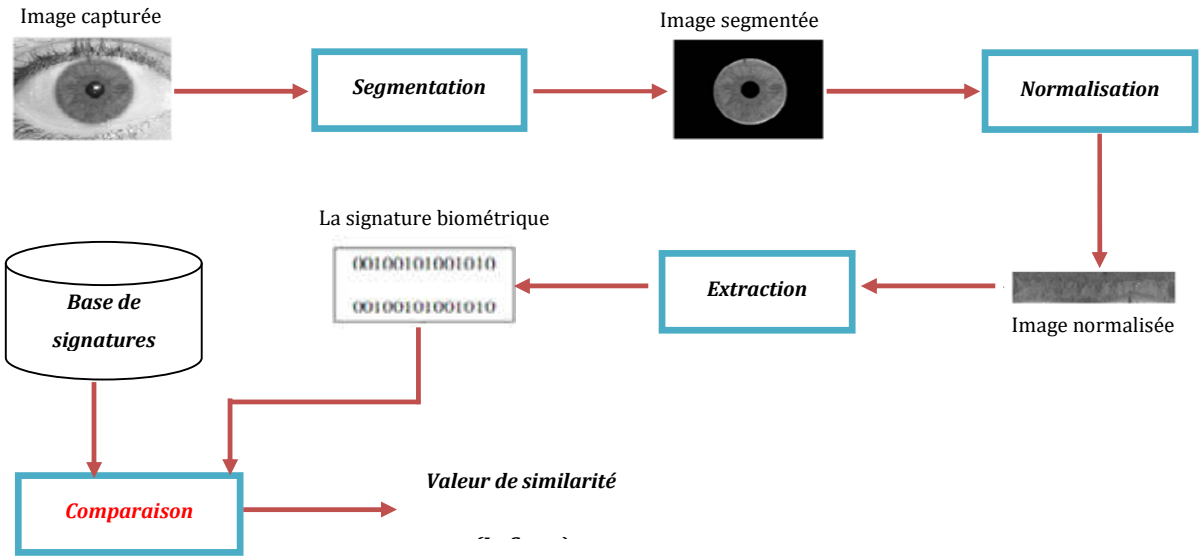


Figure III.3: Etapes de la reconnaissance par l'iris.

III.1.5. Traitement de l'image adaptée [EMI 07]

La méthode de JOHN DAUGMAN :

Elle est la base du logiciel exécutable utilisé dans tous les systèmes d'identification d'iris déployés jusqu'ici

commercialement , incluant ceux par British Telecom, laboratoires des USA Sandia, Laboratoire Physique National Britannique, Nbtc, Panasonic, Atterrisseur,0ki, EyeTicket, IBM SchipholGroup, Joh.Enschede,IriScan, iridien, et Sensar. Tous les organismes d'essai ont rapporté un taux d'erreur de 0 dans leurs essais.

John Daugman est le pionnier dans le domaine de la reconnaissance des personnes par l'iris. Il a proposé une méthode complète de traitement d'images d'iris basée sur le codage de la phase de Gabor 2D. Des évaluations récentes montrent que même aujourd'hui la méthode de Daugman reste meilleure en termes de performances et de vitesse. Néanmoins, les solutions commerciales imposent encore aux utilisateurs des contraintes fortes à **code** l'acquisition afin d'obtenir des images de bonne qualité.

Le code de l'iris : La méthode Daugman

Le système de Daugman est basé sur plusieurs avancées majeures et originales. Tout d'abord il a proposé une méthode de détection de l'iris dans l'image de l'œil. Détecter l'iris revient à détecter au moins les pixels formants la frontière entre l'iris et la pupille et l'iris et le blanc de l'œil fig.III.1. Plus de précision 30 seront données dans le sixième chapitre de cette thèse. Il a aussi proposé une méthode pour normaliser la forme de l'iris, une méthode d'extraction de paramètres intrinsèques de l'iris, un moyen de transformer ces paramètres extraits en un code de taille constante et un moyen de prise de décision qui sied au temps aux systèmes de vérification qu'à ceux d'identification des individus.

Normalisation de l'iris : Méthode pseudo polaire

Comme c'est indiqué dans le chapitre un, l'iris est un disque irrégulier. Ces irrégularités sont dues à la dilatation et contraction de la pupille, au fait que les deux cercles ne sont pas concentriques et au fait des changements non linéaires de la texture de l'iris. Ces caractéristiques ont poussé Daugman à développer une méthode de normalisation pseudo-polaire du disque de l'iris appelée la méthode 'Rubber Sheet' dont une signification imagée pourrait être vu comme une tentative d'étendre le disque de l'iris comme du caoutchouc. Cette méthode est pseudo-polaire car les deux cercles de l'iris et de la pupille ne sont pas concentriques. Le procédé peut être expliqué de la manière suivante :

A chaque pixel de l'iris dans le domaine cartésien lui est assigné un correspondant dans le domaine pseudo polaire suivant la distance du pixel par rapport aux centres des cercles et l'angle qu'il fait avec ces centres. Plus précisément la transformation se fait suivant l'équation suivante

$$x(r, \theta) = (1-r)\, x_p(\theta) + r\, x_z(\theta)$$

$$y(r, \theta) = (1-r)\, y_p(\theta) + r\, y_z(\theta)$$

Où xp(θ) représente l'abscisse du point de la frontière détectée de la pupille dont le segment qui passe par ce point et le centre de la pupille fait un angle θ avec une direction choisie. De même y p(θ) représente l'ordonné de ce même point, alors xs(θ) ys(θ) représentent les coordonnées des points obtenus par le même principe mais sur le contour de l'iris. L'image en bas de la figure III.4 montre une image normalisée obtenue par ce processus. Elle est rectangulaire de taille constante, généralement la taille choisie est de 80*512 pixels. La largeur de l'image représente la variation sur l'axe angulaire alors que la hauteur représente les variations sur l'axe radial.

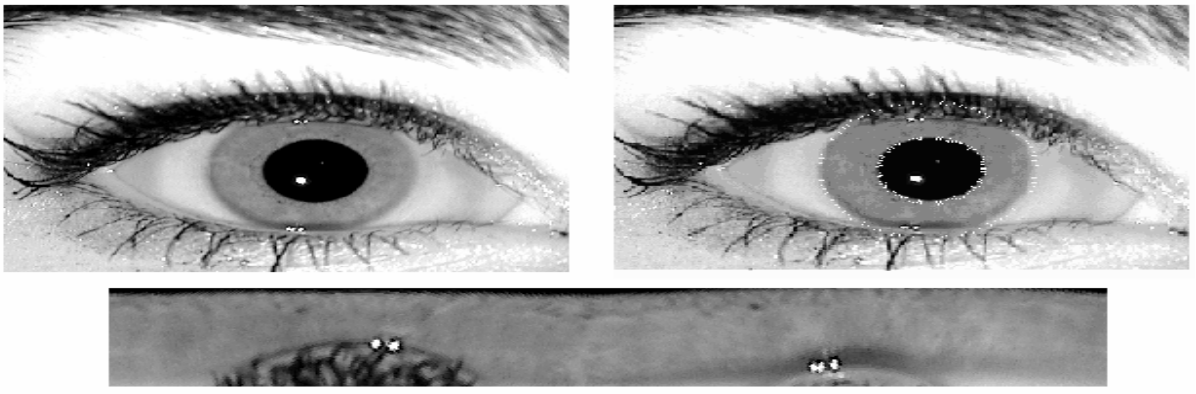


Figure III.4. Une image de l'œil (figure haut gauche), une image d'iris segmenté (haut droite) et une image d'iris normalisé (bas)

Extraction des caractéristiques : Utilisation des filtres de Gabor

L'extraction des caractéristiques repose sur l'utilisation des filtres de Gabor 2D que Daugman a adopté au traitement d'images. Les filtres de Gabor sont connus comme le moyen d'analyse espace-fréquence qui minimisant l'incertitude de Heisenberg qui exprime que plus on est précis dans l'analyse de l'information dans l'espace du pixel et moins on le sera dans l'espace fréquentiel et vice versa. Cette spécificité a fait des filtres de Gabor un moyen puissant d'analyse de texture et de classification. Les filtres de Gabor analysent la texture de l'iris suivant différentes résolutions et différents angles, leur forme est donnée par l'équation ci-dessous.

$$\int_\rho \int_\varphi e^{-i\omega(\theta_0 - \varphi)}\, e^{-(r_0 - \rho)^2/\alpha^2}\, e^{-i\omega(\theta_0 - \varphi)^2/\beta^2}\, I(\rho,\varphi)\rho d\rho d\varphi \qquad \textbf{III.1}$$

Où I (ρ, φ) représente l'image en coordonnées polaires. α et β les paramètres des dimensions de la fenêtre d'analyse de Gabor, ω la fréquence de l'ondelette de Gabor couvrant 3 octaves en proportion inverse de β. Enfin r0 et θ0 représentent les coordonnées des points d'analyse de l'ondelette de Gabor.

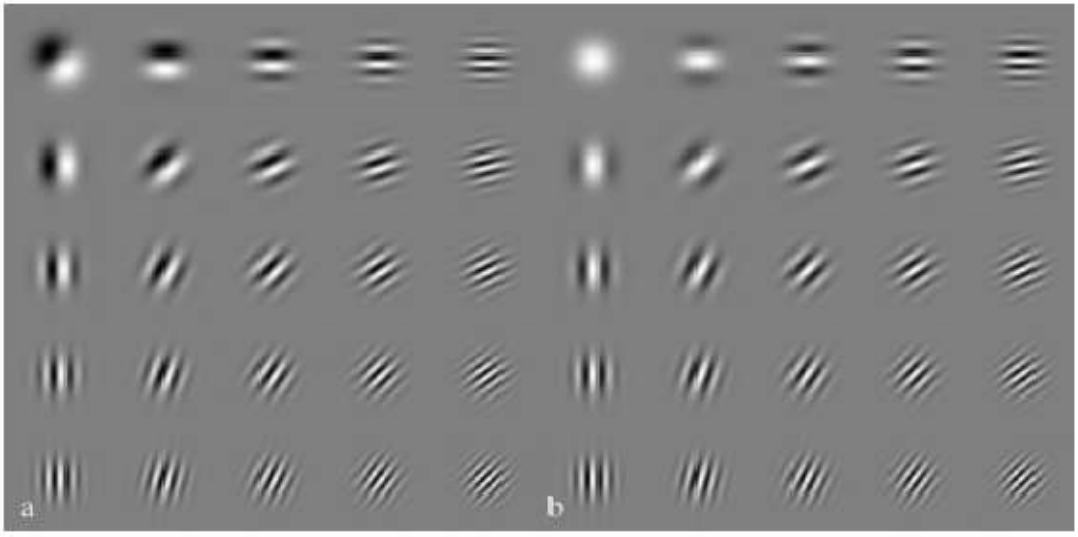


Figure III. 5 La banque de filtres de Gabor suivant plusieurs orientations et plusieurs résolutions parties réelles (b), et parties imaginaires (a).

Comme on peut le remarquer dans l'équation III-1, les filtres de Gabor ont une forme complexe qu'il est possible d'exploiter. En effet étant en quadrature de phase, il est important d'étudier la dépendance entre la partie réelle et la partie imaginaire des coefficients de Gabor. Deux choix triviaux s'offrent à nous, l'étude de l'amplitude et l'étude de la phase de Gabor. Il est établi que la phase des analyses multirésolution est plus informative que les amplitudes.

Daugman a d'ailleurs fait ce choix en considérant uniquement la phase de Gabor. En effet chaque phase de Gabor sera codée sur 2 bits suivant le principe du codage quatre quadrants illustré dans la figure III,6. Selon que la phase appartienne à l'un des quatre quadrants uniformément découpé du cercle trigonométrique, elle sera codée différemment.

Il est à noter que chaque passage entre un quadrant et un quadrant adjacent entraine un changement d'un seul bit. Ceci limitera les erreurs si la phase calculée est à la frontière entre deux quadrants adjacents. Cette opération revient à coder les signes de la partie réelle et de la partie imaginaire des coefficients de Gabor obtenus et d'assigner 1 au code si le coefficient est positif et 0 si le coefficient de Gabor est négatif.

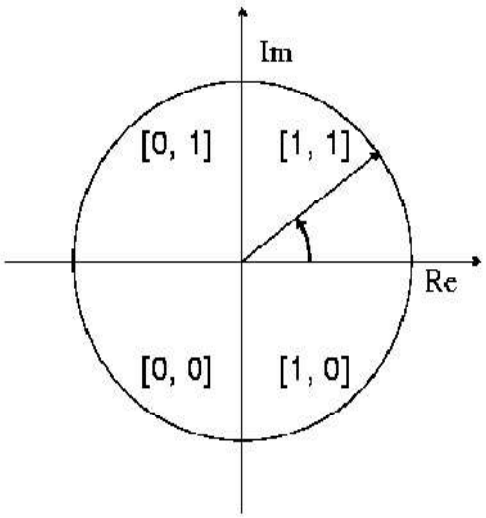


Figure III.6 Le principe de codage de phase sur quatre quadrants et en deux bits.

Cette opération est réitérée plusieurs fois, autour de plusieurs points d'analyse, suivant plusieurs résolutions et orientations des filtres de Gabor jusqu'à ce que l'on obtienne un code de taille 256 octets ou 2048 bits.

La figure III.7 représente plusieurs codes obtenus par la méthode proposée par Daugman.

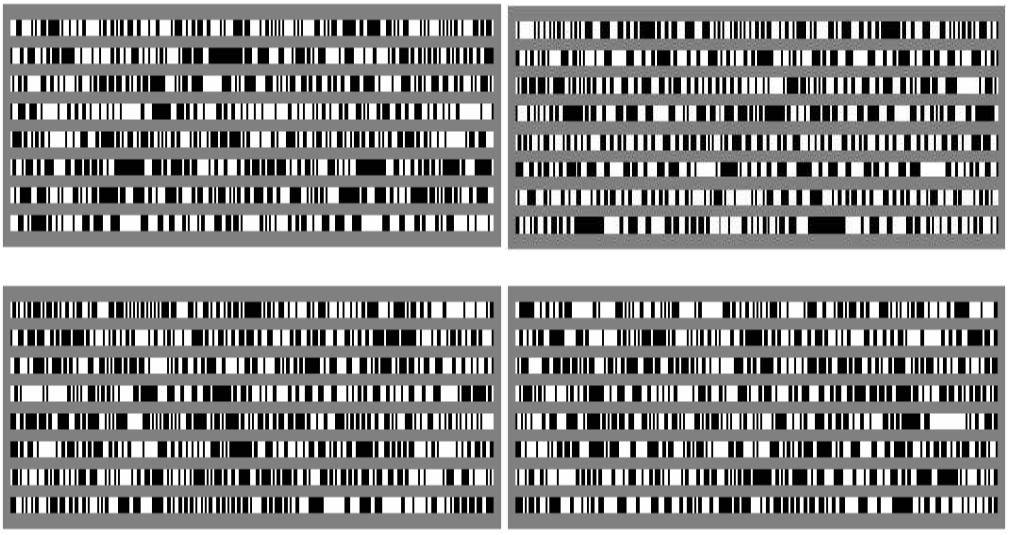


Figure III.7 Différents exemples d'iriscode générés par la méthode Daugman.

En plus des codes, des masques sont calculés de taille fixe (2048 bits) qui indiquent pour chaque bit du code s'il faut le prendre en considération ou non. Les bits ignorés proviennent généralement des points d'analyse couverts par les paupières, les cils, un faible rapport qualité bruit, des réflexions lumineuses …

Calcul de Score : La distance de Hamming

Le calcul de score s'effectue au moyen du calcul de la distance de Hamming qui est donnée par la formule suivante :

$$\mathrm{HD}_{\mathrm{raw}} = \frac{\|(\mathrm{code}A \otimes \mathrm{code}B) \cap \mathrm{mask}A \cap \mathrm{mask}B\|}{\|\mathrm{mask}A \cap \mathrm{mask}B\|}.$$

Où code A et code B sont deux codes calculés à partir de deux images d'iris par le procédé précédemment décrit et mask A et mask B représentent leurs masques associés. Littéralement la distance de Hamming calcule le nombre de bits différents et valides pour les deux iris entre le code A et le code B. Plus la distance de Hamming est faible, plus les deux codes se ressemblent. Une distance 0 correspond à une parfaite correspondance entre les deux images alors que deux images de personnes différentes auront une distance de Hamming proche de 0.5.

L'introduction des masques A et B dans la mesure de la distance de Hamming fait que celle-ci n'est pas mesurée uniformément quelque soient les deux échantillons que nous tentons de mettre en correspondance. En effet plus les paupières, les cils et autres bruits couvrent la texture de l'iris et plus les codes correspondants contiennent des bits erronés qui n'interviendront pas dans le calcul de la distance de Hamming. Or une distance mesurée à partir de peu de bits valides n'a pas la même signification, ni sans doute la même plage de variation, qu'une distance mesurée sur plus de bites. Daugman propose 34 alors une méthode de normalisation de la distance de Hamming pour tenir compte du nombre de bits qui interviennent dans le calcul de la distance a été calculée. La nouvelle distance de Hamming normalisée est alors calculée selon la formule suivante :

$$\mathrm{HD}_{\mathrm{norm}} = 0.5 - (0.5 - \mathrm{HD}_{\mathrm{raw}})\sqrt{\frac{n}{911}}.$$

Où n représente le nombre de bits valides, HDraw la distance de Hamming précédemment définie et 911 un coefficient de normalisation qui correspond à la moyenne du nombre de bits valides pour une comparaison entre deux codes d'iris.

Pour pallier aux problèmes de rotations qui sont dus aux positions de l'œil par rapport à la caméra, Daugman génère 7 iris codes chacun correspondant à un angle particulier de rotation de l'image de référence. La comparaison entre deux iris revient donc à comparer un iris code avec les 7 iris codes correspondants aux différentes rotations. La distance considérée est la distance minimale normalisée entre les sept comparaisons.

Prise de décision : Les lois de Bernoulli

Il s'agit maintenant de prendre une décision finale quant à la nature de la comparaison effectuée par rapport à la distance mesurée. Selon l'architecture fixée plus haut, il faudrait fixer un seuil de décision en deçà duquel les deux iris comparés seront considérés comme appartenant à la même personne.

Généralement, en biométrie ou plus généralement dans un problème de reconnaissance des formes, la procédure de détermination du seuil se fait en constituant une base de données qu'on appelle base d'apprentissage différente de la base sur laquelle seront effectués les tests. Le seuil qui donne les meilleures performances sur la base d'apprentissage est alors utilisé sur la base de test.

Mais Daugman a une toute autre approche. En effet, en utilisant les théorèmes liés aux essais de Bernoulli, Daugman a réussit à accomplir quelque chose de très rare en biométrie : prédire la distribution des distances inter-classe et donc fixer des seuils optimaux en les généralisant sur des bases plus grandes et sans constituer de base d'apprentissage. En effet Daugman a supposé qu'un code d'une personne peut correspondre à plusieurs lancés de pièces puisque la probabilité d'avoir 0 ou 1 dans un code d'iris est égale à 0.5. La loi de Bernoulli stipule qu'en N tentatives de lancés de pièce de monnaie, la probabilité d'avoir x fois face peut être prédite par une loi binomiale. En matière d'iris l'adaptation d'une telle formule n'est pas évidente. En effet si la longueur du code est constante et égale à 2048 bits, il n'est pourtant pas juste de supposer que les 2048 bits sont indépendants les uns des autres. En effet la texture de 35 l'iris est fortement corrélée surtout le long de l'axe des angles sans oublier un détail technique de la méthode de Daugman selon lequel à une seule phase correspond 2 bits dans le 'iris code'.

Pour mesurer le nombre d'opérations indépendantes que fait intervenir le calcul de l'iris code, Daugman a calculé sur une base de 70 personnes toutes les comparaisons possibles entre iris de deux personnes différentes et a tracé la distribution des distances calculés. A partir de cette distribution il a été en mesure de calculer le nombre de comparaisons indépendantes qu'on effectue généralement quand deux iris sont comparés en approximant la distribution observée par une distribution binomiale. D'après les tests de Daugman, ce nombre est égal à 256 et constitue le nombre de points caractéristiques que possède un iris appelé aussi degrés de liberté.

Des essais sur des bases de plus en plus grandes ont montré la précision de l'estimation de la distribution inter-classe apprise sur finalement peu de personnes. Comme indiqué précédemment, un système d'iris a été installé dans les émirats arabes unis dès 2001. Une base de référence constituée de 632 500 personnes a été mise à disposition du laboratoire de l'université de Cambridge par le ministère de l'intérieur émirati. Sur cette base Daugman a effectué 200 milliards de test imposteurs et a tracé la distribution des distances obtenues et l'a comparé à la distribution obtenue sur sa base de données originelle sur laquelle seulement 9 millions de comparaison entre iris différents ont été effectuées. Les deux distributions montrent une coïncidence quasi parfaite en termes de moyennes, d'écart type et de comportement (0.49 de moyenne et 0.033 d'écart type contre 0.49 de moyenne et 0.0317 pour la deuxième). La figure III.8 montre l'exactitude des estimations de Daugman sur ces deux bases de tailles différentes.

Nous avons vu que Daugman effectue 7 comparaisons pour obtenir une distance entre deux images d'iris. Ces opérations répétées ne sont pas sans conséquence sur les distributions inter-classe calculées précédemment par Daugman. En effet même pour des comparaisons différentes, le fait d'effectuer plusieurs essais fait dévier la distribution inter-classe de la distribution théorique. Cependant même dans ce cas Daugman est parvenu à prédire le comportement de cette distribution modifiée après k rotations sur l'image d'iris à partir de la distribution binomiale originelle en utilisant la formule suivante:

$$f_k(x) = \frac{d}{dx} F_k(x)$$
$$= k f_0(x) [1 - F_0(x)]^{k-1}$$

Où fk est la nouvelle distribution à estimer, f0 la distribution estimée précédemment sur une seule rotation possible k est le 36 nombre de rotation possible (7 dans ce cas), et Fk et F0 les probabilités de fausse acceptation respectivement dans le cas de k rotations et une seule rotation. La nouvelle distribution fk est confrontée aux observations obtenues sur la base émirati et encore une fois la coïncidence est parfaite entre la distribution théorique et celle observée.

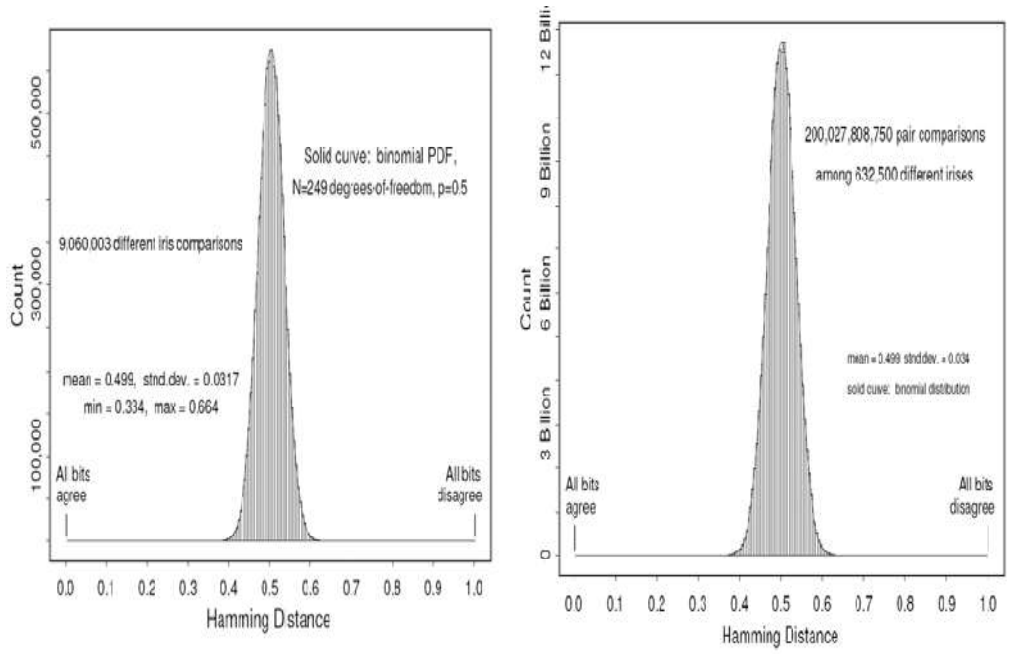


Figure III.8 Les distributions inter-classe sur deux bases de données différentes et de différentes tailles. Les distributions sont tirées de l'article de Daugman, .

Finalement puisque la distribution inter-classe est estimée de manière fiable, il est possible de fixer des seuils qui correspondent à des fonctionnements particuliers du système d'iris. Généralement le seuil choisi pour les systèmes d'iris est égal à 0.33 ce qui correspond à un fonctionnement du système d'iris à 0% de FAR.

Daugman a proposé aussi une prise de décision dépendante de la qualité de l'image d'iris (pourcentage d'iris apparent). En effet, comme on peut le remarquer dans le tableau Tab3-1, plus le nombre de bits valides est petit plus la distance de Hamming lui correspond un seuil plus petit. A partir de l'équation de la distance normalisée et à partir des observations de Daugman voici un tableau récapitulatif des pourcentages d'iris apparent en fonction du nombre de bits mis en correspondance et du seuil de décision associé.

number of bits compared	*approximate percent of iris visible*	*maximum acceptable fraction of bits disagreeing*
200	17%	0.14
300	26%	0.20
400	35%	0.24
500	43%	0.27
600	52%	0.29
700	61%	0.31
800	69%	0.32
911	79%	0.33
1000	87%	0.34
1152	100%	0.35

Tableau III.1 Seuils fixés par Daugman selon le nombre de bits valides qui ont servi au calcul de la distance de Hamming normalisée et donc selon le pourcentage d'iris apparent.

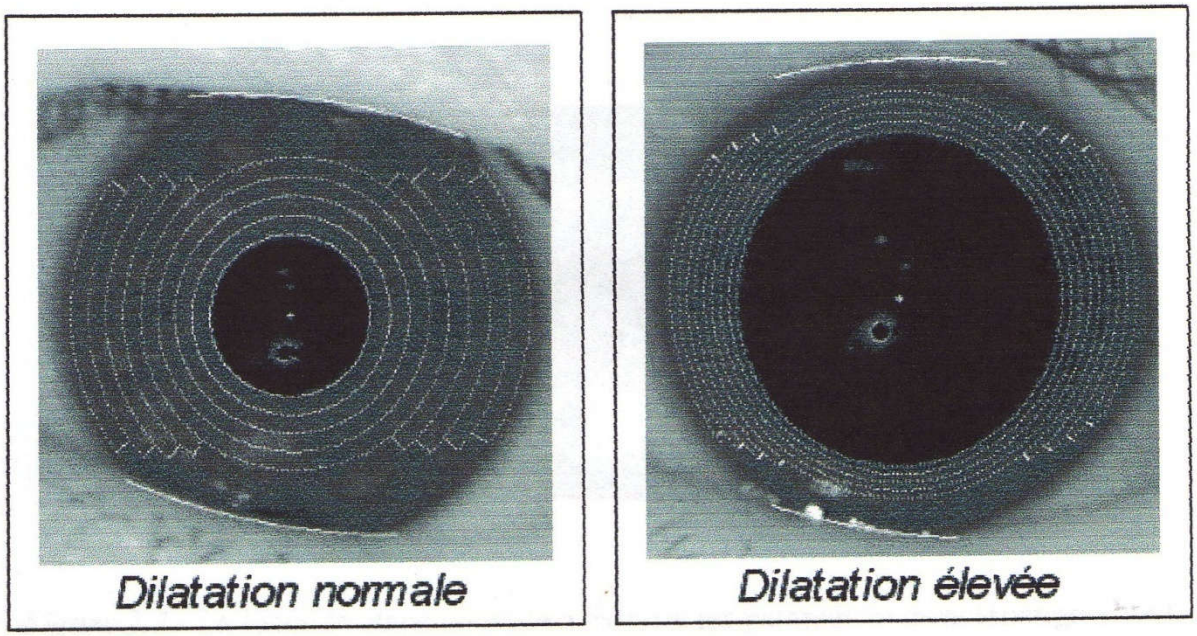
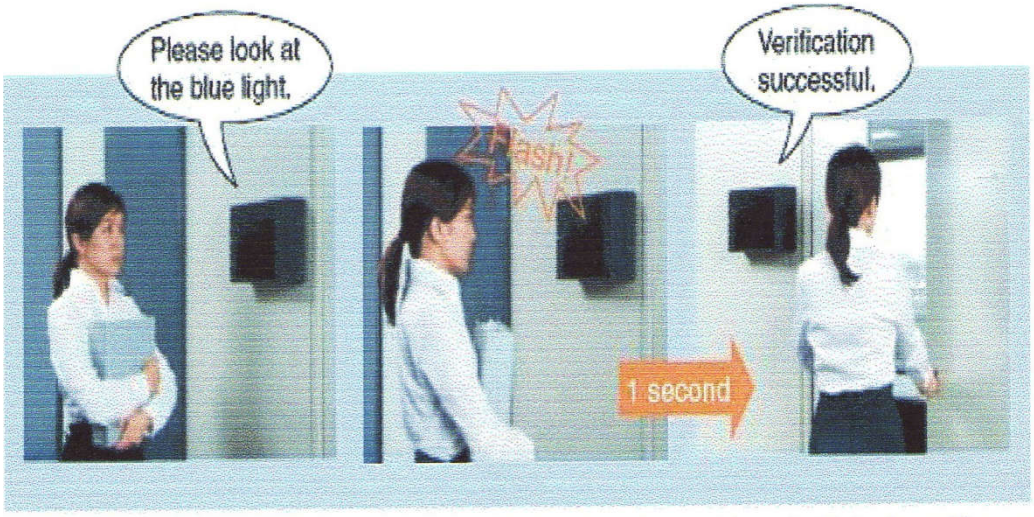


Figure III.9: dilatation normale et dilatation élevée de la pupille

- La taille des bandes varie en fonction de la dilatation de la pupille (voir illustration). Cette technique permet de s'affranchir du degré de dilatation de la pupille.
- Avec le même nombre de bande sur une pupille très dilaté, on retrouve le même motif que sur l'œil avec une dilatation normale de la pupille.



Figures III.10: La première étape consiste à chercher la position de l'iris l'image

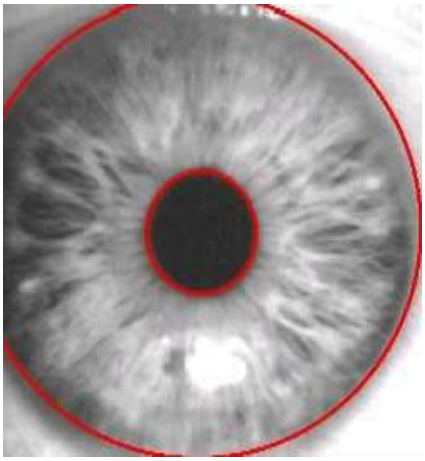


Figure III.11 La seconde étape consiste à extraire les paramètres caractéristiques de l'iris.

III.2 Identification par les empreintes digitales :

Pourquoi l'empreinte digitale :

- La reconnaissance des empreintes digitales est la technique biométrique la plus ancienne et la plus mature. Elles ne se modifient donc pas au cours du temps (sauf par accident comme une brûlure par exemple).
- La probabilité de trouver deux empreintes digitales similaires est de 10^{-24}.Les jumeaux, par exemple auront des empreintes très proches mais pas semblables.
- Les systèmes d'identification qui sont basés sur cette modalité représentent 50% du marché.
- Le taux d'erreur des produits disponibles sur le marché est proche de 0%.

Dans cette partie, nous présentons les caractéristiques d'empreinte digitale puis, nous citons les différentes représentations de l'image d'empreinte, ensuite nous identifions les propriétés des images d'empreintes digitales, puis nous citons les différentes approches et les travaux qui portent sur l'extraction des caractéristiques de cette modalité. On terminera cette partie par les différents problèmes rencontrés lors de l'extraction des minuties

III.2.1 Empreintes digitales :

L'empreinte digitale est la caractéristique d'un doigt. On estime que les empreintes digitales commencent à se former entre la 10è et la 16è semaine de vie du fœtus, par un plissement des couches cellulaires. Les circonvolutions des crêtes leur donnant leur dessin caractéristique vont dépendre de nombreux facteurs, comme la vitesse de croissance des doigts, l'alimentation du fœtus, sa pression sanguine, etc. Ce qui fait que non seulement chaque individu, mais aussi chaque doigt, a son empreinte propre. Alors si deux vrais jumeaux ont des empreintes digitales ressemblantes, elles sont pourtant différentes. Ainsi les empreintes digitales sont utilisées depuis longtemps pour l'identification et l'investigation juridique.

Figure III.12: Empreinte digitale acquise par un capteur optique

Une empreinte digitale se compose de crêtes et de bifurcations qui présentent de bonnes similitudes dans chaque petite fenêtre locale, comme le parallélisme et la largeur moyenne (figure III.13). Cependant, les recherches sur l'identification d'empreinte digitale ont montré que celles ci ne sont pas bien distinguées par leurs crêtes et bifurcations, mais par des minuties qui sont des points anormaux sur les crêtes.

- ***Les minuties*** : Les empreintes digitales présentent plusieurs types de points dont la détermination repose sur des règles précises et complexes. Les bifurcations et les fins de crêtes permettent la reconstitution de toutes les minuties, toute minutie peut se composer de combinaisons de bifurcations et de fins de crêtes. Par exemple, les anneaux peuvent être visualisés en tant que deux bifurcations qui se superposant et un ilot peut être représenté par deux fins de crêtes à courte distance (figure III.14).

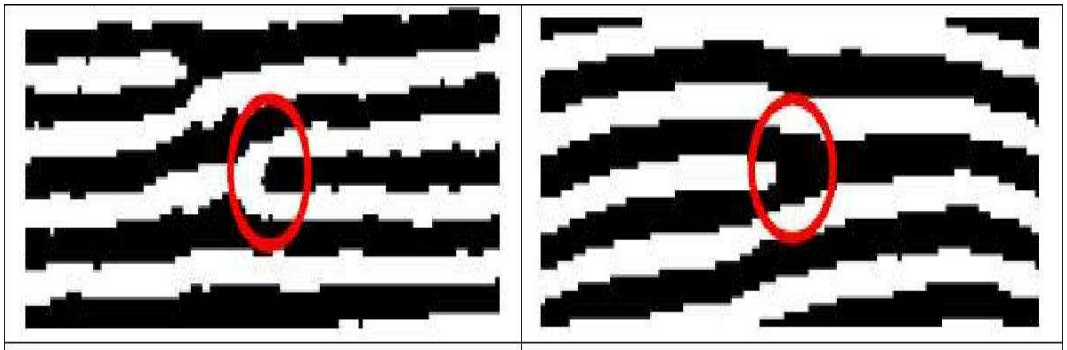


Figure III.13: Deux types de minuties les plus utilisés dans la littérature

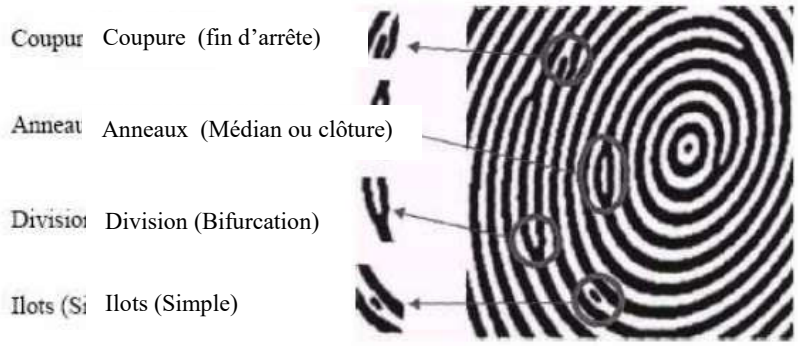


Figure III.14: Exemple de quatre familles de crêtes.

III.2.1.1 Conception du système de reconnaissance des empreintes digitales :

Un système de reconnaissance des empreintes digitales est un système automatique de reconnaissance de formes qui se compose de trois étapes principales :

- **Acquisition :** Les empreintes digitales sont capturées et stockées sous forme d'images.

Extraction des caractéristiques: les caractéristiques essentielles sont extraites à partir des images.

- **Prise de décision :** Les caractéristiques acquises sont comparées avec les caractéristiques stockées dans une base de données et, à partir du résultat de cette comparaison ; une décision est prise

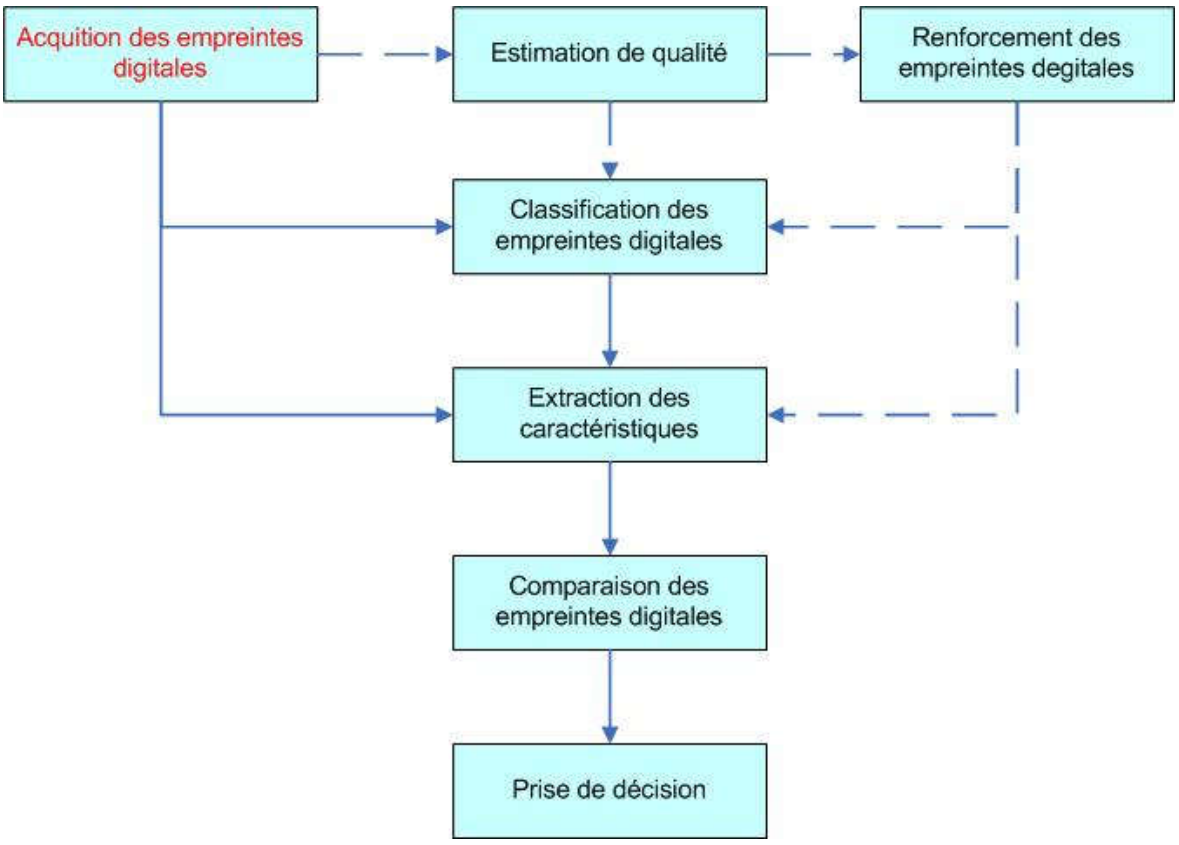


Figure III.15 : Conception d'un système biométrique basé sur les empreintes digitales

III.2.1.2 Représentation des empreintes digitales

Pour bien distinguer des empreintes digitales et pour répondre est-ce que deux empreintes digitales sont extraites à partir du même doigt, Il est nécessaire de choisir des caractéristiques qui sont invariantes malgré à l'orientation de placement du doigt sur le capteur et la déformation élastique du doigt pendant l'acquisition.

Plusieurs représentations des empreintes digitales sont proposées, et elles sont classifiées dans deux types principaux: représentation locale et représentation globale. La représentation globale est un attribut entier du doigt et la représentation locale se compose de plusieurs composants, chaque composant typiquement dérivé d'une région dans l'espace limitée de l'empreinte digitale. Généralement, des représentations globales sont employées pour la classification d'empreinte digitale et des représentations locales sont employées pour la comparaison d'empreinte digitale.

a-Représentation globale :

Une des caractéristiques globales significatives utilisées pour des empreintes digitales est son type. Le modèle entier d'empreinte digitale est classé par un certain nombre des classes et généralement, les empreintes digitales sont classés en six classes principales: Les arcs (arch, tented arch) Les boucles (gauches, droites) et les spirales (whorl, whorl (twin loop)) (figure III.16(a)). Les empreintes digitales sont aussi distinguées par l'épaisseur de crêtes, la séparation de crêtes, leur profondeur et les locations des points critiques (les noyaux et les deltas) (figure III.16(b)).

- ***Le noyau ou centre*** : le noyau est le lieu de courbure maximale des lignes d'empreinte les plus internes. Il est aussi appelé le point core (figure III.16. (b)).
- ***Les deltas*** : un delta est proche du lieu où se séparent deux lignes d'empreintes vérifiant les propriétés suivantes : ces lignes se séparent suivant deux directions orthogonales et sont les lignes les plus internes vérifiant la propriété précédente (figure III.16.b)).

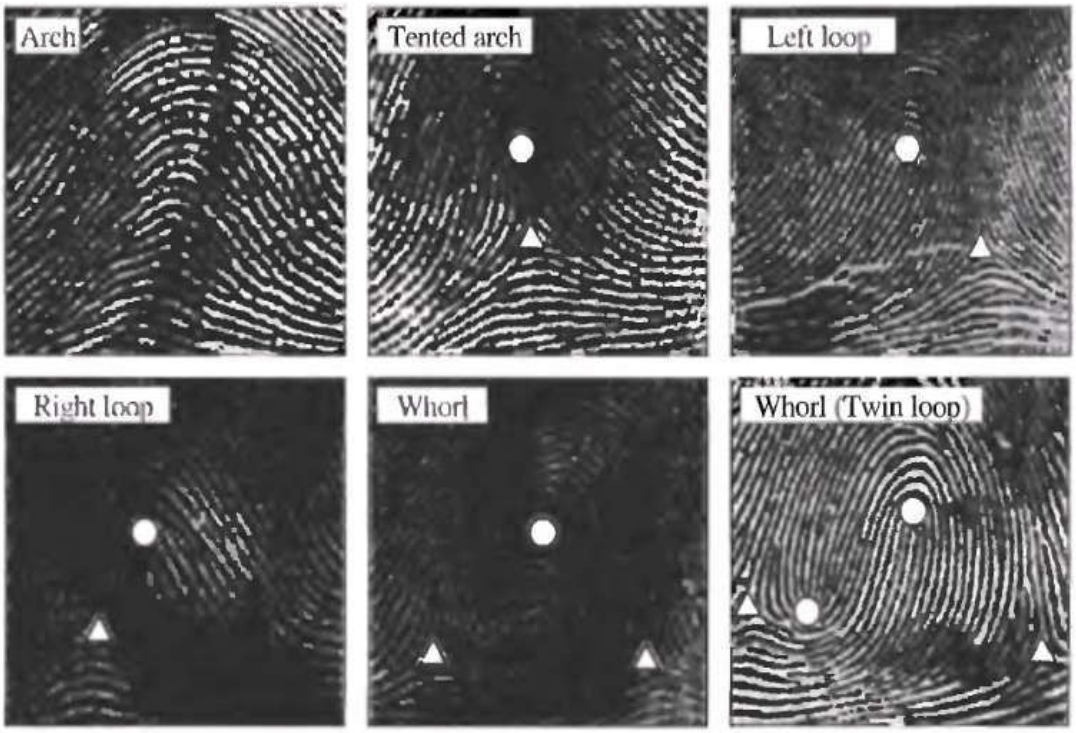


Figure III.16 (a)Six classes des empreintes digitales

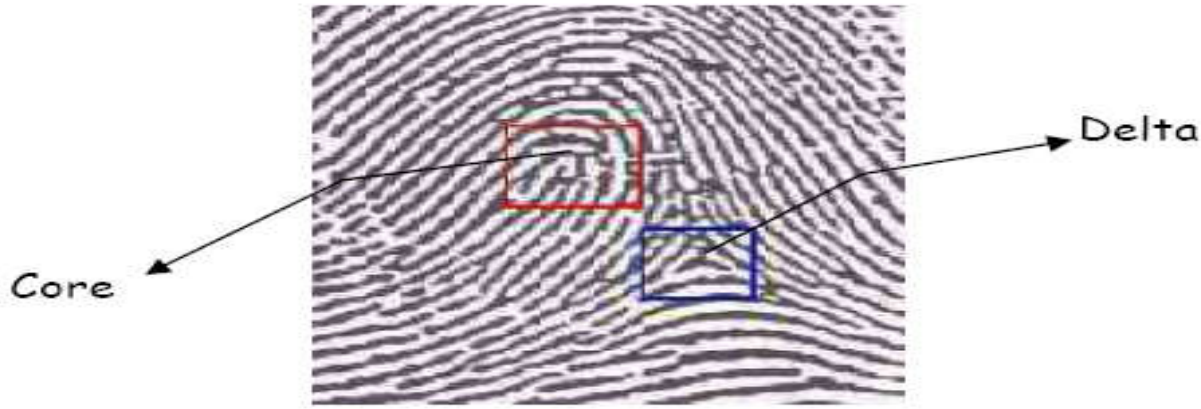


Figure III.16 (b) les noyaux et les deltas

b-Représentation locale:

Les caractéristiques locales les plus utilisées sont basées sur les minuties des crêtes (figure III.14). Les minuties sont les points anormaux sur les crêtes. L'ensemble des minuties extraites d'une empreinte digitale peut caractériser cette l'empreinte digitale. Les minuties sont relativement robustes avec des variations des empreintes digitales. Il existe plusieurs types de minuties ; cependant deux types des minuties sont les plus utilisés : la fin de crêtes et la bifurcation (figure III.14).

La représentation des minuties la plus simple constitue une liste de points définis par leurs coordonnées spatiales et en pratique, les minuties sont renforcées en ajoutant des caractéristiques comme l'orientation des crêtes, le compte des crêtes (le nombre des crêtes visitées pendant le traversa linéaire entre les deux minuties.), l'orientation du doigt, les locations des noyaux ou des deltas et la classe d'empreinte digitale. Généralement, une empreinte digitale avec une bonne qualité contient environ 50 à100 minuties.

Prétraitement :

Les algorithmes de reconnaissance des empreintes digitales sont sensibles à la qualité des images de celles-ci. L'étape de pré-traitement est alors nécessaire avant d'effectuer les étapes suivantes. La qualité des images d'empreintes digitales dépend de plusieurs facteurs comme : le contact avec le sonde, la qualité de la sonde, la profondeur des crêtes /bifurcations, etc. Généralement ; le prétraitement se compose du lissage, l'amélioration de contraste, le filtrage de domaine de spatiale/ fréquence. Dans les cas extrêmes, une empreinte digitale avec une qualité très pauvre peut être automatiquement renforcée en utilisant le filtrage de Gabor [Web.4].

III.2.1.3 Extraction des caractéristiques :

La plupart des systèmes de reconnaissance d'empreintes digitales emploient des minuties comme des caractéristiques des empreintes digitales. Ce paragraphe présentera alors les méthodes pour extraire des minuties à partir d'empreintes digitales.

Un extracteur de minuties cherche des fins de crêtes et des bifurcations dans les empreintes digitales. Si les crêtes sont bien déterminées, alors l'extraction de minuties est une tâche relativement simple. Cependant, dans la pratique, il n'est pas toujours possible d'obtenir une carte parfaite de crêtes. Donc la performance des algorithmes actuellement disponibles d'extraction de minuties dépend fortement de la qualité des images des empreintes digitales.

Généralement, un algorithme d'extraction de minuties se compose de 4 étapes principales : Estimation d'orientation, extraction des rides, amincissement et extraction des minuties .Le processus entier d'un algorithme d'extraction de minuties est montré dans la figure III.17

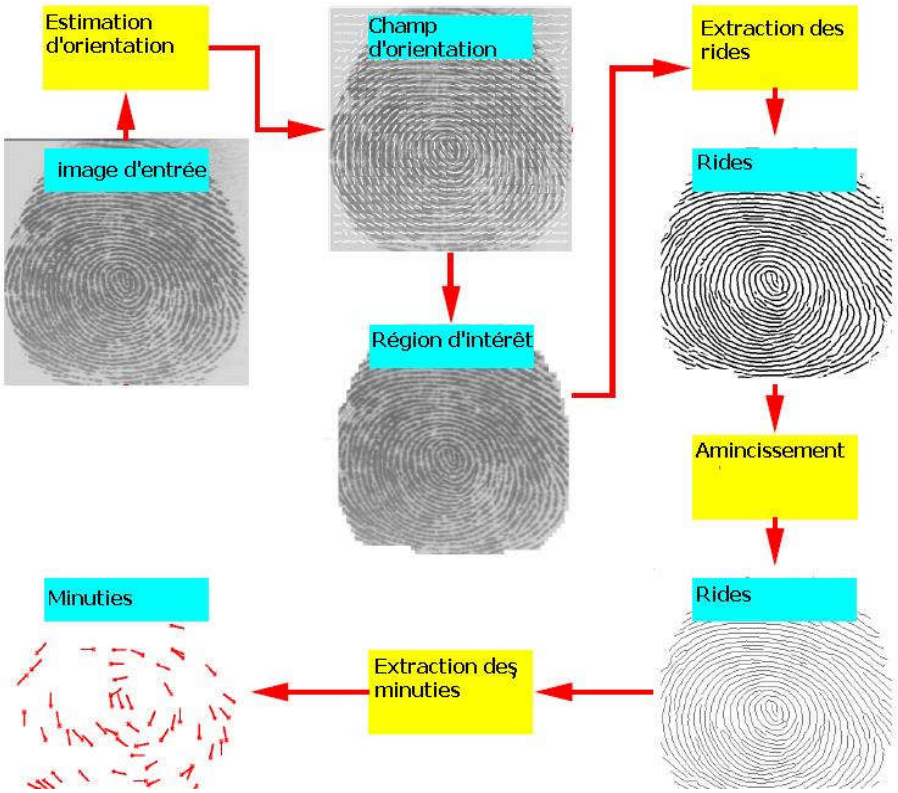


Figure III.17 : Processus d'extraction des minuties [Jai.00]

III.2.1.4.1Estimation d'orientation :

Le champ d'orientation d'une image d'empreinte digitale représente la nature intrinsèque de celle-ci (figure III.18).C'est une étape essentielle pour déterminer les crêtes et trouver la région d'intérêt de l'image d'empreinte digitale, Il existe plusieurs méthodes pour estimer le champ d'orientation des images d'empreinte digitale. Anil Jain et al. [Jai 00] ont proposé une méthode efficace pour estimer le champ d'orientation d'une image.

Figure III.18 : Le champ d'orientation d'une image d'empreinte digitale

L'idée principale de cette méthode est que l'image d'empreinte digitale se divise en plusieurs fenêtres de taille WxW, Pour tout pixel dans chaque fenêtre, on calcule les gradients Gx et Gy et puis on calcule l'orientation locale de ce pixel en utilisant la formule :

$$V_x(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{u=j-\frac{vv}{2}}^{j+\frac{vv}{2}} (2G_x(u,v)G_y(u,v)) \qquad (1)$$

$$V_y(i,j) = \sum_{u=i-\frac{vv}{2}}^{i+\frac{W}{2}} \sum_{u=j-\frac{vv}{2}}^{j+\frac{W}{2}} (G_x'(u,v) - G_y'(u,v)) \quad (2)$$

$$\theta(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{V_x(i,j)}{V_y(i,j)}\right) \quad (3)$$

Où ;

W est la taille de la fenêtre locale;
Gx et Gy sont les grandeurs de gradient dans respectivement des directions de x et de y,
CL (*i, j*) *est l'orientation locale du pixel (i,j)*

Le résultat de cet algorithme est comme dans la figure III.8.

III.2.1.4.2 Segmentation.

Après d'avoir estimé le champ d'orientation d'une image d'empreinte digitale, un algorithme de segmentation basé sur le niveau de certitude du champ d'orientation est employé pour localiser la région d'intérêt dans l'image d'empreinte digitale. Le niveau de certitude du champ d'orientation au pixel (i,j) est défini comme suit:

$$CL(i,j) = \sqrt{\frac{1}{w^2}\frac{V_x'(i,j) + V_y'(i,j)}{V_e(i,j)}} \quad (4)$$

$$V_e(i,j) = \sum_{u=i-\frac{vv}{2}}^{i+\frac{W}{2}} \sum_{u=j-\frac{vv}{2}}^{j+\frac{W}{2}} (G_x^2(u,v) + G_y^2(u,v)) \quad (5)$$

Où *W est la taille de la fenêtre locale;*
Gx et Gy sont les grandeurs de gradient dans des directions de x et de y
CL (*i, j*) *est l'orientation locale du pixel (i,j)*

Pour chaque pixel, si son niveau de certitude du champ d'orientation est inférieur à un certain seuil T, le pixel est alors marqué comme pixel de fond. Sinon, il est marqué comme un pixel de la région d'intérêt.

III.2.1.4.3 Détection de crêtes

L'objectif de l'algorithme de détection de rides est de séparer les rides des vallées dans une image d'empreinte digitale. Il existe plusieurs d'approches :

a-Fixe/adaptatif seuil: les pixels plus sombres qu'un seuil de constante/variable sont déterminés pour être des pixels de rides dans l'empreinte digitale. Ces approches généralement ne fonctionnent pas bien pour les parties bruyantes et l'image avec un contraste bas. [Mal.03]

b-Minimum local : cette approche emploie une propriété de rides qui consiste à ce que les valeurs de niveau gris sur des rides atteignent leurs minimums locaux tout le long de la direction normale de l'orientation locale des rides [Mal.03].

Normalement le résultat obtenu est une image binaire dans laquelle les pixels noirs sont les pixels des rides et les pixels blancs sont des pixels des vallées ou du fond. Généralement les rides détectées sont épaisses, puis un algorithme amincissant est employé pour obtenir des rides avec un pixel de petite grandeur [Web.4]. Ces rides sont utiles pour détecter des minuties.

III.2.1.4.4 Détection de minuties

Lorsque les crêtes sont bien déterminées les minuties seront facilement détectées:

- Les pixels avec trois pixels voisins sont identifiés comme bifurcations.
- Les pixels avec un pixel voisin sont identifiés comme arêtes de crêtes .Cependant, Ce n'est pas le fait que toutes les minuties détectées sont des bonnes minuties à cause des bruits.

III.2.1.4.5 Post-traitement

Dans cette étape, les vraies minuties sont extraites en utilisant un certain nombre d'heuristiques. Par exemple, trop de minuties dans une petite région peuvent indiquer la présence du bruit et elles pourraient être jetées. Deux fins de crêtes trop proches indique des fausses minuties produites par une coupure dans la ride etc. [Mal.03]

III.2.1.5 Assortiment des empreintes digitales

Il est très difficile d'assortir exactement deux empreintes digitales. La cause principale est la variabilité dans différentes impressions du même doigt (c.-à-d., grandes variations d'intra-classe). Les facteurs principaux responsables des variations d'intra-classe sont: déplacement, rotation, déformation non-linéaire, variation des pressions, changement d'état de peau, bruit, et erreurs d'extraction des caractéristiques etc. Par conséquent, les empreintes digitales d'un même doigt peuvent être différentes tandis que les empreintes digitales de différents doigts peuvent être ressemblantes.
Pour résoudre ce problème, il existe plusieurs approches classifiées en 3 catégories principales :

1. **Assortiment basé sur la corrélation :**

Cette approche est basée sur la corrélation des pixels de deux empreintes digitales. Deux images d'empreinte digitale sont superposées et la corrélation (au niveau intensité) entre les pixels correspondants est calculée pour différents alignements (par exemple déplacements et rotations). Cette approche est assez facile à réaliser mais son résultat est sensible à la variation comme la rotation, le déplacement, etc.

2. **Assortiment basé sur les crêtes**

Dans cette approche, on utilise des caractéristiques extraites des crêtes (orientation, texture, forme de ride, etc. pour comparer les empreintes digitales. L'avantage de cette approche est que les caractéristiques de crêtes peuvent être extraites plus exactement, cependant les distinctions de ces caractéristiques sont faibles

3. **Assortiment basé sur les minuties :**

C'est l'approche la plus utilisée dans la littérature, des minuties sont extraites à partir des deux empreintes digitales et stockées sous forme d'un ensemble de points dans le plan de deux dimensions. L'assortiment basé sur minuties essentiellement se compose de trouver l'alignement entre les minuties du motif et les minuties d'entrée. Le résultat est le nombre maximum des pairs de minuties. Il existe 3 méthodes différentes pour assortir des minuties

- Assortiment des minuties basé sur la transformation des Hough.
- Assortiment des minuties basé sur la minimisation d'énergie.
- Assortiment des minuties basé sur l'alignement.

III.2.1.6 Classification des empreintes digitales :

L'identification automatique basée sur des empreintes digitales exige l'empreinte digitale d'entrée à assortir avec un grand nombre d'empreintes digitales stockées dans une base de données (par exemple, la base de données de FBI contient plus de 200 millions des empreintes digitales). Pour réduire le temps de recherche et la complexité, il est souhaitable de classifier ces empreintes digitales d'une façon précise et cohérente tels que l'empreinte digitale d'entrée doit être assortie seulement avec un sous-ensemble des empreintes digitales dans la base de données. Rappelons (voir le paragraphe III.2.4.2.a) que les empreintes digitales sont classifiées en six classes différentes : arch, tented arch, left loop, right loop, whorl et twin loop

- Une empreinte digitale d'**arch** a les rides qui entrent d'un côté, se lèvent à une petite bosse, et sortent du côté opposé d'où elles sont entrées. Les archs n'ont pas des boucles ou des deltas;

- Une empreinte digitale de **tented arch** est semblable à une empreinte digitale d'arch. sauf qu'au moins une ride montre une courbure élevée et il y a une boucle et un delta.

- Une empreinte digitale de **loop** a une ou plusieurs rides qui entrent d'un côté, courbent en arrière, et sortent le même côté d'où elles sont entrées. Une boucle et un delta sont présents. Des loops peuvent être encore subdivisées: les loops qui ont des rides qui entrent et sortent du côté gauche s'appellent le lelt loop et les loops qui ont des rides qui entrent et sortent du côté droite s'appellent le right loop.

- Une empreinte digitale de **whorl** contient au moins une ride qui fait un chemin 360-dégrée complet autour du centre de l'empreinte digitale. Deux boucles et deux deltas peuvent être trouvés dans des empreintes digitales de whorl;
  La figureIII.8.a montre les exemples d'empreintes digitales de chaque classe.

  Dans la littérature les approches de classification sont divisées en 5 catégories [Mal.03]

  - Classification basée sur les règles
  - Classification syntaxique
  - Classification structurelle
  - Classification statistique
  - Classification par réseau de neurones

  Les détails techniques de ces approches sont présentés dans [Mal.03]

III.2.1.7 Capture de l'image d'une empreinte digitale :(figure III.19)

Obtenir des images numériques d'empreintes digitales n'est pas une chose simple, car la surface à capturer est de faible dimension par rapport au contenu des informations. De plus, certaines ethnies ont de très fines empreintes digitales par rapport à d'autres populations (la population asiatique par exemple), de même que pour les enfants. Il est donc important de faire le bon choix de capteur par rapport à la population d'utilisateurs.

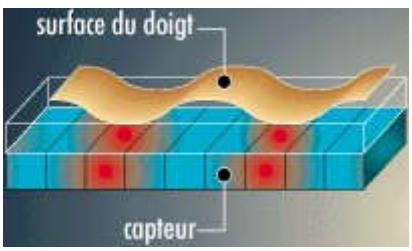


Figure III.19 coupe d'un doigt sur un capteur

La capture de l'image d'une empreinte digitale consiste à trouver les lignes tracées par les crêtes (en contact avec le capteur) et les vallées (creux).

Le point commun à toutes les technologies utilisées pour la prise d'image d'une empreinte, est que l'image est constituée à partir des points de contact du doigt sur le capteur.

Les familles de capteurs

Les techniques utilisées pour la mesure sont diverses : capteurs optiques (caméras CCD/CMOS), capteurs ultrasoniques, capteurs de champ électrique, de capacité, de température...
Ces capteurs sont souvent doublés d'une mesure visant à établir la validité de l'échantillon soumis (autrement dit, le doigt) : mesure de la constante diélectrique relative de l'échantillon, sa conductivité, les battements de coeur, la pression sanguine, voire une mesure de l'empreinte sous l'épiderme...

a) Capteur optique

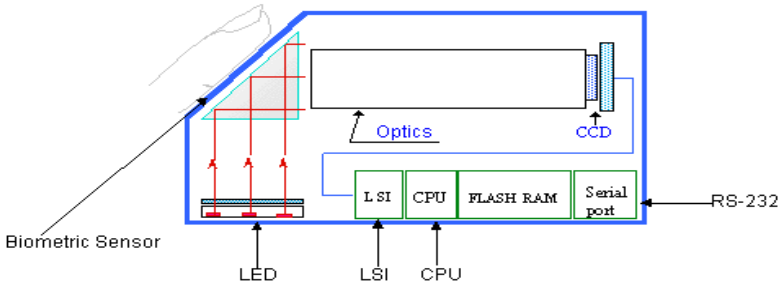


Figure III.20 Capteur optique

Il s'assimile à une mini caméra. Le doigt est apposé sur une platine en plastique dur ou en quartz, qui est en vis-à-vis de la mini caméra. Il résiste très bien aux fluctuations de température, mais est gêné par une lumière ambiante trop forte.

De plus il est assez volumineux. Son coût est intéressant, et il est intrinsèquement protégé contre les décharges électrostatiques. Il permet d'avoir des images précises et nettes.

Ce procédé de capture d'image est le plus ancien après l'encre. Il est fréquemment utilisé particulièrement dans les applications judiciaires pour la qualité des images. Le principe physique utilisé est "la réflexion totale frustrée".

Avantages	Inconvénients
• Son ancienneté et sa mise à l'épreuve. • Sa résistance aux changements de température, jusqu'à un certain point. • Son cout abordable. • Sa capacité à fournir des résolutions de plus de 500 dpi.	• Il est possible que l'empreinte d'utilisateurs précédents reste latente, d'où une possibilité de dégradation de l'image par surimpression. • Apparition possible de rayures sur la fenêtre. • D'autre part, le dispositif CCD peut s'user avec le temps et devenir moins fiable. • Problèmes de contrastes (doigt propre et sec devient trop clair tandis qu'un doigt humide et recouvert d'un film gras devient très foncé), problème résolu grâce au film liquide mais système mal accepté. (mouille le doigt !)

Tableau III.2 Avantages et inconvénients du capteur optique

b) **apteur en silicium**

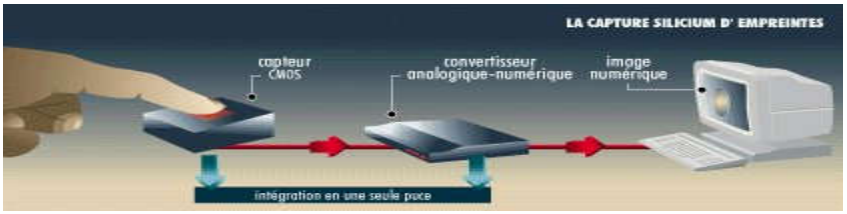


Figure III.21 Capteur en silicium

Il utilise l'un de quatre effets observables sur les semi-conducteurs : l'effet piézo-électrique, l'effet capacitif, l'effet thermo-électrique et l'effet photo-électrique.

Il est en général de très petite taille, d'une durée de vie assez longue, et son coût est très intéressant.

Mais, comme tout composant, il est fragile aux décharges électrostatiques et il peut-être détruit si des règles de fabrication et d'installation ne sont pas observées.

Ces nouvelles technologies visent surtout les applications de masses, grâce à une taille réduite et des coûts moins importants que les lecteurs optiques.

Avantages	Inconvénients
• Cout assez bas.	• Capteur vulnérable aux attaques extérieures fortuites ou volontaires.

Tableau III.3 Avantages et inconvénients du capteur en silicium

c) Capteur thermique

La technique de capture thermique est utilisée par le FingerChip d'Atmel. Le capteur mesure une différence de température obtenue selon que la peau touche (dans le cas d'une crête de l'empreinte) ou ne touche pas (pour une vallée) le capteur.

Le FingerChip est constitué d'une puce en silicium recouverte d'une couche de matériau pyro-électrique, c'est-à-dire sensible aux différences de température. La puce est elle-même formée d'une matrice de pixels adjacents. La différence de température, initialement apparue au contact du matériau pyro-électrique, est transformée de par les propriétés de ce matériau en charges électriques. Celles-ci sont alors amplifiées et mesurées par les pixels en silicium de manière à former une image en noir et blanc. C'est une traduction fidèle de l'empreinte de l'utilisateur.

Cette technologie thermique présente de nombreux avantages. En particulier, elle permet d'obtenir une image de très grande qualité avec des empreintes « difficiles », par exemple quand les crêtes et les vallées sont très peu marquées.

d) Capteur ultra sonique

Il utilise une onde ultra sonore qu'il envoie vers le doigt, puis calcule le temps mis par l'onde pour faire un aller-retour et, point par point, fournit l'image de l'empreinte

Il est très précis, et hérite des propriétés des ultrasons de traverser certains matériaux (gants en latex, saletés, etc.). Mais il est volumineux et très coûteux. Il est intéressant pour une population d'utilisateurs très hétérogène.

Avantages	Inconvénients
• Facilité d'usage avec de grandes plaques • Capacité à surmonter des conditions de lecteurs non optimales (les poussières sont souvent transparentes aux ultrasons)	• Aucun inconvénient technique significatif n'a pu être identifié à ce jour au travers des textes et des témoignages des experts. • Cout élevé.

Tableau III.4 Avantages et inconvénients du capteur ultra sonique

III.2.1.8 Etapes de traitement de l'empreinte digitale

Plusieurs méthodes sont employées pour reconnaître les empreintes digitales : localisation des minuties, analyse spectrale à l'aide d'ondelettes, traitement de textures, etc.

****Localisation des minuties**

cette méthode ne retient que l'emplacement des minuties les plus pertinentes. Elle est peu sensible aux déformations des doigts entre plusieurs vérifications (doigts plus ou moins appuyés sur le capteur).

****Traitement de textures**

des paramètres issus de certaines propriétés de la texture des empreintes (orientation, fréquence, etc.) sont comparés. Cette méthode permet un traitement très rapide, et donc un temps de réponse très court.

Il existe bien d'autres méthodes, mais elles ne sont pas divulguées par les entreprises qui les développent pour un souci de propriétés intellectuelles.

****Stockage de l'empreinte sous le format approprié.**

Le format BITMAP de Windows peut être utilisé comme format d'entrée des images à traiter ainsi que pour échanger des images avec les applications. L'origine des images n'a pas d'importance (scanner, fichier, caméra, code barre...).

****Filtrage des images (Segmentation).**

Le but de cette étape est de supprimer toute ambiguïté en détectant des zones de bruit et en faisant ressortir la plus grande partie possible d'information utile au système.
Cette fonction se charge également de détecter l'absence d'empreinte, un niveau élevé de bruit dans l'image (image sale ou lecteur défectueux), un positionnement incorrect du doigt.

****Evaluation de la qualité de l'empreinte capturée.**

Le système calcule un facteur de qualité qui permet d'établir un critère automatique de fiabilité du *"gabarit"* de l'empreinte qui sera ensuite calculée.

****Squelettisation de l'empreinte.**

Dans l'image binarisée (noir et blanc), les lignes se voient clairement mais elles ont des tailles différentes. Pour pouvoir détecter rapidement les minuties (terminaisons, bifurcations), il est nécessaire d'obtenir une image plus schématique de l'empreinte, dans laquelle toutes les lignes ont la même épaisseur (1 pixel).

****Extraction des minuties.**

C'est le processus final qui complète l'obtention de la *"signature"* de l'empreinte. A partir d'une image de l'empreinte préalablement traitée, on extrait grâce à différents algorithmes une structure de données (ou signature).

Le "gabarit" retenu pour caractériser l'empreinte, est basé sur un ensemble suffisant et fiable de minuties.

On entend par suffisant, le nombre minimum de minuties nécessaire pour pouvoir établir des comparaisons fiables entre empreintes. Par expérience, ce minimum se situe à 14 minuties.

On entend par fiable, les minuties qui ne sont pas influencées par des défauts lors de l'acquisition de l'image ou par l'altération temporaire de l'empreinte digitale (blessure, érosion, etc.). Avec un petit nombre de minuties (15 ou 20) correctement localisées, il est possible d'identifier une empreinte parmi plusieurs millions d'exemplaires.

Généralement, chaque minutie occupe environ un espace de 16 octets sans compactage ni compression. Ceci explique la taille de chaque fichier *"gabarit"*, 240 octets pour 15 minuties et 1600 octets pour 100 minuties. Si le stockage final est compacté, on peut économiser de l'espace mémoire et si on le comprime, on peut obtenir les pourcentages classiques en compression de fichiers.

Lors du processus d'extraction, on détecte initialement 100 minuties en moyenne, parmi lesquelles environ 60 % correspondent à de fausses minuties qui seront identifiées lors d'un processus ultérieur. Le logiciel extrait donc une quarantaine de minuties réelles de l'empreinte. Cette valeur est nettement supérieure aux minima, ce qui augmente la fiabilité. De plus, ce chiffre est loin du total de minuties détectées, ce qui laisse supposer que n'ayant conservé que les plus fiables, on a éliminé les minuties erronées qui auraient pu détériorer le comportement du système.

III.2.1.9 Etapes de comparaison d'empreintes digitales

Le système de vérification d'identité est basé sur la comparaison de deux ensembles de minuties (fichier "gabarit"), correspondants respectivement à deux doigts à comparer.

Pour déterminer si deux ensembles de minuties extraits de deux images correspondent à des empreintes du même doigt, il est nécessaire d'adopter un système de comparaison qui soit insensible à d'éventuelles translations, rotations et déformations qui affectent systématiquement les empreintes digitales.

A partir de deux ensembles de minuties extraites, le système est capable de donner un indice de similitude ou de correspondance qui vaut :

- 0 % si les empreintes sont totalement différentes.
- 100 % si les empreintes viennent de la même image.

Deux fichiers " *gabarit* " calculés à partir de la même empreinte ne donneront jamais 100 % de ressemblance du fait des différences qui existent lors de l'acquisition de deux images (petites déformations ou déplacements), ils donneront cependant toujours un niveau élevé de similitude.

La décision à partir de cet indice de similitude de savoir si deux empreintes sont issues du même doigt est une question purement statistique. Pour décider d'accepter la similitude entre deux *" gabarit "*, il faut établir un seuil d'acceptation.

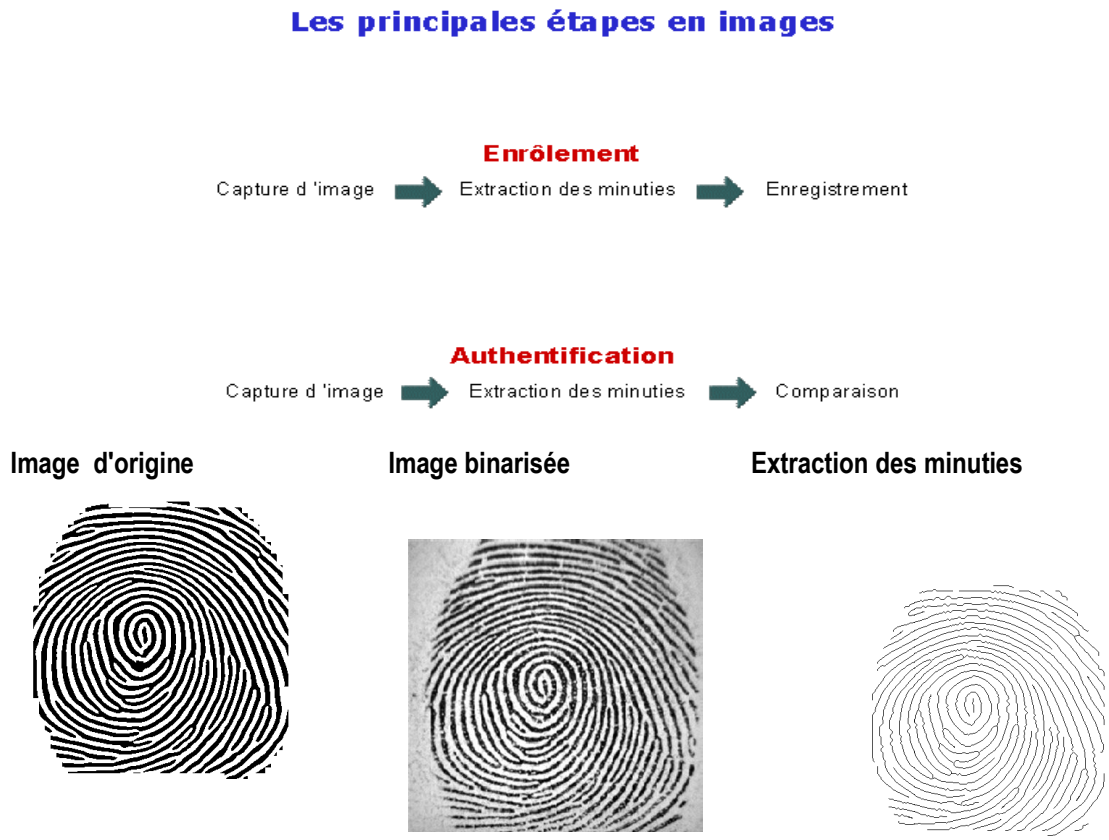


Figure III.22 les principales étapes en images

III.3 Conclusion:

Nous avons abordé en détail les deux signatures biométriques que nous jugeons efficaces compte tenu des nombreux avantages énumérés auparavant.

En effet, l'empreinte digitale et l'iris offrent des facilités d'utilisation appréciables, elles sont peu couteuses et leur traitement est rapide. Leur association est utilisée notamment dans les zones de haute sécurité.

Le chapitre V montrera la fusion de ces deux modalités et permettra de mettre en exergue tous les bienfaits de cette bimodalité.

CHAPITRE IV :

LES SYSTEMES IMMUNITAIRES

Les Systèmes Immunitaires

Partie 1 : Système Immunitaire Naturel

IV.1.1 Introduction

Le système immunitaire d'un organisme est un ensemble coordonné d'éléments qui permet de discriminer le « soi » du « non-soi ». Il agit comme un mécanisme de défense contre les pathogènes, tels que les virus, les bactéries, les parasites, les cellules cancéreuses, certaines particules ou molécules « étrangères » (dont certains poisons).Il est responsable aussi du phénomène de rejet de greffe.

On dénombre plusieurs variantes de systèmes immunitaires parmi les espèces animales, et parfois un même organisme peut accueillir plusieurs systèmes immunitaires (le cerveau humain, par exemple, possède son propre système immunitaire, distinct de celui du reste du corps). De nombreuses espèces, dont les mammifères, utilisent la variante démontrée dans la Figure IV.1 :

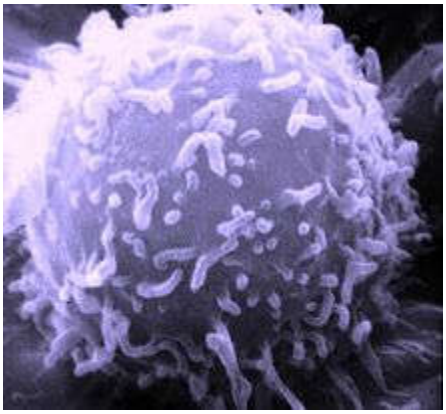


Figure IV.1 Un lymphocyte, principale composante du système immunitaire humain

Les principaux agents du système immunitaire sont les cellules immunitaires appelées leucocytes (ou globules blancs) produites par des cellules souches, au sein de la moelle osseuse.

Il existe deux types de mécanismes de défense :

1. Les mécanismes de défense non-spécifique ou innée ou naturelle, comme la protection de la peau et les muqueuses, l'acidité gastrique, les cellules phagocytaires ou les larmes.
2. Les mécanismes de défense spécifique, comme l'action dirigée des lymphocytes et la production d'anticorps spécifiques.

IV.1.2 Généralités

On appelle réponse immunitaire l'activation des mécanismes du système immunitaire face à une agression de l'organisme. L'immunologie est la science qui étudie les mécanismes biologiques, physiologiques et physico-chimiques permettant à l'organisme de reconnaître les agents infectieux, comme des corps étrangers et ainsi de se protéger contre leurs effets nocifs, ces systèmes de défense efficaces, parfois complexes dont les organismes supérieurs ont su se doter au cours de l'évolution contre les corps étrangers [Gom04].

Le système immunitaire est divisé en deux systèmes de défenses principaux : le système immunitaire inné (défense présentée dés la naissance de l'individu), et le système immunitaire adaptatif (ensemble des défenses apprises ou acquises au cours du temps) [ROI.90].

Les cellules qui forment le système immunitaire sont appelées leucocytes. La hiérarchie de cette famille est montrée dans la figure IV.2 :

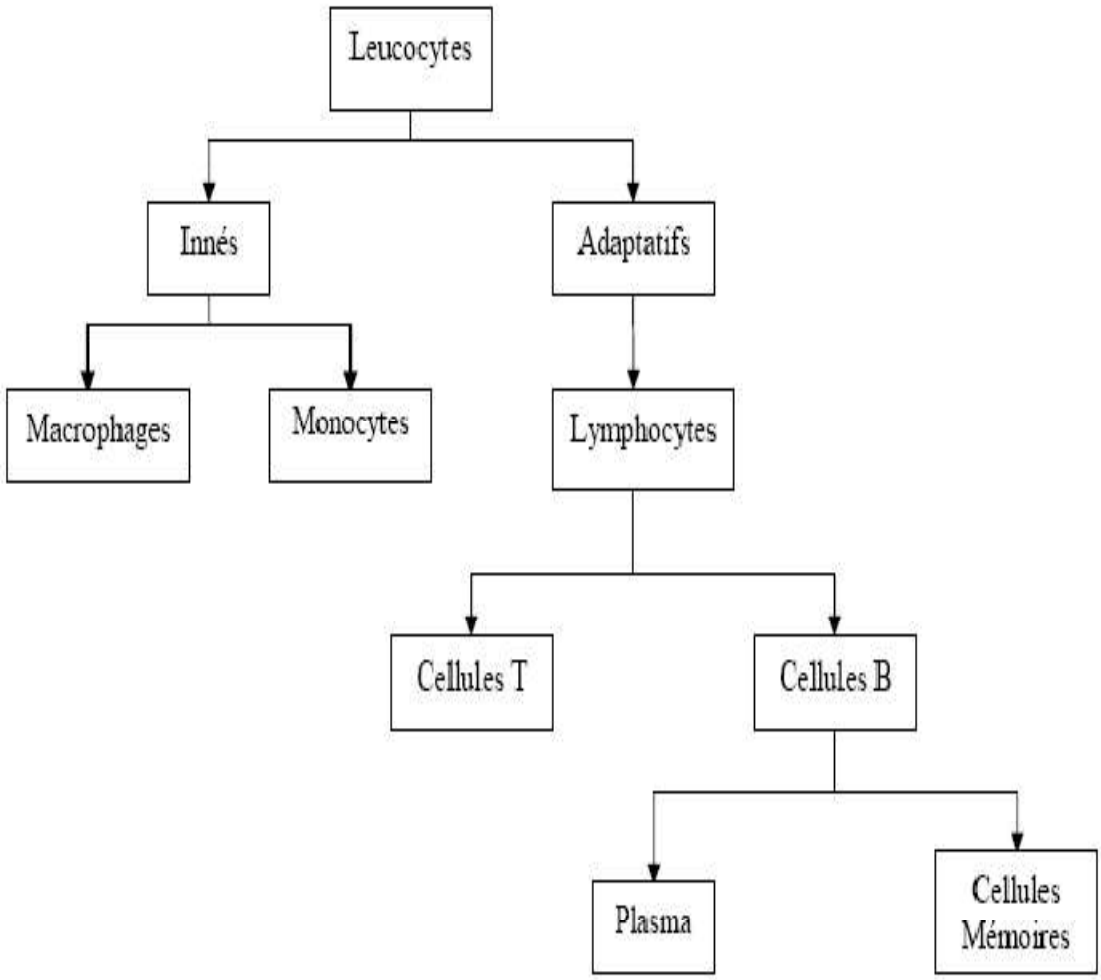


Figure IV.2 Hiérarchie des cellules immunitaires

La réponse immunitaire innée est rarement intéressé par les informaticiens, à cause de ses capacités statiques, réagissant à l'infection sans pour autant apprendre à y réponde de manière plus efficace. Par contre, la réponse immunitaire adaptative est d'un grand intérêt dans le domaine informatique. Principalement grâce à ses capacités d'apprentissage adaptatif et de mémorisation.

IV.1.3 Système inné - système acquis

Une fois les défenses externes pénétrées (peau, poil), les microbes (antigènes) entrent en contact avec les cellules et les produits du système immunitaire qui réagissent face à cette intrusion. Plusieurs types de cellules et de molécules de défense sont présents sur le lieu de l'invasion ou migrent de leur site vers le lieu d'infection. Ils constituent la première ligne de défense qui est appelée système immunitaire inné du fait qu'il est présent dés la naissance et évolue au cours de la vie de l'individu par interaction avec l'environnement, inclut des éléments tels que la peau et les muqueuses. Il utilise différents mécanismes tels que la toux, l'éternuement, les larmes ainsi que la salive pour éliminer les agents nocifs. Les cellules et les molécules de ce système inné sont

principalement responsables des premières phases de l'expulsion du microbe et peuvent augmenter l'inflammation. Les cellules impliquées dans la réponse innée sont appelées phagocytes et incluent dans leurs rangs les monocytes et les macrophages [LYD02].

Ces cellules présentent à leurs surfaces des récepteurs qui sont programmés pour reconnaître une forme antigénique. Ces récepteurs sont produis seulement après l'introduction de cet antigène dans le corps
[ROI90].

Les phagocytes se lient aux agents infectieux pour les ingérer. Une fois digéré, l'antigène est découpé en plusieurs morceaux qui sont présentés par les macrophages comme un signal de présence de l'agent infectieux. Les cellules qui effectuent cette tâche de signalisation sont appelées cellules présentatrices d'antigènes. Ce signal peut être utilisé pour stimuler d'autres phagocytes et/ou la réponse immunitaire adaptative.

La seconde ligne de défense constitue le système immunitaire acquis. Celui-ci est appelé à agir lorsque le système immunitaire inné agit avec le microbe et spécialement s'il est incapable de supprimer le microbe envahisseur. La différence majeure qui existe entre les deux systèmes est que le système acquis montre une spécificité considérable et se rappelle qu'un microbe particulier a précédemment envahie le corps, ce qui permet une expulsion rapide du microbe la deuxième fois ou la troisième fois qu'il entre. Les cellules impliquées dans la réponse immunitaire adaptative sont appelés lymphocytes, et peuvent être divisées

En deux catégories : les cellules B et les cellules T. les cellules B se développent dans la moelle et les cellules T dans le Thymus [LYD02].

Les cellules, les molécules et les caractéristiques des systèmes innés et acquis sont montrées dans le tableau IV.1 :

	Caractéristiques	**Cellules**	**Molécules**
Immunité naturelle	Répond rapidement	Phagocytes (PN et macrophages	Cytokines Complément
	Possède une certaine spécifié	Mastocytes, cellules dendritiques	Protéines de la phase aigue
	Pas de mémoire	Cellules Natural Killer	
Immunité acquise	Lente au départ		Anticorps Cytokines
	Hautement spécifique		
	mémoire	Cellules T et B	

Tableau IV.1 Les systèmes immunitaires inné et acquis

L'immunité spécifique contient deux mécanismes principaux, l'un est responsable de la distinction entre le soi et le non soi, l'autre permet au système de mémoriser les antigènes rencontrés.

IV.1.4 Cellules du système immunitaire

IV.1.4.1 Cellules du système immunitaire inné

- **Macrophages :**

Grandes cellules phagocytaires mononuclées résidant dans la plupart des tissus. Dérivées des monocytes sanguins, elles contribuent à l'Immunité innée et interviennent dans les phases non adaptatives précoces de défense de l'hôte. Elles fonctionnent comme cellules présentatrices d'antigènes professionnelles et comme cellules effectrices de l'Immunité humorale et cellulaire.

- **Monocytes :**

Globules blancs ayant un noyau en forme de fève. Ils sont des précurseurs de macrophages.

- **Phagocytes**

Cellules spécialisées dans la fonction phagocytaire.les phagocytes principaux chez les mammifères sont les neutrophiles et les macrophages.

- **Basophiles**

Rares globules blancs du sang constituant un des trois types de granulocytes.ils contiennent des granules qui se colorent par des colorants basiques.

- **Mastocytes**

Grandes cellules dérivées de la moelle osseuse et situées dans le tissu conjonctif partout dans l'organisme. Elles contiennent de gros granules dans lesquels sont stockés divers médiateurs chimiques dont l'histamine. Elles jouent un rôle crucial dans les réactions allergiques.

- **Cellules Natural killer (NK)**

Grands lymphocytes cytotoxiques granuleux qui circulent dans le sang. Les cellules NK sont importantes dans l'Immunité innée contre les virus et d'autres agents pathogènes intracellulaires ; elles tuent aussi certaines cellules tumorales. Elles interviennent dans les réactions de cytotoxicité à médiation cellulaire dépendante des anticorps(ADCC).

- **Cellules dendritiques**

Les cellules dendritiques sont appelées ainsi car elles contiennent plusieurs plis se trouvant sur la surface de la membrane, similaire en apparence aux dendrites du système nerveux. Ces plis permettent une interaction maximale avec d'autres cellules du système Immunitaire.

Il existe trois principaux types de cellules dendritiques (voir tableau IV.2).

Types de cellules dendritiques	Localisation
Cellules de Langerhans (LH)	peau
Cellules interdigitées (CDI)	Zone de la cellule T du ganglion
Cellules dendritiques folliculaires (FCD)	Follicule des cellules B des tissus lymphoïdes

Tableau IV.2 Cellules dendritiques

IV.1.4.2 Cellules du système immunitaire adaptatif

- **Lymphocytes**

Les lymphocytes fournissent la caractéristique de la mémoire de cette réponse immunitaire acquise. Les deux types de lymphocytes qui contribuent à la réponse acquise sont les cellules T et les cellules B lesquelles ont une morphologie similaire figure IV.3. Elles possèdent des récepteurs d'antigènes spécifiques mais différents et d'autres molécules de surface nécessaires pour l'interaction avec d'autres cellules. Les cellules B maturité donnent les plasmocytes qui produisent et sécrètent les anticorps.

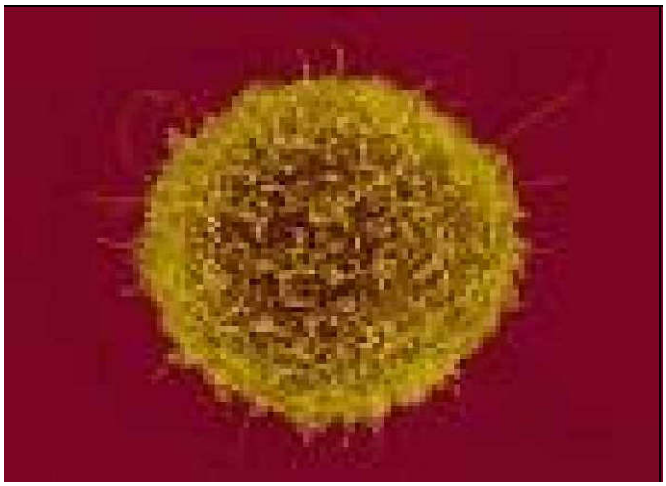


Figure IV.3 Lymphocyte sanguin

- **Les lymphocytes T**

Les cellules T fonctionnent dans les organes et tissus lymphoïdes secondaires du corps pour contrôler les microbes intracellulaires et fournir une aide aux réponses des cellules B (anticorps).

Deux différents types de ces cellules T participent à ces fonctions :

- Les cellules T helper (Th) aident à la croissance et à la différenciation de la cellule B.
- Les cellules T cytotoxiques (Tc) reconnaissent les antigènes viraux présents sur la surface des cellules et procèdent à l'élimination de ces dernières.

- **Les lymphocytes B**

Les cellules B sont produites dans la moelle osseuse et tout comme les cellules T, elles migrent vers les tissus lymphoïdes secondaires où elles répondent aux antigènes étrangers. Les anticorps qui se trouvent sur leur surface sont leurs récepteurs d'antigènes. Lorsqu'elles sont activées par l'antigène la plupart du temps avec l'aide de la cellule T, elles prolifèrent et atteignent la maturité formant des cellules à mémoire, qui restent capables de répondre à l'antigène si celui-ci est réintroduit et en plasmocytes (des usines produisant et secrétant de grandes quantités d'anticorps de même spécifié que celle du récepteur de l'antigène se trouvant sur la cellule B parente).

IV.1.5 Cellules T et B et coopération cellulaire

Les lymphocytes qui subissent une expansion clonale sont de deux types majeurs : cellules T et B. La maturation des lymphocytes T et sous la dépendance du thymus et lorsqu'elles sont simulées par un antigène elles augmentent l'immunité cellulaire. La maturation des lymphocytes B est sous l'influence de la moelle osseuse et/ou des tissus associés aux formations intestinales et augmente les populations lymphoïdes qui, au contact avec un antigène, prolifèrent, et se différencient en plasmocytes. Ces plasmocytes produisent un facteur humoral (anticorps = immunoglobuline) qui est spécifique pour l'antigène et est capable de le neutraliser et/ou de l'éliminer. Le développement de la réponse immunitaire à un antigène, nécessite également la coopération cellulaire. Les populations cellulaires T et B ainsi que les macrophages, interagissent dans le développement d'une immunité spécifique. En particulier, les sous-populations de cellules T régulent les réponses immunes cellulaire et humorale. Bien que les réponses immunes à la majorité des antigènes (particulièrement les protéines) requièrent une coopération cellulaire, certains antigènes (T indépendant) peuvent lancer une réponse immune en l'absence de lymphocyte T [LYD02].

IV.1.6 Distinction entre le soi et le non soi

De tous les mécanismes qui constituent le système immunitaire naturel, celui-ci est le plus important. A tout moment le système doit être capable d'identifier ses propres molécules (le soi) des molécules étrangères. Les cellules T sont à la base de la distinction entre le soi et le non soi. Non seulement elles peuvent se lier comme elles peuvent détruire les cellules du soi infectées.

En plus, elles sont indispensables à l'activation des cellules B et donc au lancement de la réponse immunitaire. En effet, même si une cellule B reconnaît un antigène, elle ne peut s'activer que si elle reçoit une confirmation des cellules T.

Lors de la maturation des cellules T dans le thymus, elles sont confrontées à un échantillon de molécules du soi. N'importe quelle cellule T qui s'active en présence de cet échantillon est immédiatement détruite. Ceci garantit que les cellules T matures ne vont jamais se lier avec des molécules du soi. Ceci veut dire aussi que si une cellule T se lie à une certaine molécule, cette dernière est forcément une molécule non soi [DEN06].

IV.1.7 Réactions Immunitaires

La reconnaissance par les cellules immunitaires d'antigènes du "non soi" déclenche des réactions immunitaires que l'on classe en deux catégories:

- Les réactions non spécifiques lorsqu'elles sont indépendantes des antigènes.

- Les réactions spécifiques, elles sont généralement déclenchées par un antigène spécifique [REV01].

IV.1.7.1 La Réponse Immunitaire non spécifique (innée)

La réponse immunitaire non spécifique a lieu dans les tissus sur les sites d'infections et s'accompagne le plus souvent d'une réaction inflammatoire. Exemple: la phagocytose.

IV.1.7.2 La Réponse Immunitaire spécifique (adaptative)

Elle est due à un antigène spécifique qui provoque la production par l'organisme d'anticorps spécifiques. Elle comporte trois étapes principales et nécessite une coopération entre les cellules immunitaires

IV.1.8 Antigène

IV.1.8.1 La diversité des antigènes

La première phase de destruction d'un germe invasif est de le reconnaître comme étant un organisme étranger c'est-à-dire un non-soi. Le système immunitaire considère l'envahisseur comme possédant un nombre d'antigènes. Un antigène est une substance qui provoque une réponse immunitaire sous forme de prolifération de lymphocytes et production d'anticorps spécifiques pour l'antigène introduit. Celui-ci contient habituellement des protéines, des glucides, des lipides et des acides nucléiques. Des réponses peuvent être produites virtuellement à tout ce qui est introduit dans une forme appropriée [LYD02].

IV.1.8.2 La structure d'un antigène

Sur le plan structural, un antigène doit être suffisamment unique pour le système immunitaire pour qu'il se produise une réponse immune. Il est habituel qu'un antigène, une molécule qui est antigénique possède plusieurs structures moléculaires différentes uniques, dont chacune peut produire une réponse immune. Ainsi, les anticorps ou les cellules produites contre un antigène ne sont pas dirigés contre toute la molécule mais contre différentes parties de la molécule. Ces déterminants antigéniques ou épitopes figure IV.4 sont les plus petites unités d'un antigène auxquelles un anticorps ou une cellule peut se lier.

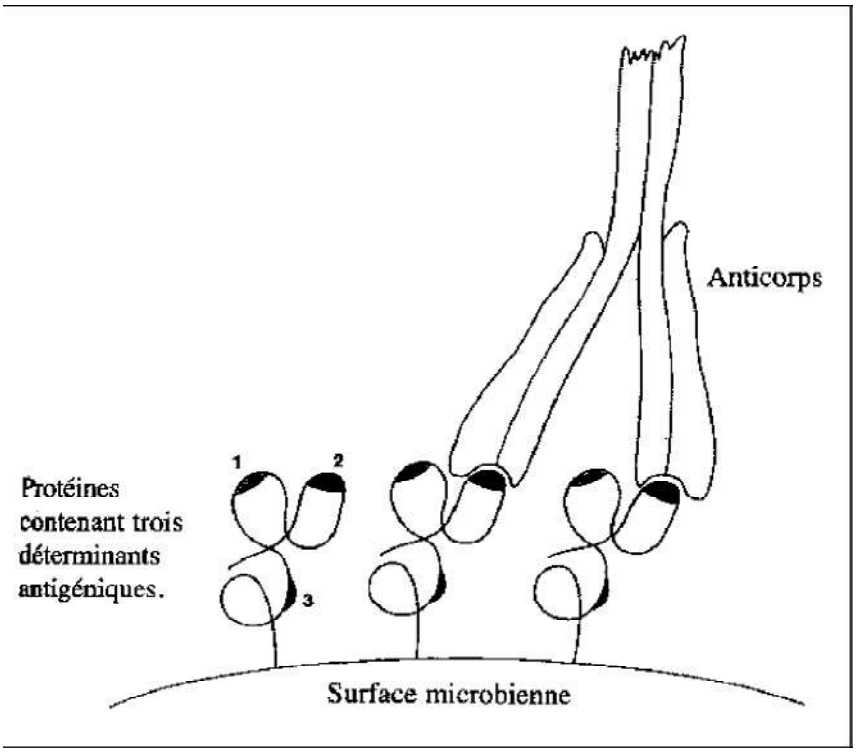


Figure IV.4 Déterminants antigéniques (épitope) reconnus par les anticorps

IV.1.9 Les anticorps « Structure de base »

IV.1.9.1 Constituants moléculaires

Les anticorps souvent appelés immunoglobulines, sont des glycoprotéines qui se fixent aux antigènes avec une grande affinité et une grande spécifié. Chez l'homme, il existe cinq classes d'antigènes physiquement et chimiquement distinctes (IgG, IgA, IgM, IgD, IgE) [PET80].

IV.1.9.2 Unités des anticorps

Les anticorps possèdent une unité de base constituée de quatre chaînes polypeptidiques (deux paires identiques de chaînes légères (L) et lourdes (H)) reliées par des ponts disulfures covalents et des liaisons non covalentes figure VI.5. Le clivage protéolytique de ces molécules donne deux fragments Fab (la partie de la molécule liant l'antigène) et un fragment Fc (la partie de la molécule responsable des fonctions effectrices comme l'activation du complément). Les chaînes L et H sont divisées en régions V et C (la région V contient le site de liaison de l'antigène et la région C détermine le sort de l'antigène) [LYD02].

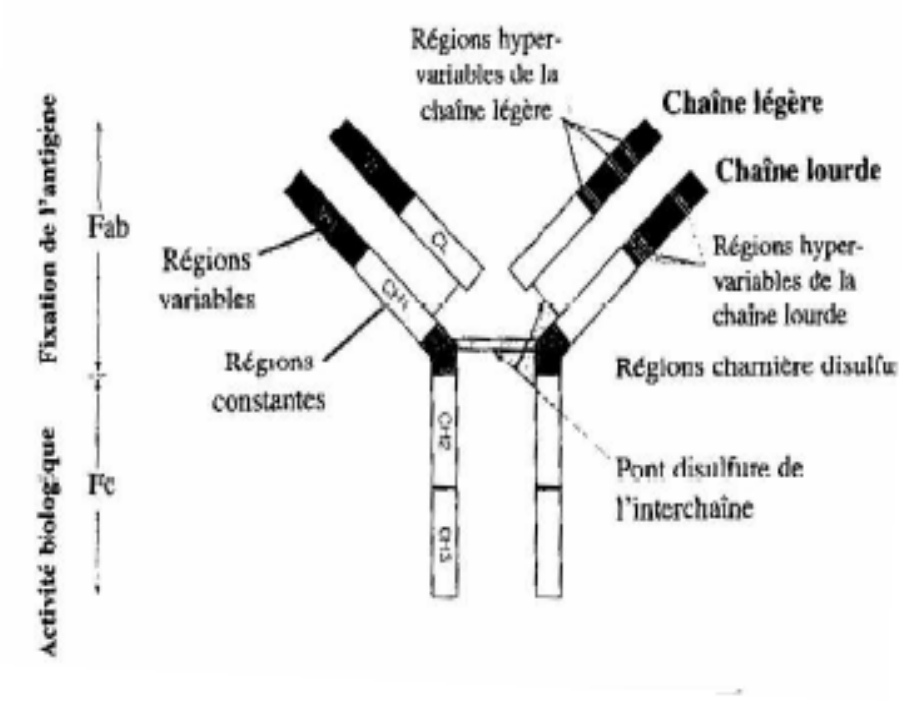


Figure IV.5 Structure de base à 4 chaînes de toutes les immunoglobulines.

IV.1.10 La réponse en anticorps

Il existe trois types de réponses immunitaires :

- La réponse inflammatoire aigue.
- La réponse en cellules T.
- La réponse en anticorps.

  - Nous nous intéressons au troisième type de la réponse immunitaire, dont les anticorps participent à la réponse immunitaire naturelle, et le principe d'immunité artificielle est inspiré de ce type de réponse.

IV.1.10.1 Sélection et activation des cellules B

Après pénétration dans l'organisme, un antigène se lie spécifiquement aux cellules B possédant les récepteurs pour cet antigène. Grâce aux cellules T helper, ces cellules B vont subir une expansion clonale, et certaines d'entre elles vont se différencier en plasmocytes qui synthétiseront l'anticorps spécifique pour l'antigène responsable du déclenchement de la réponse immunitaire [LYD02].

IV.1.10.2 Réponses primaire et mémoire

A la première exposition à un antigène, on assiste au développement d'une réponse
Immunitaire dite primaire donnant lieu à la production d'anticorps de type IgM. Cette étape est suivie habituellement par une réponse immunitaire de type IgG dans les 4 à 5 jours qui suivent figure IV.6. Cette réponse limitée s'arrêtera lorsque l'antigène n'est plus disponible pour simuler les cellules B. Lorsque le même antigène est réintroduit, il existe davantage des cellules B mémoire spécifiques à cet antigène qui, après différenciation, vont donner lieu à une réponse plus rapide avec production, habituellement, d'anticorps de type IgG [ROI90].

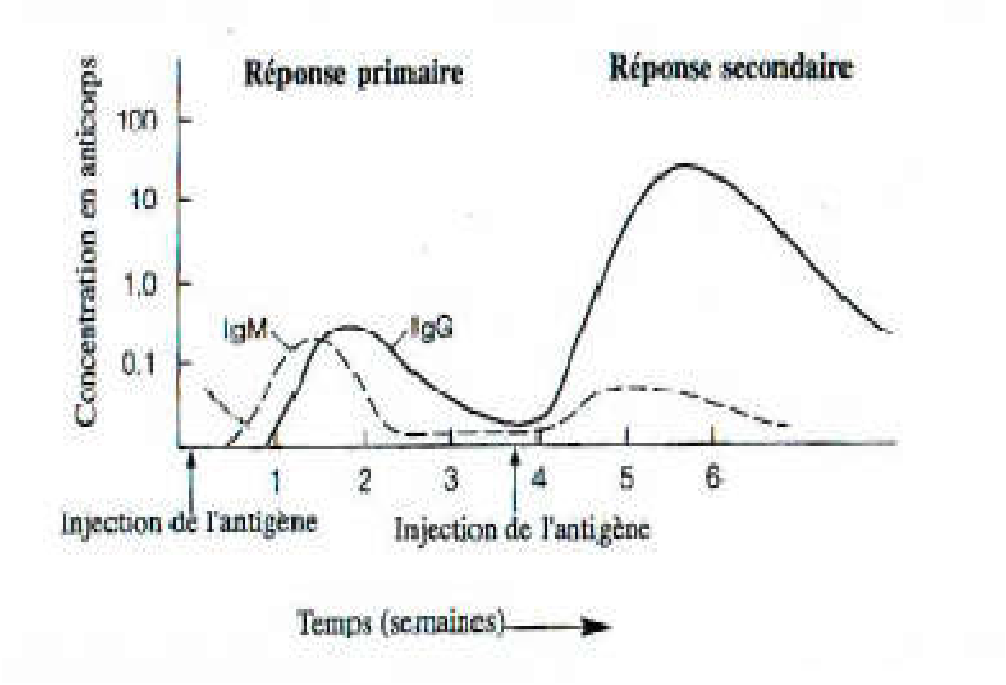


Figure IV.6 Cinétique de la réponse immunitaire

IV.1.10.3 Maturation de l'affinité

L'affinité est la fixation serrée d'un site de liaison d'un anticorps à un déterminant antigénique (autant la fixation est serrée autant l'anticorps reste lié à l'antigène). L'affinité des anticorps à un déterminant antigénique varie considérablement. Les anticorps produits par une réponse mémoire possèdent une plus haute affinité que ceux produits en réponse primitive.

Les anticorps produits au cours de la réponse secondaire [DEN06] ont une plus haute affinité pour l'antigène que ceux produits lors de la réponse primaire en raison :

a) De la restimulation antigénique d'une grande quantité de cellules mémoires ayant des récepteurs à l'antigène de haute affinité et capables de se lier à des quantités limitées d'antigènes.

b) Des mutations ponctuelles au niveau de l'ADN codant pour les régions variables des chaînes H et L de l'anticorps, ce qui conduit à la production d'anticorps ayant une plus grande affinité pour cet antigène.

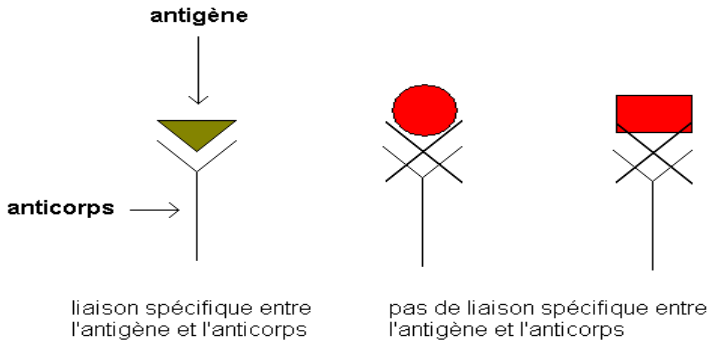


Figure. IV.7 Liaison antigène-anticorps

IV.1.11 Sélection Clonale

- Chaque cellule immunitaire (lymphocyte T ou lymphocyte B) possède à sa surface des récepteurs qui lui permettent de reconnaître un seul antigène.
- les cellules spécifiées préexistant à la première rencontre avec l'antigène correspondant.
- la réponse à l'antigène implique une prolifération de la cellule qui possède les récepteurs correspondants : c'est donc un clone de cellules qui possèdent les mêmes récepteurs qui va répondre (qui va être sélectionné par l'antigène) [CAS02].

- **Mise en œuvre**

Le principe de la Sélection Clonale peut être résumé comme suit (figure IV.7):

- Au départ, la concentration de l'antigène est tellement faible que seule l'Immunité innée est activée. Comme l'antigène est nouveau aucune cellule B n'est assez spécifique pour se lier avec.
- Au fur et à mesure que l'antigène se développe. Sa concentration devient assez élevée pour activer les cellules B les moins spécifiques.
- Une fois les cellules B activées, elles vont se multiplier pour produire un grand nombre de clone. Chaque clone est une cellule B identique à la cellule qui la produite le grand nombre de clones. Le nombre de clone est proportionnel à l'affinité de la liaison cellule B – antigène.
- Pour augmenter la spécificité des Anticorps et l'efficacité de la réponse immunitaire, les clones entrent dans une phase d'hyper mutation, modifiant ainsi la structure de leurs récepteurs (Anticorps). Comme les mutations sont aléatoires, les cellules obtenues (dites matures) peuvent devenir plus spécifiques ou moins spécifiques.
- Lorsque la concentration de l'antigène diminue (à cause de la réponse immunitaire), seules les cellules B les plus spécifiques continuent à être activées, les autres (les moins spécifiques) ne sont plus activées et finissent par mourir. Ceci a pour effet de rendre la population de cellules B de plus en plus spécifique à chaque génération.
- Après maturation, les cellules B deviennent soit des cellules plasma, soit des cellules mémoires. Les cellules plasma sont de véritables usines à Anticorps capables d'en produire en quantité impressionnantes. Les cellules mémoires quand à elles, vont survivre longtemps après la disparition de l'antigène, et peuvent une fois activée produire de grandes quantités d'Anticorps en très peu de temps.

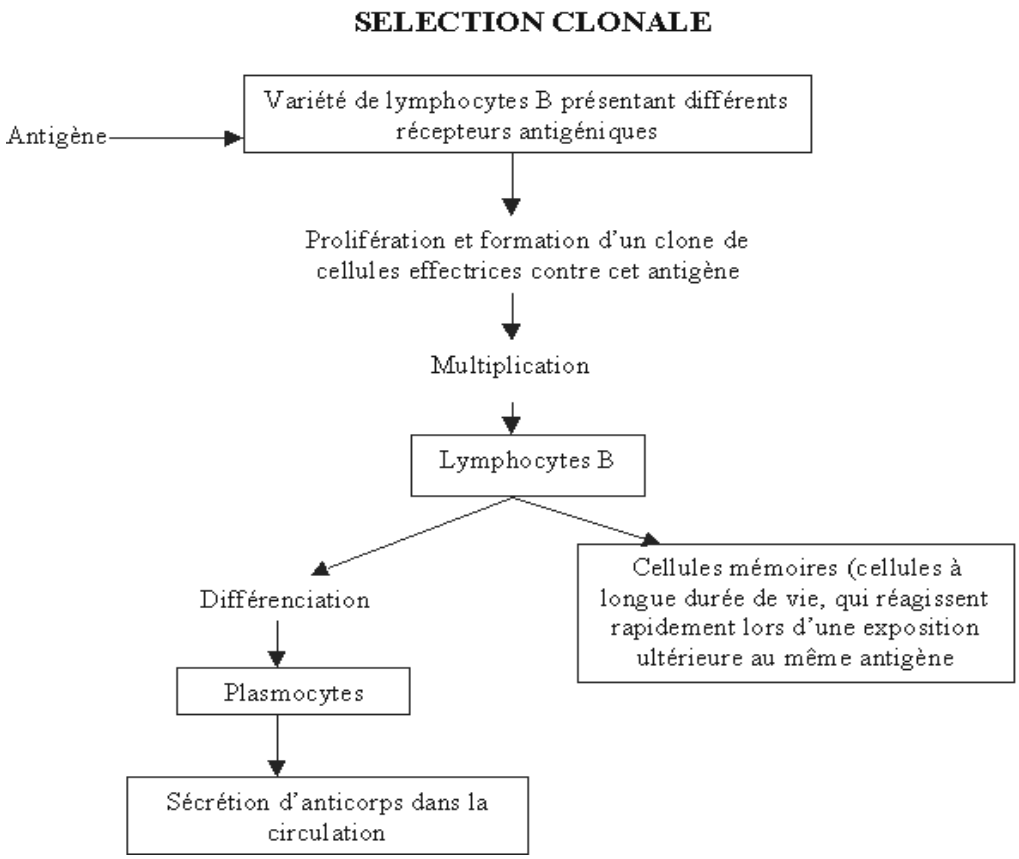


Figure. IV.8 Fonctionnement de la sélection clonale

IV.1.12 Sélection négative

La sélection négative permet la discrimination entre les différentes affinités et ainsi élimine les thymocytes qui réagissent fortement aux interactions entre le complexe majeur d'histocompatibilité (CMH) présentant un peptide du soi. Cette sélection est importante pour développer une tolérance au soi. La médulla est composée de différents types cellulaires dont les plus importants sont les cellules dendritiques et macrophages dérivées de la moelle osseuse [CAS02].

IV.1.13 Les réseaux immunitaires

La théorie des réseaux immunitaires, proposée originellement par N.K.Jerne en 1974, a offert un nouveau point de vue en ce qui concerne l'activité des lymphocytes, la production des anticorps, la tolérance, la distinction entre soi et non soi, la mémorisation ainsi que l'évolution du système immunitaire. Cette théorie suggère que le système immunitaire soit composé d'un réseau régulé de cellules et de molécules qui peuvent se reconnaître les unes des autres même sans la présence d'antigènes [TIM02].

Le système immunitaire a été défini formellement comme un énorme réseau complexe de paratopes qui identifient des ensembles d'épitopes, et des épitopes qui reconnaissent des ensembles de paratopes. Donc chaque cellule peut aussi bien reconnaître qu'être reconnue. Les éléments importants du réseau ne sont pas seulement les molécules, mais aussi les interactions entre ces molécules.

Les cellules immunitaires peuvent répondre positivement ou négativement à un signal de reconnaissance. Une réponse positive induit l'activation de la cellule, sa prolifération et la sécrétion d'anticorps ; alors qu'une réponse négative conduit à la tolérance et à la suppression Figure IV.9.

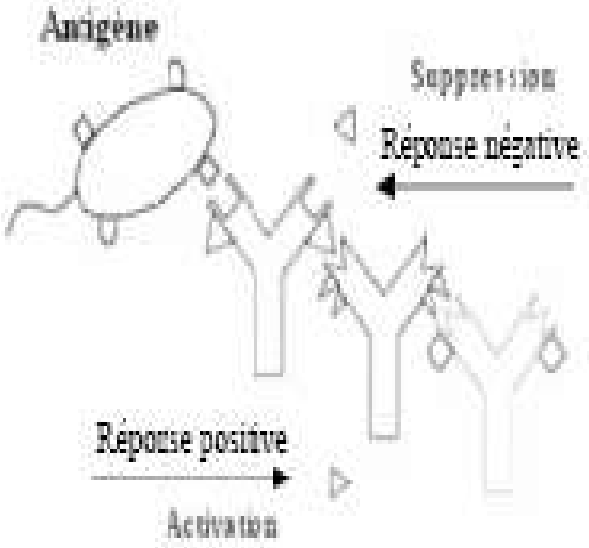


Figure. IV.9 Activation/ Suppression d'un anticorps

La théorie des réseaux immunitaires peut être résumée comme suit figure IV.10 [TIM02].

L'ensemble d'épitopes (Ib) est appelé l'image interne de l'épitope (ou antigène) parce qu'il peut être reconnu par le même ensemble Pa qui a reconnu l'antigène. De plus, chaque épitope de l'ensemble Ia est reconnue par un ensemble de paratopes. Donc, la totalité de l'ensemble Ia est reconnue par un ensemble encore plus large de paratopes Pc associé à un ensemble d'épitopes Ic. Les flèches indiquent une stimulation lorsque les épitopes sont reconnus par les paratopes des récepteurs des cellules, et une suppression lorsque des Paratopes reconnaissent les épitopes des récepteurs des cellules.

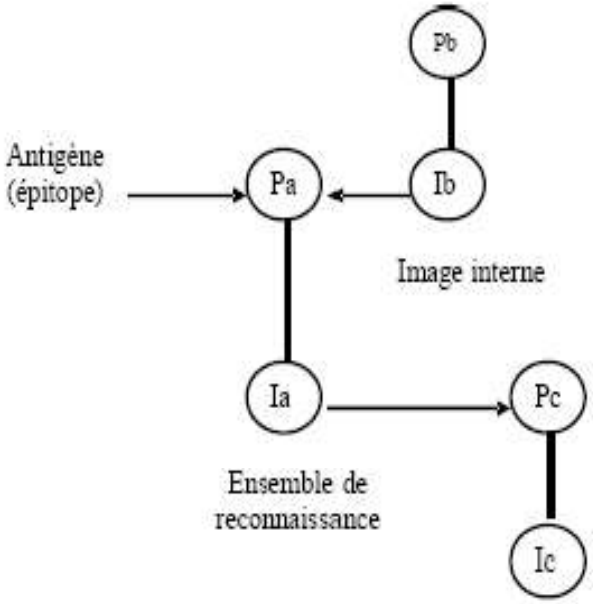


Figure IV.10 Principes des réseaux immunitaires

IV.1.14 Les maladies du système immunitaire

Le système immunitaire peut poser des problèmes soit en excès soit en défaut :
En effet si le système immunitaire s'attaque aux cellules de l'organisme qui ne sont pas pathologiques (par mauvaise reconnaissance), il va alors se créer une maladie auto-immune qui va se caractériser par une inflammation continue de certains tissus ou par la nécrose complète de certains tissus (par exemple, un diabète de type I).
S'il ya un défaut du système immunitaire, dans ce cas les pathogènes ou les cancers pourront se développer plus aisément.

IV.1.15 Le vaccin

C'est une substance préparé à partir de microbes, virus ou parasites pathogènes (tués, inactivés ou atténués) qui, inoculée, confère à l'individu une immunité contre le germe (antigène) correspondant. Lors d'une vaccination le corps apprend à reconnaître un germe et à s'en défendre, de ce fait il est clair qu'il faut introduire de petites quantités d'antigène pour ne pas rendre l'organisme malade.

IV.1.16 Conclusion

Le Système Immunitaire Naturel est un sujet d'un grand intérêt de recherche grâce à ces capacités puissantes. Il utilise des caractéristiques comme la mémoire, et la récupération associative pour résoudre des taches de classification et de reconnaissance.

Il se devise en deux parties : Système Immunitaire inné présent dés la naissance, et le système immunitaire adaptatif, qui montre des propriétés intéressantes dans l'apprentissage du Système Immunitaire Naturel (apprentissage et mémorisation) .Les caractéristiques intéressantes du Système Immunitaire ont encouragé leur adaptation au domaine informatique pour la résolution de problèmes du monde réel.

Partie 2 : Système Immunitaire Artificiel

IV.2.1 Introduction

Un système immunitaire artificiel (SIA) est une catégorie d'algorithmes inspirée par les principes et le fonctionnement du système immunitaire naturel (SIN) des vertébrés. Ces algorithmes exploitent typiquement les caractéristiques du système immunitaire naturel pour ce qui est de l'apprentissage et de la mémorisation comme moyens de résolution de problèmes. Les fonctionnements simulés dans les SIA comprennent la reconnaissance de motifs, l'hypermutation, la sélection clonale pour les cellules B, la sélection négative pour les cellules T, la maturation d'affinité et la théorie des réseaux immunitaires.

IV.2.2 Historique

Les travaux sur les SIA ont commencé dans le milieu des années 1980 avec l'article de Farmer, Packard et Perelson sur les réseaux immunitaires (1986). Cependant c'est seulement dans le milieu des années 1990 que les SIA devinrent un sujet à part entière. Les travaux de Forrest et all Sur la sélection négative commencèrent en 1994, tandis que Dasgupta menait des études sur les algorithmes de sélection négative. Hunt et Cooke commencèrent leurs travaux sur les modèles de réseaux immunitaires en 1995. Timmis et Neal continuèrent ces travaux en y apportant des améliorations.

Le premier livre sur les Systèmes Immunitaires Artificiels a été édité par Dasgupta en 1999. Les travaux de De Castro & Von Zuben et Nicosia & Cutello sur la sélection clonale furent remarqués en 2002.
De nouvelles voies, comme la théorie du danger (observation des dégâts plutôt que celle des agents pathogènes) et des algorithmes inspirés par le système immunitaire inné (SII) ont également été explorées.

Au départ, les travaux sur les SIA visaient à trouver des abstractions efficientes des phénomènes découverts dans le système immunitaire.

IV.2.3 Reconnaissance des formes

On s'appuie sur le schéma classique d'un processus de reconnaissance de formes pour décrire les principaux traitements à effectuer et leurs objectifs.
Buts des étapes du schéma [WIK.] :

- Numérisation : obtenir une représentation des données à traiter qui soit manipulable en machine.
- Prétraitement : élimination des bruits, normalisation, re-échantillonnage, amélioration des contrastes, etc.
- Calcul des représentations : obtenir une représentation des données compatible avec les outils d'apprentissage et de décision utilisés.
- Apprentissage : à partir d'un ensemble d'exemplaires, construire une représentation des classes.
- Analyse : assigner une forme inconnue à une classe.
- Post traitement : valider les décisions de l'analyse sur la base de connaissances (du domaine).

  Dans la pratique, un système de reconnaissance des formes s'éloigne souvent de ce schéma. Des traitements en amont sont souvent nécessaires pour isoler la forme à reconnaître de son contexte, ce qui, en soit, est un problème de reconnaissance (segmentation forme/fond, délimitation d'une forme dans un ensemble). Des traitements ultérieurs sont aussi utiles pour valider les décisions et éventuellement les remettre en cause.

IV.2.4 Différents algorithmes du système immunitaire artificiel

IV.2.4.1 Sélection négative

La Sélection Négative est une abstraction des mécanismes qui permettent au SIN de distinguer entre le soi et le non soi. Elle se concentre sur la génération de détecteur de changement, ces derniers sont censés détecter qu'un élément de chaînes (le soi) a changé.

IV.2.4.1.1 Algorithme de la sélection négative

L'algorithme de la sélection négative, est décrit comme suit : [FOR94]
Au départ nous avons un ensemble de chaînes S qui représentent le soi.

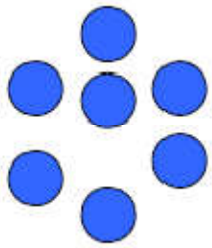


Figure IV.11 chaine de soi

On génère aléatoirement un ensemble de détecteurs RD dans l'espace de travail.

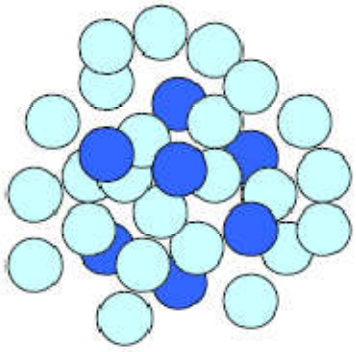


Figure IV.12 chaines soi et détecteurs

Tous les détecteurs de RD qui reconnaissent au moins une chaîne de S, en terme de distance c'est-à-dire le plus proche d'au moins d'une chaîne, sont éliminés.

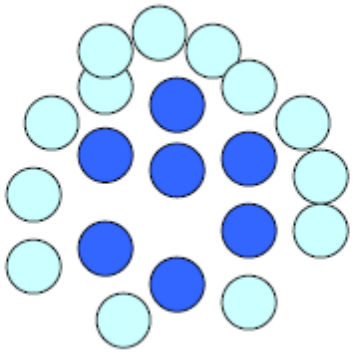


Figure IV.13 Tolérisation

Si une chaîne de S change de forme (mutation), elle à de grandes chances qu'elle soit reconnue par un des détecteurs de RD.

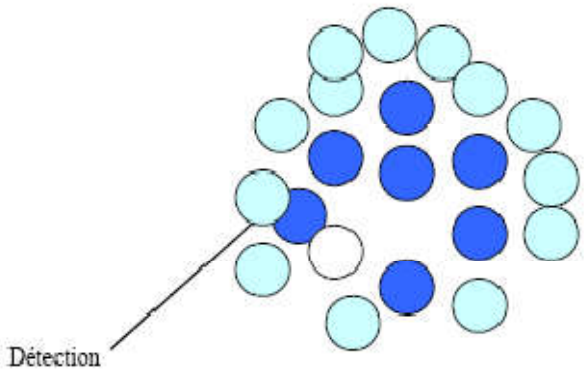


Figure IV.14 Détection de changement

La détection négative est inefficace dans le choix des détecteurs [DEN06] Une partie de l'espace des formes peut être couverte par plusieurs détecteurs qui se recouvrent ; et d'autres parties peuvent ne pas être recouvertes du tout. Et le pire est que, pour certains ensembles de chaînes, des trous peuvent apparaître qui ne peuvent être couverts par n'importe laquelle des configurations possibles de détecteurs, sans que cela conduise à recouvrir des chaînes du soi.

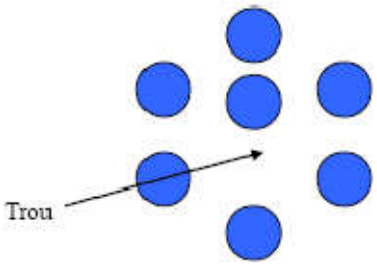


Figure IV.15 trous dans les chaines soi

IV.2.4.1.2 Domaines d'utilisation de la sélection négative

Esponda et Forrest ont appliqué la sélection négative au problème de détection d'intrusions dans un réseau informatique. Le système, nommé LISYS, génère un ensemble de détecteurs qui, confrontés à un réseau sain, ne doivent détecter aucun

paquet transmis dans le réseau. Mais, dès qu'il y a un trafic suspect dans les réseaux, les détecteurs sont activés et l'utilisateur est prévenu [WEB01].

Esponda et al en 2003 ont appliqué la sélection négative aux bases de données « négatives », qui permettent de stocker des données dans une forme « négative » de façon à ce que la récupération des données sous leur forme d'origine est un problème NP - difficile. Les bases de données négatives sont très utiles dans le domaine de la sécurité informatique, par exemple pour stocker les mots de passes. Les requêtes de type « est-ce que la chaîne x se trouve dans la base ? » peuvent être satisfaites très rapidement, alors que des requêtes du genre « donnez moi toutes les chaînes qui commencent par '1' » sont très difficiles à résoudre [DEN06].

IV.2.4.2. Sélection Clonale

Elle est complémentaires au rôle de la Sélection Négative, la sélection clonale est la théorie utilisée pour expliquer comment une réponse immunitaire est montée quand un non soi est reconnu par une cellule B. Quand un récepteur d'une cellule B reconnaît un antigène avec une certaine affinité, il est sélectionné à proliférer et produire des anticorps dans des volumes élevés. Les anticorps sont des formes solubles des récepteurs des cellules B qui sont libérées sur la surface de la cellule pour faire face à l'envahisseur non soi. Les anticorps se lient aux antigènes conduisant à leur élimination éventuelle par d'autres cellules immunitaires. La prolifération dans le cas des cellules immunitaires est active.

Lors de la reproduction, la cellule B (clones) subit un processus de mutation qui, avec une forte pression sélective, aboutit à des cellules B avec des récepteurs antigéniques qui présentent les plus grandes affinités sélectives à l'antigène.

L'ensemble de processus de mutation et de sélection est connu sous le nom de la maturation de la réponse immunitaire. En plus d'une différenciation en cellules productrices d'anticorps, l'activation des cellules B antigénique avec affinités élevés sont sélectionnées pour devenir des cellules mémoires avec une longue durée de vie. Ces cellules mémoires sont prééminentes dans les futures réponses à ce même antigène.

- Autres caractéristiques importantes de la sélection clonale du point de vue du calcul sont:

1. Un antigène sélectionne plusieurs Cellules Immunitaires à proliférer. Le taux de prolifération de chaque cellule est proportionnel à son affinité avec l'antigène sélectif: Plus l'affinité est élevée plus le nombre de descendant est générés.

2. La mutation et la reproduction est inversement proportionnelle à l'affinité de la Cellule B.

Certains auteurs ont proposé un algorithme de Sélection Clonale, nommé CLONALG, Pour s'acquitter des processus fondamentaux impliqués dans la sélection clonale. Cet algorithme a été initialement proposé pour effectuer la reconnaissance des formes, puis adapté pour résoudre des tâches d'optimisation .Etant donné un ensemble de formats à être reconnus (P), les étapes fondamentales de l'algorithme CLONALG sont les suivantes:

1. Initialiser aléatoirement une population d'individus (M ; les anticorps).

2. Pour chaque type de P, le présenter à la population M et déterminer son affinité à chaque élément de la population M.

3. Sélectionner les meilleurs éléments N de la plus haute affinité M et générer des exemplaires de ces particuliers, proportionnellement à leur affinité avec l'antigène. Plus l'affinité est élevée, plus le nombre de copies s'accroit.

4. Muter tous les exemplaires avec un taux proportionnel inverse à leur affinité avec la contribution.

5. Ajouter ces cellules mutées à la population M et sélectionner de nouveau de ces n Maturité (optimisé) les cellules qui doivent être conservées comme modèle système.

6. Répétez les étapes 2 à 5 jusqu'à ce qu'un certain critère soit rempli, comme un modèle minimal de la reconnaissance ou l'erreur de classement.

- Cet algorithme permet au Système Immunitaire Artificiel de devenir plus performent à sa tâche de reconnaissance des schémas (antigènes). Ainsi, en fonction d'un comportement évolutionnaire.

IV.2.4.2.1 Domaines d'utilisation de la sélection clonale

De Castro et Von Zuben ont appliqué la sélection clonale à l'optimisation. Dans ce cas, chaque anticorps représente une solution possible au problème. La fonction affinité, quand à elle, renvoie la qualité de chaque solution (les meilleures solutions ont les plus grandes affinités).

Les auteurs ont proposé un algorithme de sélection clonale destiné à la détection d'intrusions. L'algorithme nommé DynamiCS, est un algorithme de classification binaire qui contient deux classes le soi et le non soi, et utilise les propriétés de la sélection clonale pour générer des cellules mémoire qui reconnaissent le non soi sans reconnaître le soi [.WEB02].

Les auteurs ont proposés aussi ClonAlg, une implémentation de la sélection clonale pour la reconnaissance des formes. Mais n'étant pas plus qu'une preuve de faisabilité, l'algorithme souffre de limitations majeures. La plus importante étant qu'il n'accepte pas : plus d'un exemple d'entraînement par classe.

White et Garrett ont proposé ClonClas, qui est une amélioration de ClonAlg [WHI03]. Les auteurs ont utilisé la sélection clonale pour chercher dans chaque classe le prototype qui la représente le mieux. Ces prototypes sont ensuite utilisés dans un système de reconnaissance de chiffres imprimés. En d'autres termes, la sélection clonale est utilisée comme un algorithme d'apprentissage.

Les principes de la sélection clonale ont aussi été appliqués à la résolution de problèmes multi objectifs. Pour ce genre de problèmes, plusieurs objectifs doivent être optimisés en même temps. Les objectifs étant souvent en conflits, l'optimisation de l'un d'eux rend les autres objectifs non optimisés. Cuello a proposé un algorithme pour la résolution des problèmes multi objectifs en utilisant les principes de la sélection clonale. L'algorithme nommé MISA est générique dans le sens où il peut être appliqué à n'importe quel problème d'optimisation quel que soit le nombre d'objectifs.

- Les deux sélections : négative et clonale, permettent la résolution des problèmes de détection d'intrusions dans un réseau informatique.
- Bien que la sélection clonale ressemble beaucoup aux algorithmes génétiques, il reste des différences majeures entre les deux approches: Dans les algorithmes génétiques, la sélection des individus est stochastique (par exemple la roulette) et on utilise le principe de croisement des chromosomes, par contre dans les systèmes immunitaires artificiels, la sélection est déterministe (sélection des meilleurs individus) et on utilise le principe de clonage et de la mutation des cellules [WEB03] [WEB04].

IV.2.4.3 Les modèles de Réseaux Immunitaires Artificiels

IV.2.4.3.1 Principe des modèles des réseaux immunitaires artificiels

De Castro et Von Zuben, en 2001, on proposé aiNet, un algorithme qui combine la théorie des réseaux immunitaires et la sélection clonale. AiNet utilise la notion d'image interne pour représenter les regroupements de données dans un réseau. Par exemple, pour l'ensemble de données de la Figure IV.17, une architecture hypothétique générée par aiNet est donnée à la figure IV.18. Les nœuds représentent les anticorps, les lignes pleines sont des connections entre les anticorps, et les lignes en pointillé sont des connections qui seront éliminées pour révéler les regroupements. Comme le nombre de nœuds du réseau est plus petit que le nombre initial de données, aiNet peut être utilisé pour la compression.

Les cellules immunitaires sont en compétition pour se lier avec l'antigène, celles qui réussissent sont activées, alors que les autres sont éliminées. De plus, la liaison Ab – Ab (anticorps – anticorps) conduit à la suppression. Dans aiNet, la suppression se fait en éliminant les anticorps qui se lient à eux-mêmes.

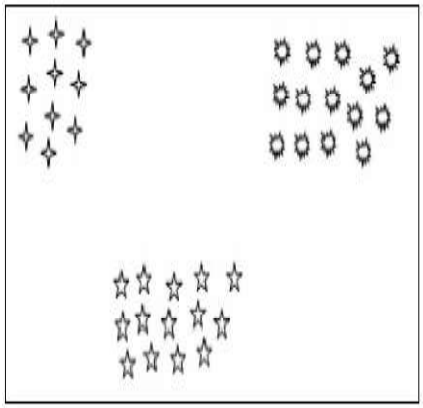


Figure IV.17 Exemple de groupements de données

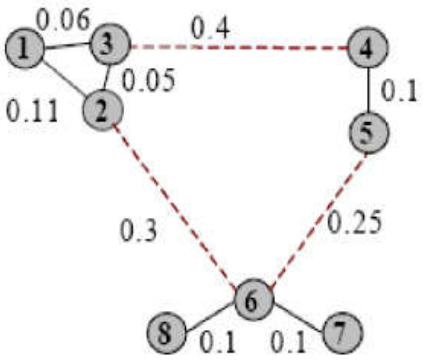


Figure IV.18 Réseau immunitaire généré par aiNet

IV.2.4.3.2. Algorithme des réseaux immunitaires artificiels d'aiNet

L'algorithme de aiNet est comme suit :

1- Initialisation

- La population d'anticorps est générée aléatoirement.
- La population de cellules mémoire est initialement vide.
- La population d'antigènes contient les données d'apprentissage.

2- Pour chaque antigène :

Répéter pour un certain nombre d'itérations :

- **Evaluation et sélection 1**

Evaluer l'affinité de tous les anticorps pour l'antigène courant.
Sélectionner **n** anticorps qui ont les plus grandes affinités.

- **Clonage**

Cloner les anticorps proportionnellement à leurs affinités.

- **Mutation**

Muter les anticorps clonés avec un taux inversement proportionnel à leur affinité pour obtenir une population mature.

- **Evaluation et sélection 2**

Evaluer l'affinité des anticorps matures pour l'antigène courant.
Sélectionner ' %' anticorps qui ont les meilleures affinités pour obtenir les cellules mémoire.

- **Suppression clonale 1**

Eliminer les cellules mémoire qui sont très similaires les unes aux autres.

- **Mémorisation**

Ajouter les cellules mémoire qui ont une affinité qui dépasse un certain seuil à la population de celles-ci (cellules mémoire).

- **Mort**

Les anticorps et cellules mémoire non mémorisés sont éliminés.

- **Suppression clonale 2**

Eliminer les cellules mémoire (de la population de cellules mémoire) très similaires.

- Il y a beaucoup de similarité entre aiNet et les algorithmes de sélection clonale. En fait, la sélection clonale artificielle est un cas particulier des réseaux immunitaires.
- Dans aiNet, ce sont les étapes de suppression clonales qui distinguent cet algorithme de la sélection clonale puisqu'elles expriment des interactions explicites entre les anticorps (cellules mémoire) dans le réseau. Alors que dans les algorithmes de sélection clonale aucune interaction explicite ne se fait entre les anticorps.

IV.2.4.3.3. Domaines d'utilisation des réseaux immunitaires

L'approche réseau est particulièrement intéressante pour le développement d'outils de calcul parce qu'elle tient compte, potentiellement, de propriétés émergentes telles que l'apprentissage et la mémorisation, la tolérance au soi, la gestion de la taille de la population de cellules ainsi que de la diversité.

Knight et Timmis ont proposé MARITA, un algorithme pour l'apprentissage supervisé inspiré de la théorie des réseaux immunitaires et de la sélection clonale. La nouveauté de leur approche est que le système est divisé en plusieurs couches, chaque couche étant responsable d'une fonction précise. La sortie de chaque couche est l'entrée de la couche suivante. Les couches du système sont : la couche d'anticorps, cellules B et cellules mémoire. Le système utilise un mécanisme de contrôle de la population qui élimine de toutes les couches les cellules qui n'ont pas été stimulées pendant une longue période.

Nasraoui et al, ont appliqué les réseaux immunitaires artificiels à l'analyse des activités d'un serveur web. Le but du système est de détecter les types d'utilisateurs à travers le parcours des utilisateurs sur le serveur. Il permet aux gestionnaires du système de mieux organiser les pages selon les types d'utilisateurs les plus fréquents. Le serveur pourra aussi prédire le type d'un nouvel utilisateur et adapter son interface à ce dernier.

IV.2.5 Mesure d'affinité

De nombreuses mesures de distance ou d'indices de similarité existent, On n'en citera ici que quelques unes parmi les plus fréquemment utilisées :

- Distance Euclidienne.
- Distance de Hamming.
- Distance de Manhattan.
- Distance de Bray-Curtis.
- Distance du Chicarré.

IV.2.6 L'algorithme A.I.R.S. (Artificial Immune Recognition System) :

IV.2.6.1 Définitions :

les définitions des principaux termes et concepts qui s'appliquent à l'algorithme AIRS sont :

- ***affinité:*** c'est une mesure de «proximité» ou de similarité entre deux anticorps ou antigènes. Cette valeur est assurée d'être entre 0 et 1 et se calcule simplement avec la distance euclidienne de vecteurs de caractéristiques de deux

objets. Ainsi, les valeurs *d'affinité petite* indiquent une forte affinité.

- ***seuil d'affinité (AT)*:** c'est la valeur d'affinité moyenne parmi tous les antigènes dans l'ensemble d'apprentissage ou au sein d'un sous-ensemble sélectionné de ces antigènes d'apprentissage.

- ***scalaire du seuil d'affinité (ATS):*** c'est une valeur comprise entre 0 et 1 ; quand elle est multipliée par le seuil d'affinité, elle fournit une valeur seuil pour le remplacement de cellules mémoire dans la boucle d'apprentissage AIRS.
- ***Anticorps* :** c'est un vecteur de caractéristique associé avec la classe. La combinaison vecteur de caractéristique/classe est appelé un anticorps quand elle fait partie d'un ARB ou d'une cellule mémoire.
- ***Antigène*:** dans sa représentation, c'est similaire à un anticorps, mais la combinaison de vecteurs caractéristiques-classe est appelée un antigène quand elle est présentée à l'ARB pour la stimulation.
- ***Artificiel Immune Recognition System(AIRS)* :** c'est l'algorithme de classification inspirée du système immunitaire naturel.
- ***Artificielle Reconnaissance Ball (ARB)*:** également connu sous le nom cellule B, l'ARB se compose des anticorps, un comptage du nombre de ressources détenues par la cellule, et la valeur de stimulation de la cellule courante.
- ***Cellule mémoire candidate*:** l'anticorps d'un ARB, de la même classe que l'antigène d'apprentissage, qui était le plus stimulée après l'exposition à l'antigène donné.
- ***Classe*:** il s'agit de la catégorie d'un vecteur caractéristique donné. Ceci est aussi appelé la sortie d'une cellule.
- ***Taux de clonage* :** une valeur entière utilisée pour déterminer le nombre de clones mutés pour un ARB donné. Dans l'implémentation actuelle, un ARB sélectionné est autorisée à produire jusqu'à (taux de clonage x valeur stimulation) clones mutés après avoir répondu à un antigène donné. Ce produit est également utilisé dans l'attribution des ressources à un ARB. Par conséquent, le taux de clonage a un double rôle : c'est un facteur d'allocation des ressources et un facteur de mutation clonale de la population des cellules.
- ***Cellule mémoire établi (mc_{match})*:** c'est l'anticorps d'un ARB qui a survécu à la concurrence pour les ressources et a été le plus stimulé à un antigène d'apprentissage et qui a été ajouté à l'ensemble des cellules de mémoire.
- ***Vecteur de caractéristiques*:** c'est une instance de données représentées par une séquence de valeurs, et où chaque élément a ses propres valeurs.
- ***Taux d'hyper-mutation*:** une valeur entière utilisée pour déterminer le nombre de clones mutés pour une cellule mémoire donné, autorisée à injecter dans la population cellulaire. Dans l'implémentation actuelle, la cellule mémoire sélectionnée injecte au moins (taux d'hyper-mutation*taux de clonage*valeur de stimulation) clones mutés dans la population cellulaire au moment de l'introduction d'antigène.
- ***Cellules mémoire (MC):*** l'anticorps d'un ARB qui était le plus stimulé par un antigène d'apprentissage donné à la fin de l'exposition à cet antigène. Il est utilisé pour l'hyper-mutation en réponse à des antigènes d'apprentissage entrant. Un *mc* peut être remplacé, toutefois. Cela se produit uniquement lorsque le *mc* candidat est plus stimulé à un antigène d'apprentissage donné que la cellule mémoire établi la plus stimulée et l'affinité entre le *mc* établi et le *mc* candidat est inférieur au produit du seuil d'affinité et de l'affinité Seuil scalaire.
- ***Taux de mutation :*** c'est un paramètre entre 0 et 1 qui indique la probabilité que toute caractéristique donnée (ou la sortie) d'un ARB sera muté.

- ***Sortie:*** il s'agit de la catégorie de classification associée à une cellule. La même que la classe du vecteur de caractéristiques correspondant à cette cellule
- ***Ressource*:** un paramètre qui limite le nombre d'ARB permis dans le système. A chaque ARB est attribué un certain nombre de ressources en fonction de sa valeur de stimulation et le taux de clonage. Le nombre total des ressources du système est fixé à une certaine limite. Si plus de ressources sont consommées que ne sont autorisées à exister dans le système, alors les ressources sont retirées du moins jusqu'à ce que le nombre de ressources d'un ARB stimulé dans le système retourne au nombre autorisé. Si toutes les ressources de données ARB sont retirées, alors l'ARB est retiré de la population de cellules.
- ***cellule initiale (seed cell)* :** c'est un anticorps, tiré de l'ensemble d'apprentissage, utilisé pour initialiser les cellules mémoire et ARB au début d'apprentissage.
- ***fonction de stimulation*:** Dans la formulation actuelle du classificateur AIRS, cette fonction doit avoir une valeur entre 0 et 1. Pour la mise en œuvre de l'AIRS présenté dans cette étude, la fonction de stimulation est inversement

proportionnelle à la distance euclidienne entre les vecteurs de caractéristiques de l'ARB et l'antigène.

- ***valeur de stimulation*:** la valeur retournée par la fonction de stimulation.
- ***seuil de stimulation:*** un paramètre entre 0 et 1 utilisé comme critère d'arrêt pour l'apprentissage sur un antigène spécifique.
- ***ensemble de test:*** ensemble d'antigènes utilisés pour évaluer les performances de classification du classificateur AIRS.
- ***Ensemble d'apprentissage :*** la collecte des antigènes utilisés pour l'entrainement du classificateur AIRS.

IV.2.6.2 Déroulement de l'algorithme

Les étapes principales impliquées dans l'algorithme AIRS sont :

IV.2.6.2 .1 Etape d'initialisation

Dans cette partie les données d'apprentissage (antigènes) seront normalisé et tout vecteur caractéristique aura des valeurs de l'intervalle [0, 1]. Un seuil d'affinité est calculé à partir cet ensemble d'antigène, qui représente l'affinité moyenne entre tous les antigènes deux à deux. Le seuil d'affinité est calculé selon la formule (IV.1) :

$$seuil\_d'affinité = \frac{\sum_{i=1}^{n}\sum_{j=i+1}^{n} affinité(ag_i, ag_j)}{\frac{n(n-1)}{2}} \qquad \text{(IV.1)}$$

avec : ag_i et ag_j deux antigènes et *affinité (a,b)* retourne la distance euclidienne normalisée entre *a* et *b*.

La dernière étape d'initialisation consiste à initialiser l'ensemble des cellules mémoires (anticorps) et la population des ARB (*A*rtificial *R*ecognition *B*all), à partir de l'ensemble des antigènes par tirage aléatoire des exemples.

IV.2.6.2.2 Etape d'identification des cellules B et génération des ARBs

Une fois que l'initialisation est achevée, cette étape aura lieu pour chaque nouvel antigène introduit. Une cellule mémoire est sélectionnée de l'ensemble entier de cellules B est nommé mc_{match}, cette dernière est tiré de tel sorte qu'elle ressemble (selon la formule (IV.2)) le plus à l'antigène en cours de traitement (la plus grande valeur de stimulation) selon la formule (IV.3) :

$$stimulation(ag, mc_{match}) = 1 - affinité(ag, mc_{match}) \qquad \text{(IV.2)}$$

$$mc_{match} = arg\,max_{mc \epsilon MCag.c}\, stimulation(ag, mc) \qquad \text{(IV.3)}$$

Une fois que la cellule mc_{match} est sélectionnée, elle sera utilisée pour générer les nouveaux ARBs (clonage), cet ensemble sera additionné à l'ensemble total des ARBs généré par l'ensemble des antigènes préalablement traité. Le nombre de clone de la cellule mc_{match} est limité selon la formule (IV.4):

$$nombre\_de\_clones = hyper\_clonal\_rate * clonal\_rate * stimulation\,(mc_{match}, ag_{en\_cours}) \qquad \text{(IV.4)}$$

IV.2.6.2.3 Compétition des ressources et développement des cellules mémoire candidates :

Cette partie se base sur les résultats de la précédente, elle complète les informations des ARBs généré en calculant les ressources selon (IV.5) pour chaque anticorps avec l'antigène en cours de traitement, ces ressources sont mises à jour durant l'apprentissage, et chaque ARB n'ayant pas de ressources sera supprimé de l'ensemble des ARBs [Wat01].

$$ressources = stimulation\,(ag, anticorps) * clonal\_rate \qquad \text{(IV.5)}$$

Les étapes (**IV.2.6.2.1) et (IV.2.6.2.2)** seront exécutés pour un antigène donné jusqu'à ce que la condition :

***s_i>= seuil _ d'affinité* soit vérifiée, avec**

$$s_i = \frac{\sum_{j=1}^{|AB_i|} ab_j.stim}{|AB_i|}, ab_j \epsilon AB_i \qquad \text{(IV.6)}$$

A la fin de ces deux étapes un ensemble d'ARBs est obtenu pour s'introduire à l'étape finale de l'apprentissage.

IV.2.6.2.4 Introduction des cellules mémoires :

Cette étape consiste à choisir à partir des ARBs la cellule candidate qui convient le plus à l'antigène en terme de similarité tenant en compte la cellule mc_{match} déjà sélectionné, la cellule candidate sera additionné à l'ensemble des cellules mémoire seulement si retourne une stimulation plus élevé que la cellule mc_{match} avec l'antigène en cours de traitement sinon la cellule mc_{match} sera retiré de cellules mémoire seulement si sa stimulation entre la cellule candidate avec mc_{match} ne dépasse pas le seuil [Wat01].

Après la fin de cet algorithme d'apprentissage les cellules mémoire générées sont prêtes pour une utilisation de classification des antigènes.

IV.3 Conclusion

Le système immunitaire artificiel est un exemple du système immunitaire naturel qui a servi pour résoudre une grande variété de problèmes informatiques. Il se divise en trois grandes familles :

1- la sélection négative, qui s'inspire des mécanismes naturels de distinction entre soi et non soi, pour résoudre des problèmes de surveillance et de détection de changement.

2- La sélection clonale artificielle, qui s'inspire des mécanismes naturels de mémorisation pour résoudre des problèmes d'optimisation.

3- les réseaux immunitaires artificiels, qui s'inspirent de la théorie des réseaux immunitaires pour construire des systèmes qui permettent la distinction et la mémorisation.

Le chapitre suivant sera consacrée à la conception de notre application basée sur l'algorithme AIRS inspiré des systèmes immunitaires artificiels, nous enchainerons par une série de tests qui nous permettront d'évaluer notre algorithme.

CHAPITRE V :

IMPLEMENTATION ET FUSION DES SYSTEMES D'IDENTIFICATION

V. Implémentation et fusion des systèmes d'identification

V.1 Introduction:

Après avoir abordé l'aspect théorique dans les chapitres précédents, nous passons à la conception et à l'implémentation de notre application pour la reconnaissance des individus par les modalités décrites dans le chapitre III. Afin de déterminer les personnes par d'identification de l'iris et les empreintes digitales ; on se doit de capturer l'image de l'œil ou de l'empreinte digitale (Figure V.1).

A- L'identification de l'iris :

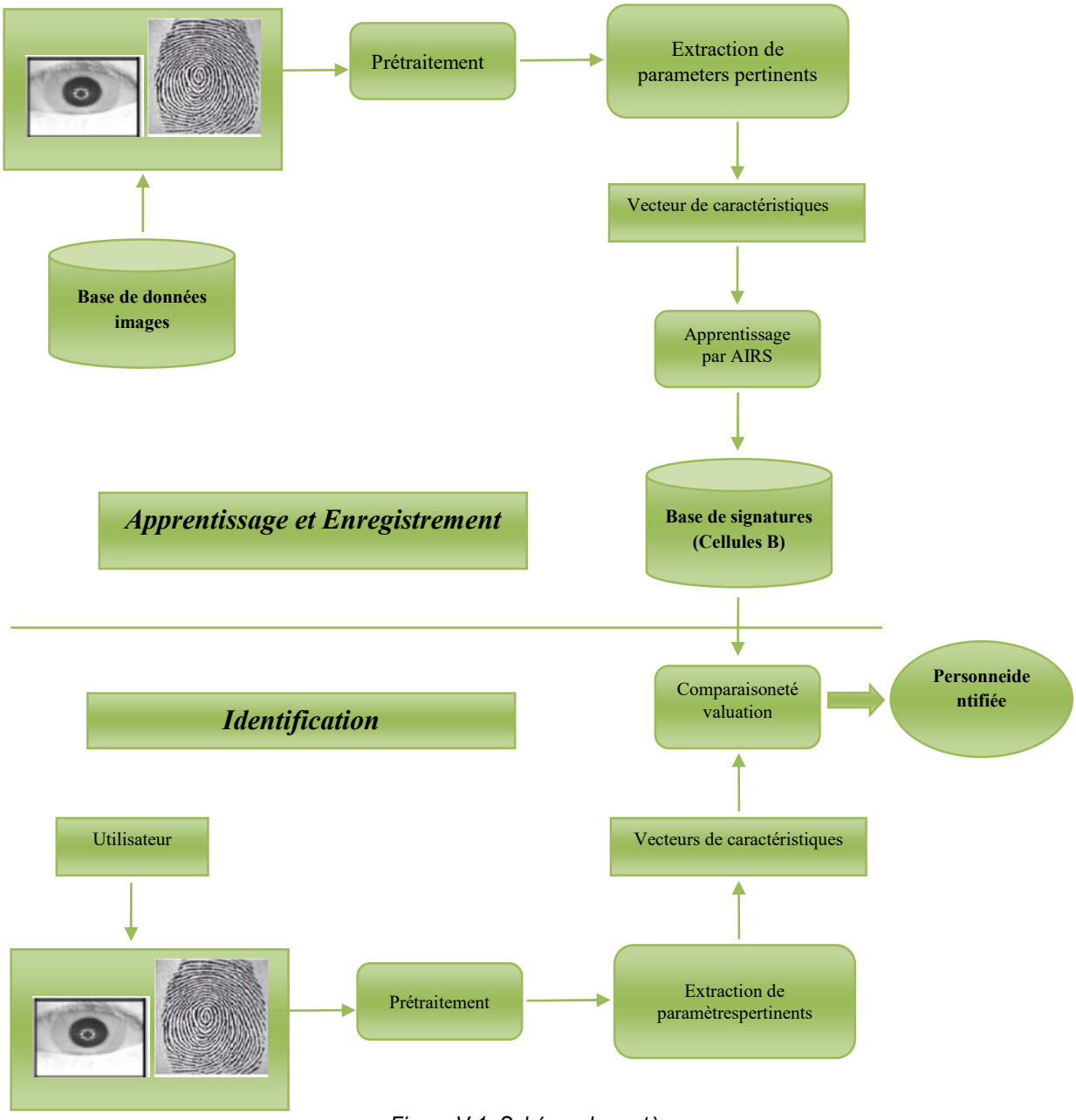


Figure V.1: Schéma du système.

Le but étant d'intégrer les personnes dans des classes, en fonction d'un critère donné. Cela nécessite l'exploitation et l'interprétation d'un certain nombre de caractéristiques extraites de l'iris ou de l'empreinte digitale d'un individu inconnu, de manière à créer une hypothèse sur sa classe d'appartenance.

Un des problèmes majeurs est le choix des caractéristiques devant représenter l'ensemble des individus à reconnaitre. Ce choix est important car il conditionne toute la méthodologie mise en œuvre pour l'identification.

L'algorithme AIRS (*Artificial*/mmune *R*ecognition *S*ystem), détaillé au chapitre IV est appliqué dans cette étude pour définir les modèles constitutifs de notre base de données, Le but est de générer un ensemble de cellules mémoires (cellules B) capable de classifier de nouveaux modèles d'individus inconnues (nouveaux antigènes).

Les systèmes d'identification des deux signatures sont implémentés séparément

V.2 Base de données de l'iris (CASIA)

Nous avons évalué notre première approche*sur la base de données d'image CASIA. Les images de cette base sont de taille : 320 x 280 pixels. Le mode d'acquisition est en infrarouge.

La base de données CASIA est composée de deux fichiers, le premier contient des iris de personnes asiatiques, et le deuxième est celui des personnes non asiatiques. Chaque fichier contient 59 personnes avec 15 positions de l'œil droit et 15 positions de l'œil gauche.

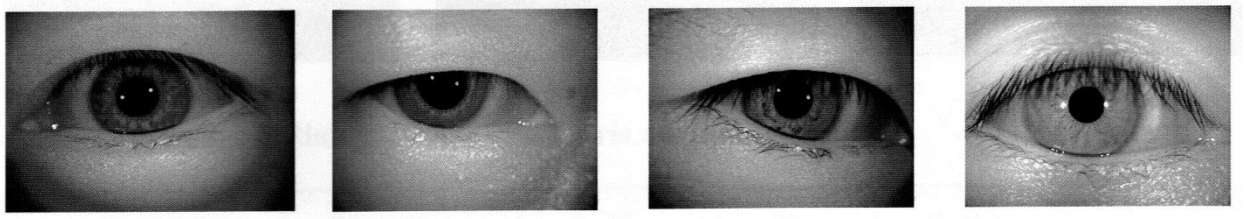


Figure V.2 : l'iris de personnes asiatiques

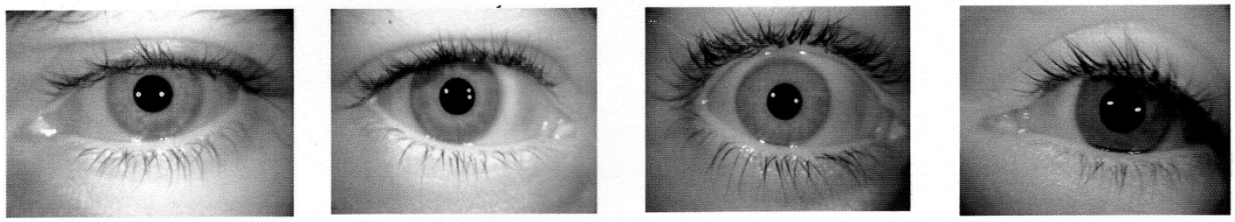


Figure V.3 : l'iris de personnes non-asiatiques

* l'étude sur l'iris comporte deux approches, Quant à la seconde ; pour notre étude, nous nous sommes contentés de 210 images représentant 30 classes de 7 images chacune.

IV.3. Segmentation :

V.3.1. Prétraitement :

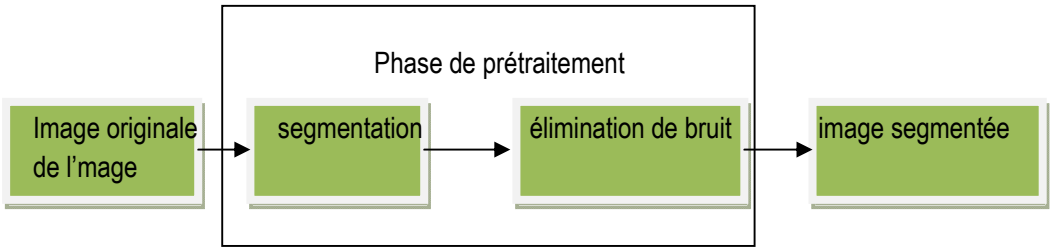


Figure. V.4.principe de prétraitement de l'iris.

Cette phase consiste à segmenter l'image de l'iris par la transformée de Houghet à normaliser en appliquant une transformation polaire. Ces deux opérations sont necessaires pour l'étape d'extraction des caractéristiques

La transformée de Hough :

La transformée de *Hough* a été proposée en 1972 par *Duda* et *Hart* comme une technique pour l'solation des objets de formes géométriques simples (des lignes, des cercles, des courbes,…etc.) dans l'image [Dud 72].

Comme cités précédemment, les objets à détecter dans l'image de l'oeil (iris, pupille, paupières) ont une forme circulaire ou ellipsoïde, ce qui s'adapte bien à une détection par *la transformée de Hough circulaire*. *Wildes* a été le premier à introduire cette méthode dans le contexte de la segmentation de la région d'iris dans les images de l'oeil [Wil 97]. Ensuite, plusieurs autres travaux ont été proposés (*Kong et Zhang* [Kon 01], *Ma et al* [Lma 04] et *Nabti et Bouridane* [Nab 07]) qui utilisent la transformée de *Hough* pour localiser le disque de l'iris.

La méthode de *Wildes*effectuée la détection de contours sur deux étapes principales. Au début, l'image capturée est transformée en image binaire de contours (*Binary Edge-Map*). Cette transformation est effectuée par la méthode de *John Canny* [Can 86], toute en calculant la première dérivation de valeurs d'intensité de l'image de l'oeil suivi d'une opération de seuillage (deux seuils prédéfinis) de l'image résultante. De plus, il est possible d'effectuer cette transformation dans une direction (horizontale ou verticale) ou dans les deux. Les points contours alignés horizontalement n'apparaissent pas dans la direction verticale. Comme exemple, différentes images binaires de contours obtenues par la méthode de Canny sont montrées sur la figure V.5 [Por 06b].

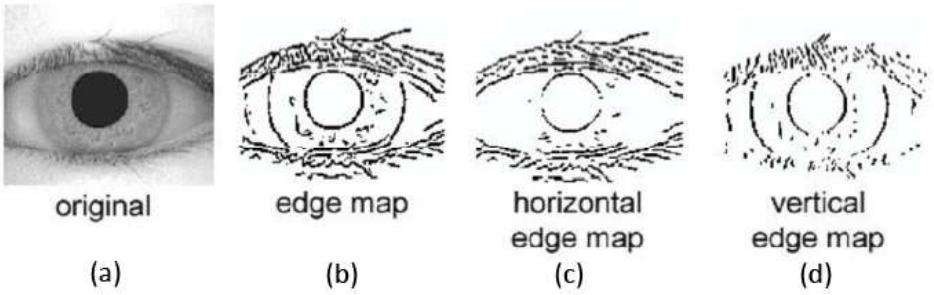


Figure V.5 : Les différents types d'image de contour par la méthode Canny (a) image de l'œil, (b) image de contour globale, (c) image de contour horizontale et (d) image de contour verticale.

Ensuite, les points contours (pixels) votent, dans un espace de paramètres de *Hough*, pour les cercles auxquels ils appartiennent. Ces paramètres sont les coordonnées du centre $C(x_c,y_c)$ et le rayon r, qui définissent un cercle quelconque par l'équation suivante :

$$r^2 = (x - x_c)^2 + (y - y_c)^2$$

Ce vote donne, en résultat, le rayon et les coordonnées du centre du cercle le mieux défini par les points contours. Dans le cas d'occlusion des paupières, *Wildes* a utilisé également la transformée de *Hough* parabolique [Wil 97]. Elle sert à détecter les bordures de paupières,supérieure et inferieure, tout en les approximant par deux arcs paraboliques représentés par l'équation suivante :

$$\left((y - k_j)cos\theta_j - (x - h_j)sin\theta_j\right)^2 = a_j\left((x - h_j)cos\theta_j + (y - k_j)sin\theta_j\right)$$

Où (a_j) est la distance focale contrôlant la courbe parabolique, (h_j,k_j) sont les coordonnées du sommet de la parabole et (θ_j) est l'angle de rotation par rapport à l'axe des abscisses.

Pour la détection de contours, *Wildes* a proposé la dérivation dans la direction horizontale pour détecter les bordures de paupières et dans la direction verticale pour détecter la bordure extérieure circulaire de l'iris. Cela est motivé par l'alignement horizontal des paupières dont les contours corrompent, généralement, les contours circulaires de l'iris. De plus, l'utilisation de l'image de contours verticale pour localiser les bordures de l'iris réduit l'influence des paupières sur le processus de la transformée de *Hough* circulaire. Effectivement, les points contours définissant le cercle, ne sont pas tous nécessaires pour une localisation correcte. Ainsi, le processus de vote, dans l'espace de paramètres de *Hough*, est optimisé car il y a moins de points de contours.

V.3.2. Segmentation de l'iris

La segmentation de l'iris se base sur la méthode de la transformée de Hough circulaire décrite précédemment qui consiste à extraire les deux bordures de l'iris (figure V.6) . Le schéma de la figure V.7 décrit le cheminement de cette méthode .
Nous remarquons bien le passageen amont par le filtre de Canny (figure V.7).Celui-ci permettra de concevoir les trois images pour la detection des contours des paupières et de l'iris.

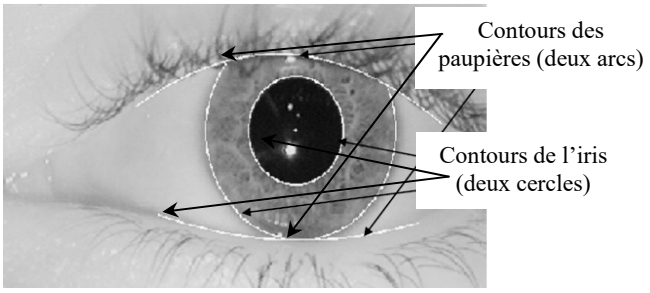


Figure V.6: Segmentation de l'iris.

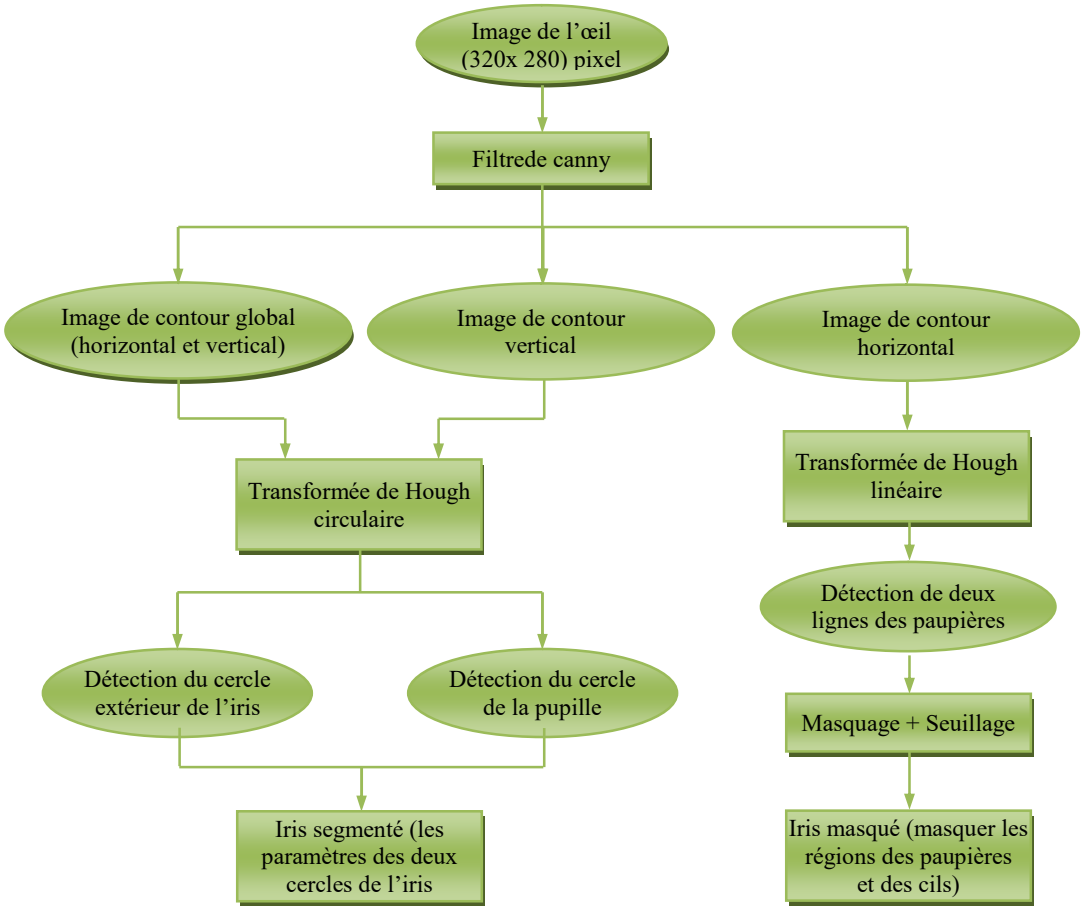


Figure V.7: Diagramme du processus de segmentation de l'iris de l'œil. [Dau 94]

V.3.3 Déroulement

Une fois l'iris determiné , nous procedons à la phase de déroulement en utilisant la transformation polaire proposée par Daugman [Dau 94] Formule(V.1)

Cette phase consiste à transformer la couronne représentant l'iris en rectangle ou bande (voir figure V.8):

Cette opération tend à supprimer l'information non-utile et ensuite la remise en forme matricielle de l'information utile.

$$I(x(r,\theta),y(r,\theta)) \rightarrow I(r,\theta) \qquad \text{(V.1)}$$

Avec *I* est une image d'iris

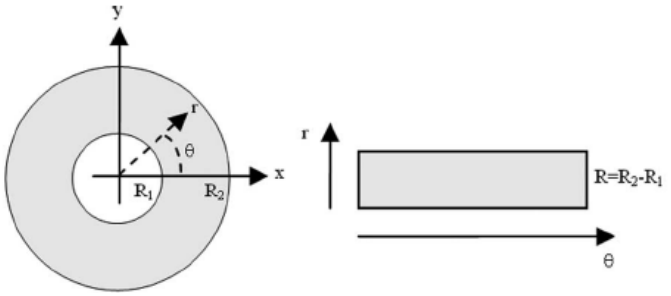


Figure V.8 : Transformation polaire.

Figure V.9 : Image d'iris déroulée.
(La largeur de l'image représente la variation sur l'axe angulaire alors que la hauteur représente les variations sur l'axe radial.)

V.3.4 Egalisation de l'histogramme

Représentée par la formule V.2 ; cette étape du schéma consiste à rendre l'histogramme de l'image aussi uniforme que possible qfin de donner une chance d'apparition équiprobable pour tous les niveaux de gris des pixels

$$f_{egal}[x,y] = 2^D - 1 * \frac{HC(f[x,y])}{w.h} \text{(V.2)}$$

Avec :

- D :dynamique.
- (w,h) : la dimension de l'image.
- HC() : l'histogramme cummulé.

Figure V.10 : Image d'iris déroulée et égalisée.

V.3.5 Extraction des paramètres pertinents à partir d'image

Pour arriver à identifier les personnes, nous devons tout d'abord choisir parmi les paramètres contenus dans l'iris, ceux les plus pertinents, et ensuite procéder au codage de cette information afin de comparer les images entre elles. L'extraction de paramètres caractéristiques de l'iris se traite généralement en utilisant les filtres de Gabor [Dau 93].Pour extraire les caractéristiques, le modèle de l'iris normalisé est codé par les ondelettes de Log-Gabor 1-D. Les ondelettes Log-Gabor sont représentées comme suit:

$$G(f) = \exp\left(\frac{-(log(f/f_0))^2}{2(log(\sigma/f_0))^2}\right) \qquad (V.3)$$

Où f_0 *est* la fréquence centrale etσ la bande passante du filtre.

Nous partagerons les images de l'iris normalisées initialement à deux dimensions en signaux d'une dimension qui, à travers les ondelettes de Gabor 1-D (formule V.3) sont filtrés .Notons que Chaque ligne du modèle d'iris normalisé est considérée comme un signal 1D (chaque ligne correspond à un anneau circulaire sur la région de l'iris).

Le signal de sortie du filtrage est ensuite démodulé et la phase est quantifiée en utilisant la méthode de Daugman [Dau 94]. La sortie est une phase quantifiée à quatre niveaux (voir figure V.11), un pour chaque quadrant dans le plan complexe et chaque filtre produit deux bits de données pour chaque phase [Opp 81]. Les valeurs de phase de tous les pixels de l'image de l'iris normalisée 240x20 sont alors quantifiées à quatre niveaux de telle sorte que chaque pixel soit représenté avec 2 bits, produisant d'une signature binaire de taille 480x20.

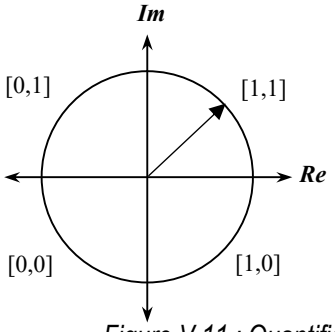


Figure V.11 : Quantification de phase

Résultats de la segmentation

• Asiatique :

Au cours des expériences, Comme le montre la figure V.12, la détection de l'iris chez les personnes asiatiques est relativement difficile du fait des paupières tombantes cachant une partie de l'iris ce qui nous a conduit à une fausse détection dans certaines captures.

Illustration1 :

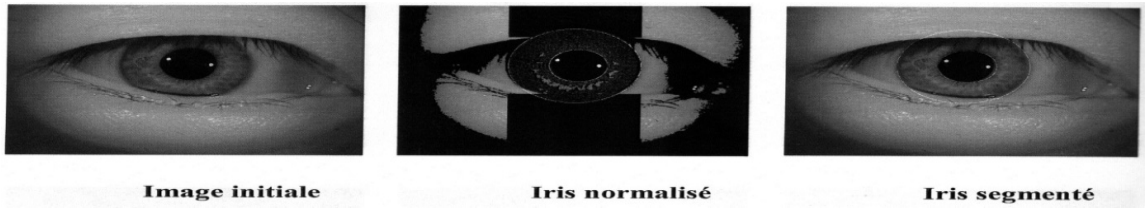


Figure V.12 Détection exacte de l'iris d'une personne asiatique

Illustration2 :

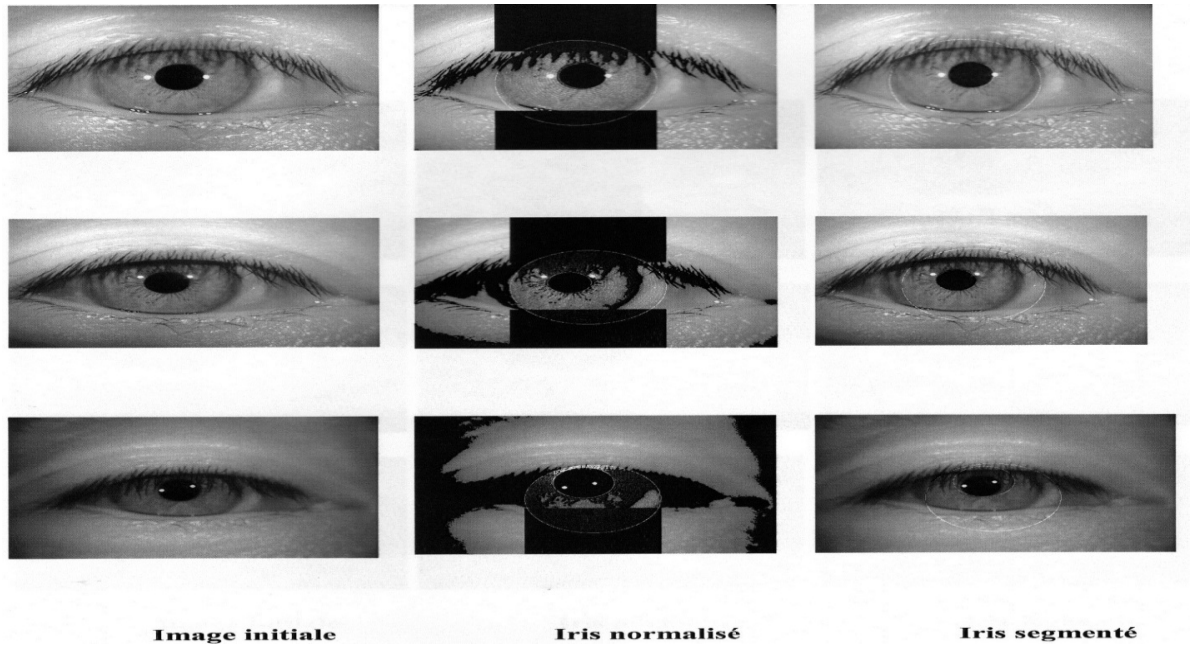


Figure V.13 Différentes captures pour la même personne

Non-asiatique : les résultats sont bons et le schéma proposé pour la détection de l'iris est fiable pour les yeux non-asiatiques. Cependant, nous pouvons noter des difficultés mineures telles que le port des lunettes ou le mauvais positionnement des personnes devant le capteur

Illustration 3 :

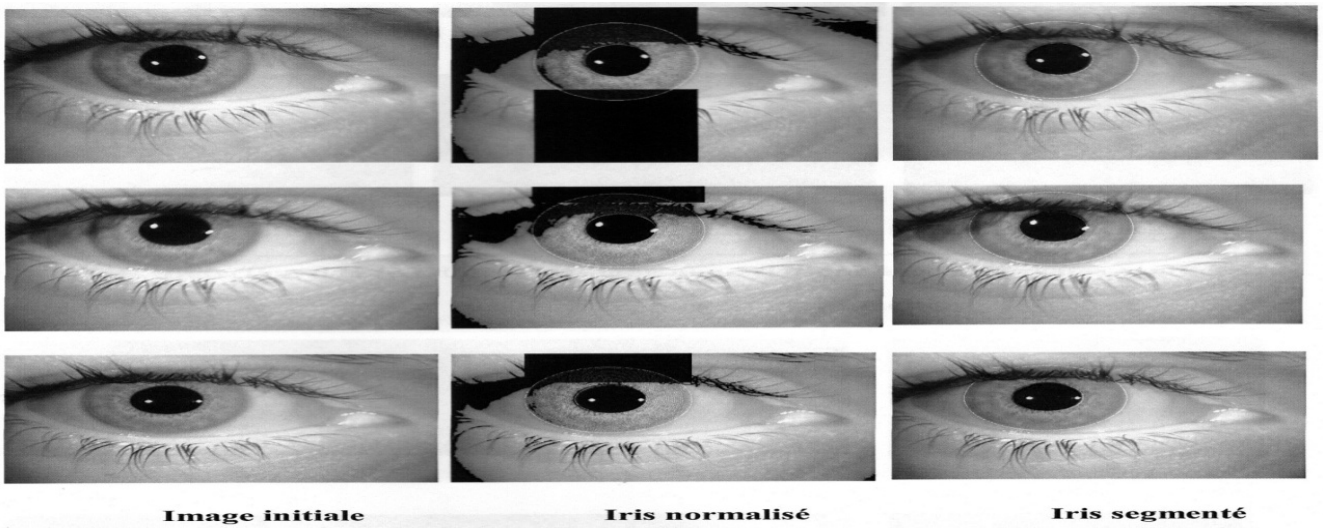


Figure V.14 Détection exacte de l'iris d'une personne non-asiatique avec différentes captures

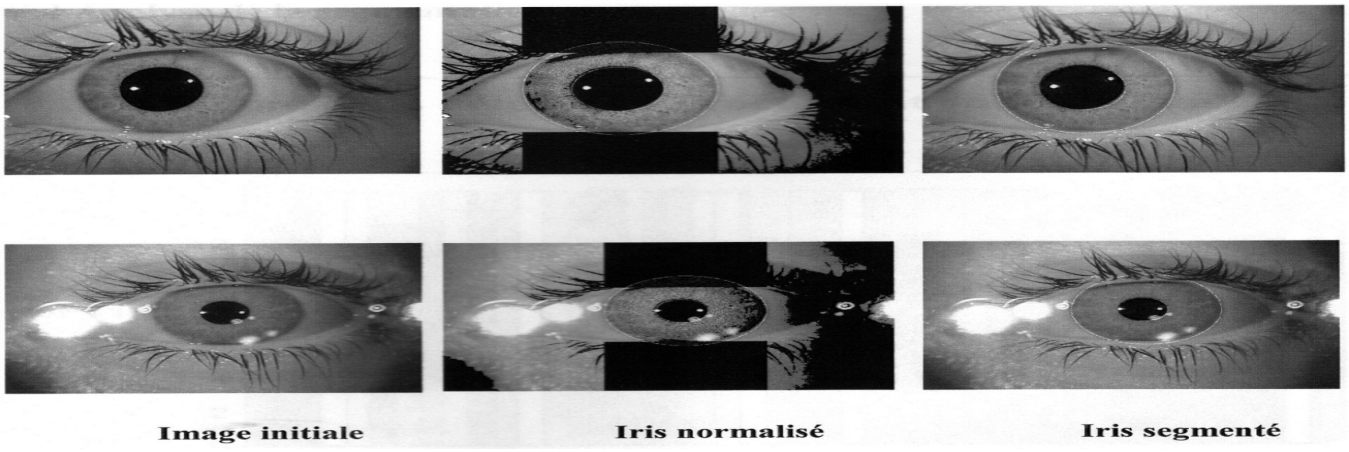


Figure V.15Détection de l'iris d'une personne non-asiatique avec différentes captures.
La 2eme capture est avec lunette.

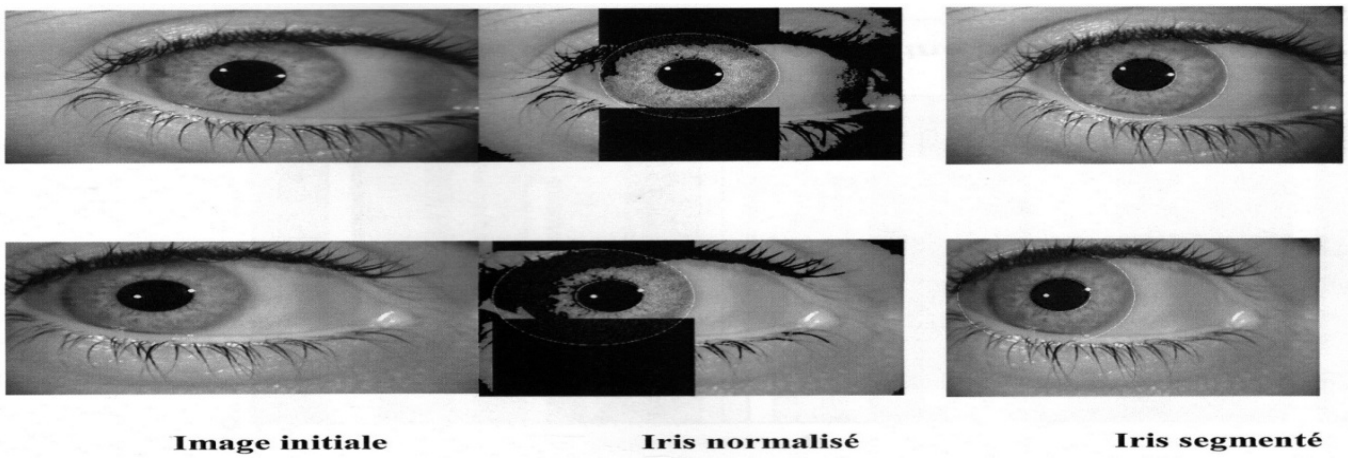
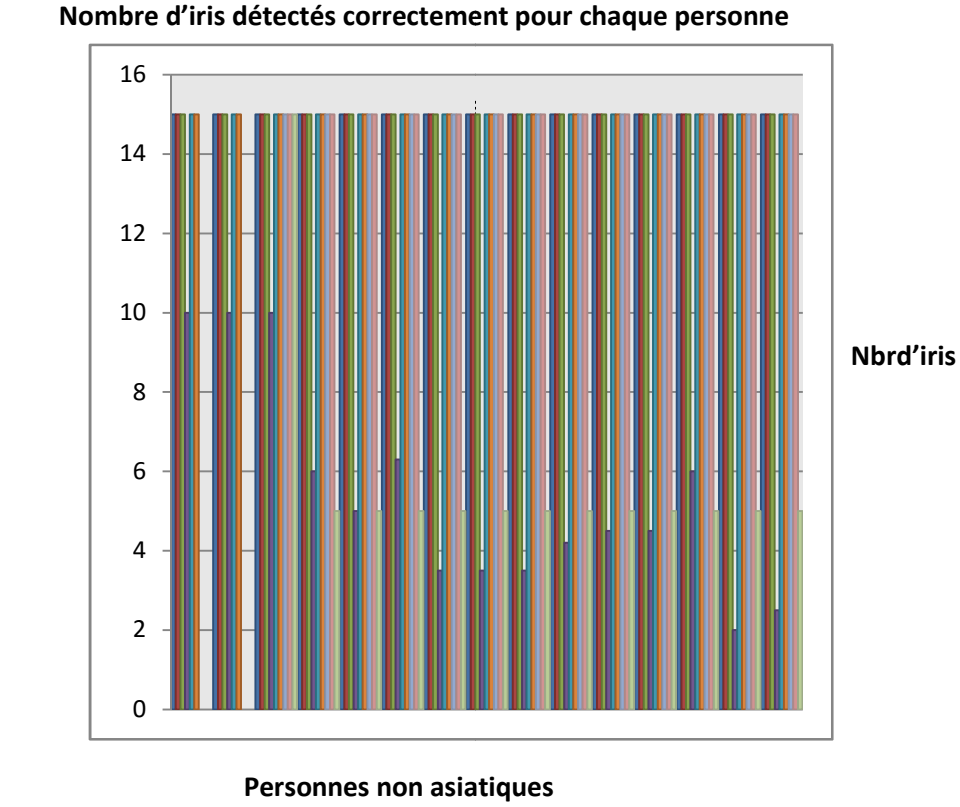


Figure V.16 Détection de l'iris d'une même personne non-asiatique avec une capture de profil.

V.4 Analyse de la segmentation



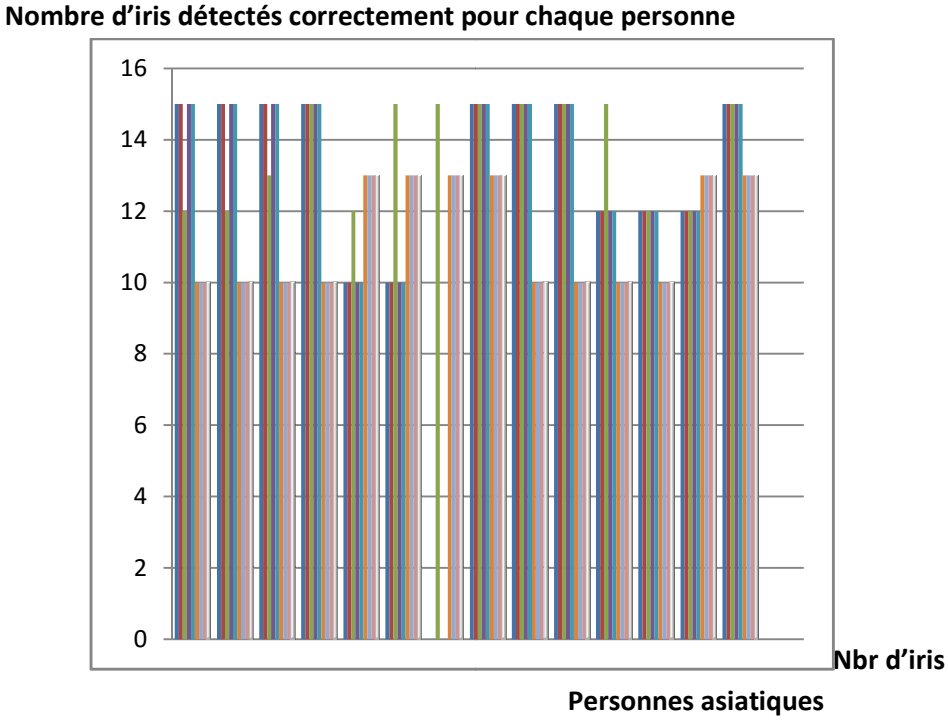


Figure V.17 détection des iris

	Non asiatique	asiatique
Nombre d'iris	356	356
Nombre d'iris détectés	320	185
Taux de détection	89,88%	51,97%
Taux global de détection	70,92%	

Tableau V.1 taux de détection

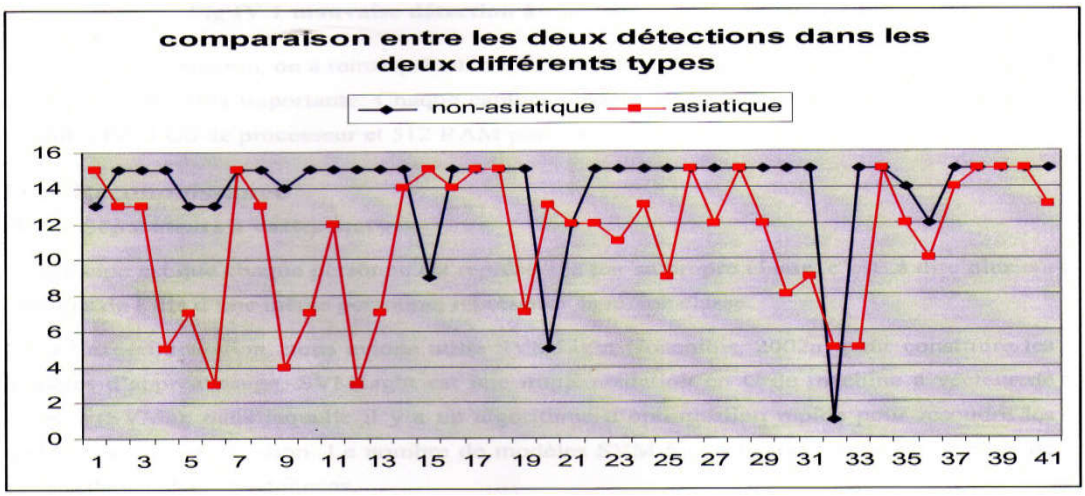


Figure V.18 graphe de comparaison entre les détections

D'après les résultats résumés dans les figures précédentes, le taux de reconnaissance est de 70,92%. Comme nous avons prévu, les résultats sont moins bons dans la partie asiatique.

Dans le graphe précédent, on remarque quelques personnes ayant un taux de détection correct moins de 15 (le nombre total des captures de chaque personne). Cette baisse s'explique que ces personnes portent des lunettes ou parfois elles sont exposées à la lumière.

Figure V.19mauvaise détection à cause de la lumière sur les lunettes.

Durant la segmentation, nous avons remarqué aussi que la transformée de Hough nécessite un temps de calcul et une mémoire importante. Chaque capture a nécessité en moyenne de 3 à 5 minutes pour définir les frontières de chaque iris.

2. Calcul de la distance de l'iris avec d'autres iris.

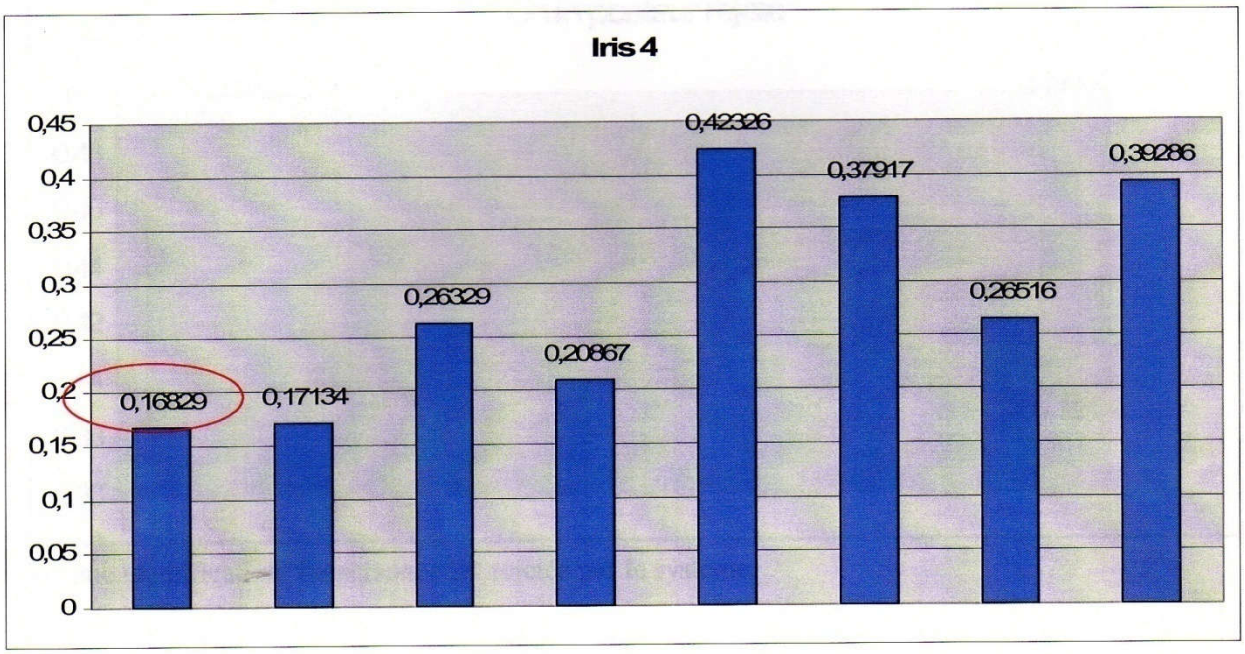


Figure V.20 distance de l'iris avec d'autres iris

La distance la plus petite est 0.16829, personne identifiée.

Exemple d'une acceptation d'un imposteur

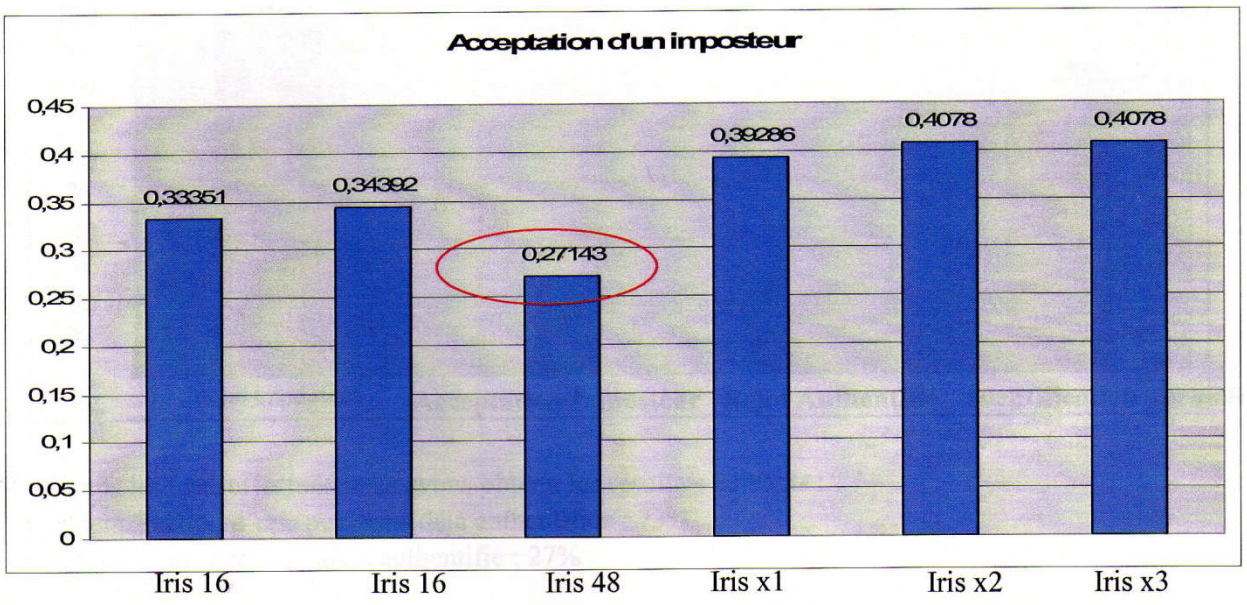


Figure V.21 acceptation d'un imposteur

La distance la plus petite est 0.2714. Dans ce cas, nous avons obtenu une fausse reconnaissance, c'est à dire qu'un imposteur a été identifié autant qu'une personne déjà authentifiée.

Exemple de rejet d'un imposteur

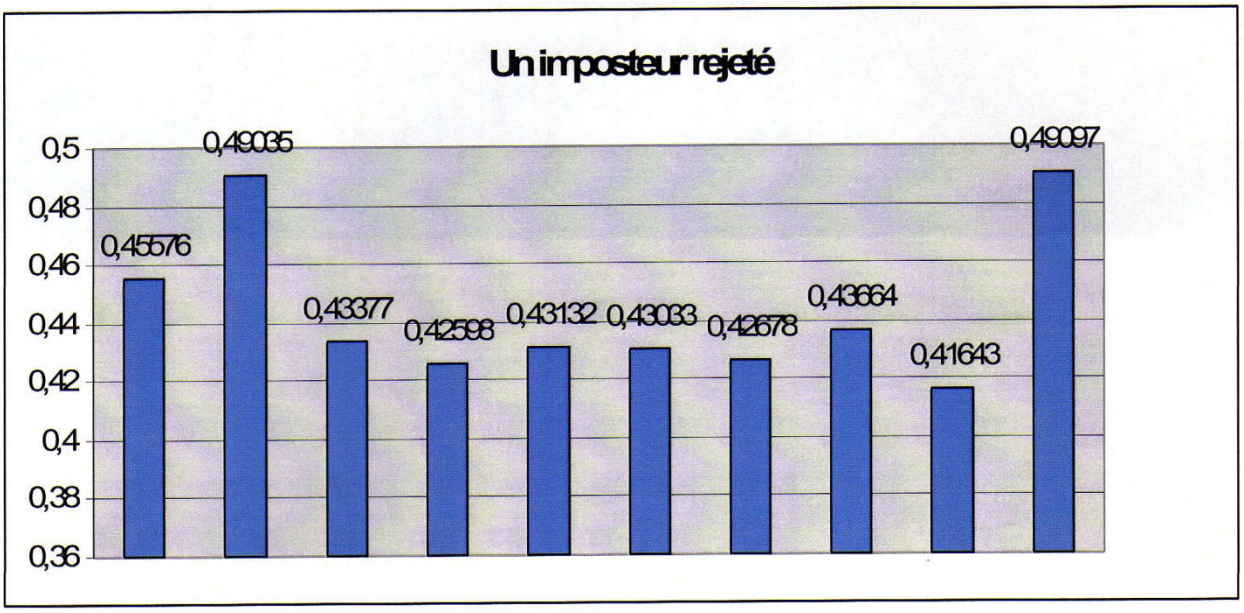


Figure V.22 rejet d'un imposteur

Aucune identification. La personne est rejetée par le système.

V.5 Conclusion

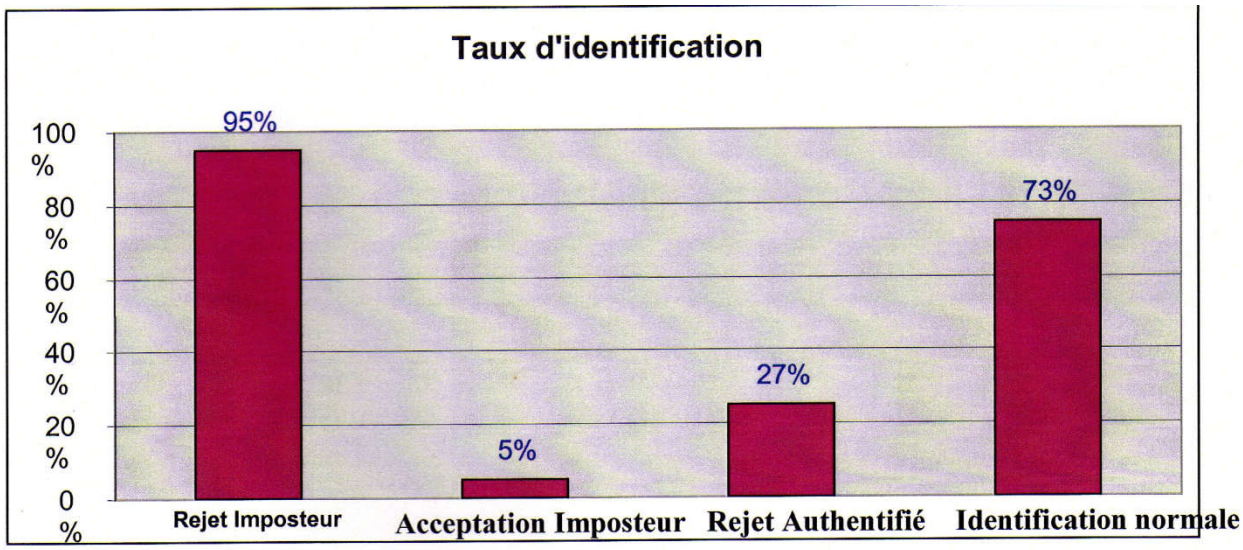


Figure V.23 résultats

D'après les tests effectués nous avons obtenu les résultats suivants :

- Identification d'une personne déjà authentifiée : 73%
- Rejet d'une personne déjà authentifié : 27%
- Rejet d'un imposteur : 95%
- Acceptation d'un imposteur: 5%

Bien que certaines des limites de la biométrie puissent être surmontées avec l'évolution de la technologie et une conception soignée des systèmes, il est important de comprendre qu'un système de reconnaissance totalement immunisé contre l'usurpation d'identité n'existe pas et n'existera certainement jamais

B- Identification des empreintes digitales :

V.6.base de données :

Nous avons opté pour 4 bases de données DBi (i≤4) de la base FVC2002 (moins contraignante que celle de FVC2004). Le mode d'acquisition est en infrarouge en forme bitmap.

Ces bases DBi sont des benchmarks pour tester des capteurs. (Tableau V.3)

	Type de capteur	Taille image	Résolution
DB1	Capteur optiqueTouchView II du Identix.	388x374	500 dpi
DB2	Capteur optiqueFX2000 du Biometrika	296x560	569 dpi
DB3	Capteur capacitif 100 SC du Precise Biometrics.	300x300	500 dpi
DB4	SFingGe v2.51générateur des empreintes digitales synthétiques	288x384	500 dpi

Tableau V.4 : Les bases de données FVC2002 avec leurs capteurs respectifs.

Les 4 bases sont formées chacune de 800 images d'empreintes digitales déterminées par 100 doigts distincts avec 8 images pour chaque doigt. Les bases de données sont formées de la manière suivante (figure V25) :

- les individus étaient demandés de mettre le doigt légèrement dans des positions verticales différentes (DB1 et DB2) et d'altérer des pressures basses et hautes sur la surfaces du capteur (DB3 et DB4).
- les individus étaient demandés d'exagérer une distorsion de la peau (DB1 et DB2) et une rotation du doigt (DB3 et DB4).
- les doigts étaient mouillés (DB1 et DB2) et séchés (DB3 et DB4).

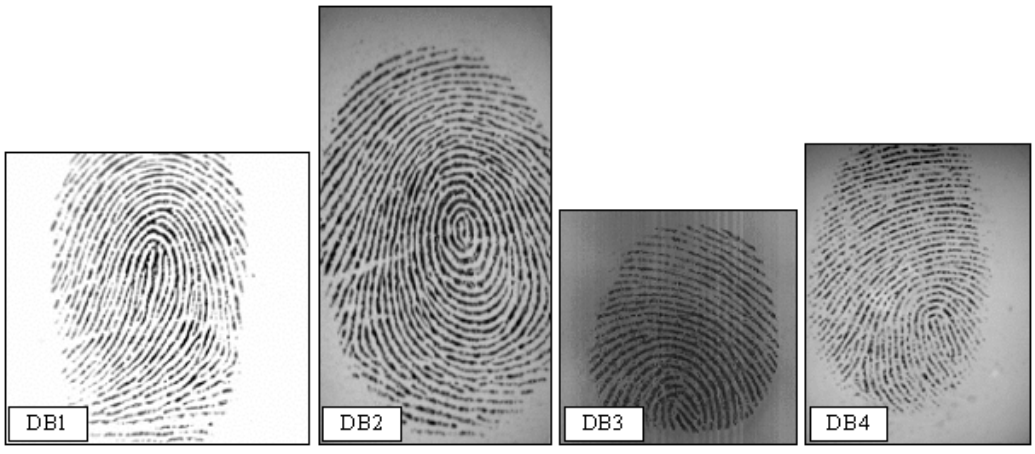


Figure V.25 : Exemple d'empreintes digitales de la base FVC2002.

Pour des raisons pratiques nous sommes limités à un nombre de 210 images comportant 30 classes d'empreinte différentes, chaque classe étant composée de 7 images.

V.7 Prétraitement

Cette étape a pour but ,l'amélioration de la qualité de l'image.En effet , elle vise à uniformiser les contrastes ; à éliminer le problème d'encre et à rectifier l'image quand le doigt est gras .Ces défauts influent sur les algorithmes de reconnaissance des empreintes digitales

Parmi les outils d'amélioration de la qualité de l'image ; on trouve :

V.7.1 Le Filtre gaussien

Le filtre gaussien est un filtre de traitement d'image appliqué par convolution (il utlise un masque(matrice) appliqué à chaque pixel)

Ce type de filtre est utilisé pour diminuer le bruit ou appliquer un flou sur une image et donner par conséquent un bon lissage .

La fonction gaussienne 2D est donnée par la formule (V.4).

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}} \qquad \text{(V.4)}$$

Où σ est l'écart type de la gaussienne

- Si σ est plus petit qu'un pixel le lissage n'a presque pas d'effet.
- Plus σ est grand, plus on réduit le bruit, mais plus l'image filtrée et floue.
- Si σ est choisi très grand, tous les détails de l'image sont perdus.

V.7.2 Détermination du point core par la méthode de l'index de Poincaré

Le principe de la méthode consiste à détecter le point core dans une empreinte digitale, pratiquement, il correspond au centre de l'empreinte digitale. Une région circulaire autour du point core est localisée et segmetée en 64 secteurs. Les intensités des pixels sont normalisées à une moyenne et une variance constantes. La region circulaire est filtrée en utilisant une banque de 8 filtres de Gabor pour avoir un ensemble de 8 images filtrées.

Une méthode très connue a été utilisée pour détecter le point core, c'est la méthode de l'index de Poincaré

Algorithme de l'index de Poincaré

1. Estimer le champs d'orientation *O* en utilisant l'algorithme d'estimation d'orientation quadratique minimale. Le champ d'orientation *O* est défini comme une image MxN. Où *O(i,j)*represente l'orientation de strie local dans le pixel (i,j). Une image est divisée en bloc wxw non chevauchés et une orientation est definit pour chaque bloc.
2. Initialiser A, une image utilisée pour indiquer le point core.
3. Pour chaque pixel (i,j) dans *O*, claculer l'index de Poincaré et assigner le pixel correspondant dans *A* la valeur 1 si l'index de Poincaré est entre 0,45 et 0,51. L'index de Poincaré dans le pixel (i,j) entouré par une courbe digitale est calculee comme suit :

$$Poincare(i,j) = 1/(2\pi) \sum_{k=0}^{N_p-1} \Delta(k)$$

$$\Delta(k) = \begin{cases} \delta(k) si |\delta(k)| < \pi/2 \\ \pi + \delta(k) si \delta(k) \leq -\pi/2 \\ \pi - \delta(k) autrement \end{cases}$$

$$\delta(k) = \theta\left(x_{(k+1) mod N_p}, y_{(k+1) mod N_p}\right) - \theta(x_k, y_k)$$

Dans notre cas, $N_p$est sélectionné comme 8.

4. Le centre du bloc qui à la valeur 1 est considéré comme le centre de l'empreinte digitale et si plus d'un seul bloc ont la valeur 1, alors calculer le moyenne des cordonnées de ces blocs.

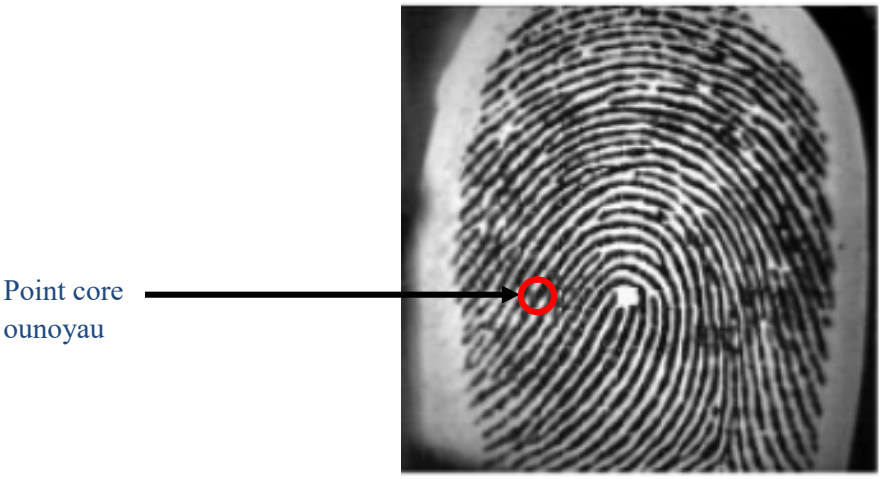


Figure V.26: détermination du point core.

V.7.3 Etape de normalisation

Elle a pour but d'enlever les effets du bruit de capteur.

Une fois le point core est localisé ; nous définissons 4 cercles concentriques d'intervalle égal à vingt pixels est dont le centre est le point core. On divise ensuite les régions en 16 surfaces chacune. La normalisation est L'application définie par :

Pour tout pixel dans une sous-région $S_i, i \in (0,1,2 \ldots .63)$,

$$N_i(x,y) = \begin{cases} M_0 + \sqrt{\frac{V_0 \times (I(x,y)-M_i)^2}{V_i}} \; si I(x,y) > M_i \\ M_0 - \sqrt{\frac{V_0 \times (I(x,y)-M_i)^2}{V_i}} \; sinon \end{cases} \qquad (V.5)$$

Où M_i et V_i sont la moyenne et la variance estimées de la sous-région S_i. M_0 et V_0 sont la moyenne et la variance désirées.

V.7.4 Etape de l'extraction des caractéristiques

Filtrage de l'image par le filtre de Gabor : Le but du filtrage est de sélectionner dans le domaine de Fourier l'ensemble de fréquences qui compose la région à détecter. Ce filtrage peut être effectué avec plusieurs types de filtres entre lesquels on retrouve les filtres de Laws, les filtres en anneau et en coin, les ondelettes et les filtres QMF. L'un des filtres le plus utilisé est le filtre de Gabor. Ce filtre n'est qu'une fréquence pure modulée par une gaussienne, c'est-à-dire, un filtre passe bande avec une enveloppe gaussienne. Ce filtre est très répandu du fait de sa propriété de résolution optimale conjointe en fréquence et en temps. En plus, des études physiologiques sur les mammifères ont montré qu'on peut assimiler le fonctionnement de certains neurones du cortex visuel à ce type de filtre. [SITE7]

Extraction des caractéristiques par le filtre de Gabor : le filtre a pour objectif de réduire la qualité des données et extraire les informations pertinentes. Pour cela le filtre de Gabor est très souvent utilisé car c'est un filtre simple à créer et possède une résolution conjointe spatiale/optimale (c'est-à-dire qu'il est très performant pour sélectionner à la fois une fréquence et l'orientation locale des caractéristiques de l'empreinte digitale (les stries).

Le filtre de Gabor localisé par une fenêtre gaussienne exprimée

$$G(x,y;f,\theta) = exp\left\{-\frac{1}{2}\left[\frac{(xcos\theta)^{'2}}{\delta x^2} + \frac{(ysin\theta)^2}{\delta y^2}\right]\right\}\cos(2\pi f x cos\theta) \qquad (V.6)$$

Où θ est l'orientation du filtre. δ_x et $\delta_y$sont des constantes spatiales de l'enveloppe gaussienne le long des axes x et y respectivement.

Le choix de la fréquence f de Gabor est très important : la qualité de l'image finale dépend directement du bon choix de ce paramètre. En effet si f est trop grande souvent considérée comme l'inverse de la moyenne de la distance inter-stries entre différentes personnes d'âges adulte est similaire, une analyse de la base de données permet alors d'estimer f et de fixer définitivement les autres paramètres du filtre. L'avantage de cette considération est de pouvoir calculer les filtres à l'extérieur du système et de gagner en temps de calcul. [23]

Remarque : La distance moyenne inter-stries est approximativement 10 pixels pour une image de 500 dpi [Mun 04]. Par conséquent *f*=1/10.

dans notre travail chaque image d'empreinte digitale déjà traitée dans l'étape précédente sera décrite par une matrice ou à la suite d'un filtrage qui va permettre l'extraction et la construction des descripteurs des points d'intérêts de représentation sous forme d'un vecteur, ces vecteurs sont très robustes et fiables et permettent une représentation claire de l'image en se basant sur son contenu. Donc on utilisera le filtre de Gabor pour filtrer les images qui nous utiliserons dans la base d'apprentissage qui donneront comme résultat des vecteurs à comparer avec les vecteurs tests.

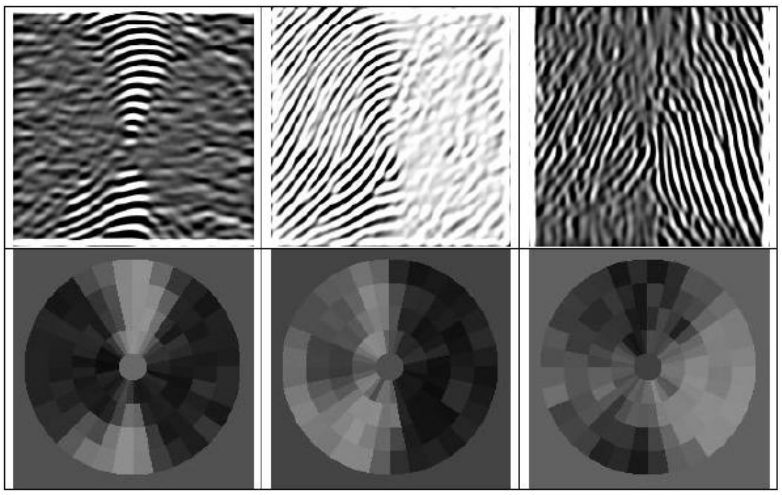


Figure V.27 : Image filtrée et leurs codes vecteurs de caractéristiques pour chaque orientation [Mun 04].

Les valeurs de *θ au nombre de 8 sont :* 0, 22.5, 45, 67.5, 90,112.5, 135 et 157.5 dégrées. Quant aux valeurs de $\delta_x$etδ_y, nous les déterminerons empiriquement et chacune vaut 4.

V.7.5 L'algorithme proposé :

Nous faisons recours à l'un des algorithmes des systèmes immunitaires artificiels AIRS (*A*rtificial*I*mmune *R*ecognition *S*ystem), afin de générer un ensemble de cellules mémoires (cellules B) capable de classifier des nouveaux modèles des individus inconnues (nouveaux antigènes).qui correspondent dans notre cas aux vecteurs caractéristiques de l'iris ou ceux de l'empreinte digitale.

L'algorithme proposé repose sur le fait d'affecter un antigène à une classe de tel sorte qu'il se rapproche le plus des anticorps de cette classe en terme de distance de Hamming; On calcule par la méthode de *Kmeans* , un centroîde pour chaque classe de cellules B qui sera utilisé pour la détermination de l'affinité avec l'antigène à classer et la classe qui donne la plus faible affinité sera la classe cible de cet antigène.

V.7.6 Experiences et résultats

Nous procédons aux expériences de validation de notre modele .Tout d'abord , Une étape d'apprentisage est déclenchée avec 3 images par personne des bases de l'iris et des empreintes digitales chacune (voir tableau V.6) puis pour le test ; avec 04 images par personnes des deux modalités chacune des benchmarks utilisés. Le choix du nombre d'images réduit dans la phase de test n'est pas fortuit. En effet , cela est tiré du principe naturel de vaccination, qui est l'introduction de petite quantité d'antigène.

Nous avons utilisé Matlab 2013 pour la phase d'implémentation

BDD / Phase	CASIA	FVC2002 (DB1,DB2,DB3, DB4)
Apprentissage	3 images/classe	3 images/classe
Test	4 images/classe	4 images/classe

Tableau V.5: Répartition des images entre la phase d'apprentissage et de test.

Afin d'obtenir de bons résultats de classification avec la méthode de l'AIRS, nous devons maitriser le contrôle de certains paramètres comme le taux maximal de clonage, le taux moyen de clonage et la probabilité de mutation. Après plusieurs opérations de tests, nous avons pu voir de bons résultats avec les valeurs ci-dessous :

Paramètres	Ensemble de valeurs	Valeurs
Taux maximal de clonage	Entier	10
Taux moyen de clonage	Entier	20
Probabilité de mutation	Réel∈ [0 1]	0.1

Tableau V.6 : Paramètres d'apprentissage.

Le tableau suivant donne les résultats de la classification que nous avons menée pour les deux signatures proposées.

Base de données	Taux d'apprentissage	Taux de Test
CASIA	100%	97.50%
DB1	100%	75.83%
DB2	98.89%	81.67%
DB3	96.67%	57.50%
DB4	100%	86.67%

Tableau V.7 : Résultat de la classification.

V.8. prise de décision

Les problèmes de la reconnaissance biométrique est un problème de reconnaissance des caractéristiques. Un tel système est un système automatique de prise de décision qui exige:

i- Des données en entrée
ii- Une représentation interne de ces données en utilisant des procédures d'extraction de caractéristiques
iii- Et enfin une décision est prise en se basant sur l'information extraite appelée modèle ou gabarit.

La prise de décision se manifeste généralement sous deux formes distinctes: appariement et classification. Un appariement rejette /accepte l'hypothèse que deux gabarits soient les mêmes. Une classification détermine la classe d'appartenance parmi un nombre de classes prédéterminées

Lors de la phase de prise de décision ; le score obtenu est comparé à un seuil fixé préalablement. Le seuil est donc fixé en fonction du niveau de sécurité souhaité.
La comparaison se fait par les distances séparant chaque vecteur de test de l'ensemble des vecteurs de références. La distance minimale est retenue et comparée à la valeur du seuil pour décider si oui ou non le vecteur est bien classé.

V.9. Tests et Résultats :

La figure suivante représente le taux d'identification en fonction des rangs ou individus.

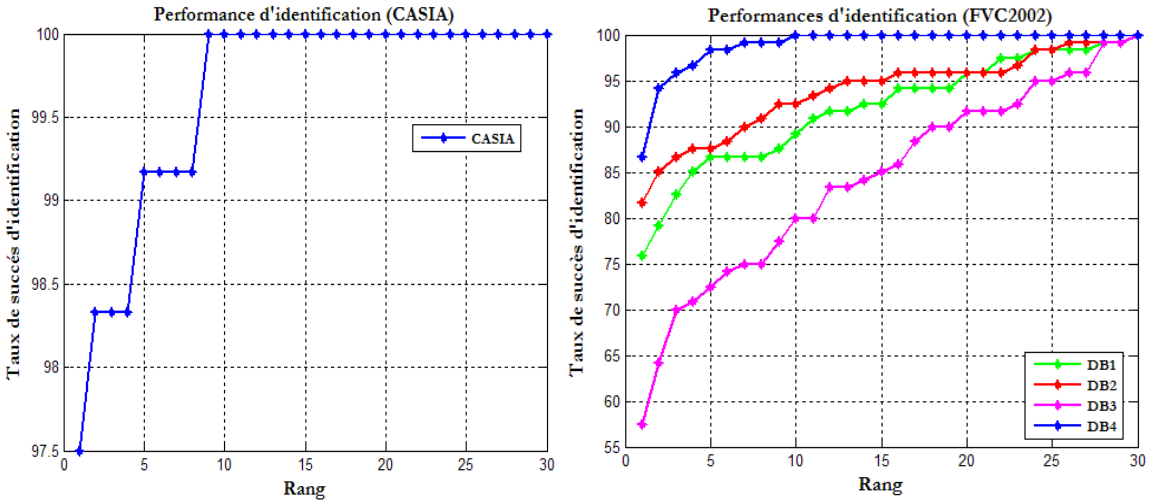


Figure V.28 : Les taux d'identification de l'iris et de l'empreinte digitale

Les courbes de la figure V.28 montrent que le système d'identification de l'iris est plus performant que le système d'identification de l'empreinte digitale.

Les résultats sont résumés dans le tableau suivant :

	la base CASIA	la base DB1	la base DB2	la base DB3	la base DB4
le taux de succès d'identification	97.50%	75.83%	81.67%	57.50%	86.67%

Tableau V.8 : les taux de succès d'identification

V .I0 Fusion des modalités :

Il s'agit de comparer la fusion des modalités (iris et empreinte digitale) et leurs performances avec les performances des systèmes de fusion. L'étude bibliographique montre que plus le niveau de fusion est bas, plus les performances sont bonnes [Gov 04] [Rat 07]. Dans notre cas, la fusion des performances des données se fait au niveau des scores de correspondance issus des deux systèmes d'identification.

V.10.1 Bases de données biométriques multimodales :

L'implémentation de notre approche nécessite la création d'un corpus multimodal que nous avons utilisé dans nos expériences. On doit créer une base de données multimodale à N individus virtuels. On notera la difficulté de trouver des bases multimodales réelles.

A partir des bases de données précédentes ; on a pu élaborer un corpus de 30 individus. Les modalités de chaque individu sont prises indépendamment. Nos bases de données référentielles sont donc : DB1-CASIA, DB2-CASIA, DB3-CASIA et DB4-CASIA

V.10.2 Fusion :

Le processus de fusion biométrique est effectué au niveau des scores pour les deux modalités et avec le classificateur AIS. Nous verrons dans la figure V.29 ; le schéma directeur de fusion des scores.

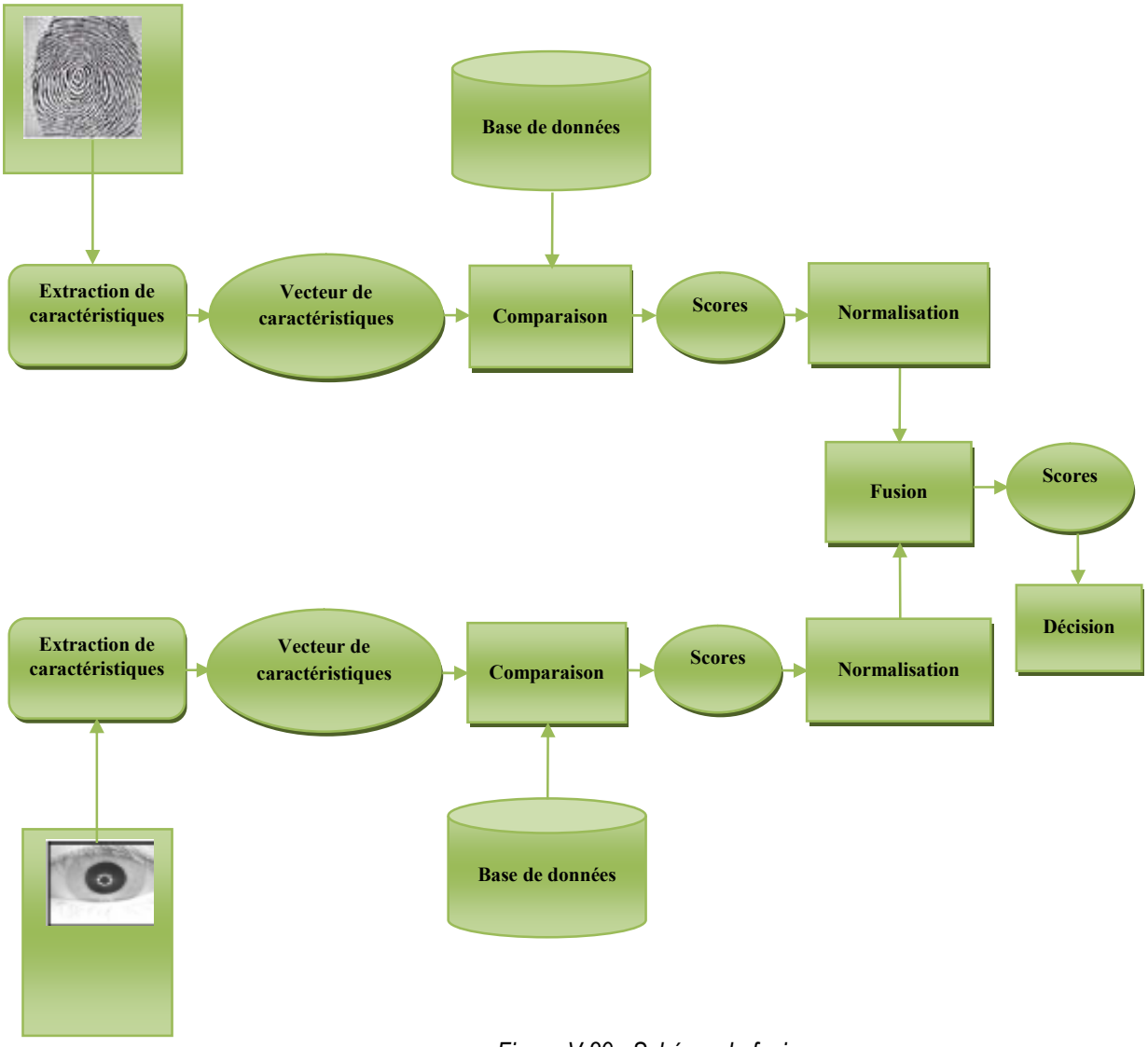


Figure V.29 : Schéma de fusion

V.10.3 Normalisation :

La normalisation des scores a pour but de transformer les scores de chaque signature pour les rendre homogènes avant de les combiner. En effet les scores provenant de chaque système peuvent être de nature différente (scores de similarité, scores de distances ….)

Les différentes techniques de normalisation de scores sont : [ANT99]

- Normalisation par la méthode Min- Max ;
- Normalisation par une fonction quadratique-linéaire-quadratique (QLQ);
- Normalisation par la méthode Z-score ;
- Normalisation par la médiane et l'écart absolu médian (MAD) ;
- Normalisation par la méthode tangente hyperbolique Tanh ;
- Normalisation par une fonction double sigmoïde.

Nous optons dans nos expériences, pour les techniques de normalisation de scores suivantes: Min-Max, Z-score et Tanh .On procèdera à l'addition des scores comme règle de fusion.

L'opération de normalisation des scores par les techniques choisies sur les quatre bases de données multimodales a donné les résultats résumés dans le tableau V.

Technique de normalisation	DB1_CASIA	DB2_CASIA	DB3_CASIA	DB4_CASIA
Min-Max	96.67%	100%	95.83%	99.17%
Z-score	96.23%	99.17%	95,12%	97%
Tanh	96.67%	99.36%	95%	98%

Tableau V.7 : comparaison des trois techniques de normalisation des scores choisies sur les 4 bases de données virtuelles

.

Nous remarquons que la technique de normalisation Min-Max offre des résultats relativement meilleurs que celles des autres techniques.

V.10.4 Les approches de fusion :

Nous choisissons comme méthode de fusion des scores, l'approche de combinaison de scores (méthode plus perforante que l'approche de classification [ANT99]). Les opérations de fusion à considérer sont maximum, somme, produit, moyenne et la somme pondérée (par le poids p pour l'iris et 1-p pour les empreintes digitales).La technique de normalisation étant Min-Max

Méthodes de fusion des scores	DB1-CASIA	DB2-CASIA	DB3-CASIA	DB4-CASIA
Maximum	87.50%	94.17%	88.33%	96.67%
Produit	94.17%	95.83%	90%	95.83%
Somme	96.67%	100%	95.83%	99.17%
Moyenne	96.67%	100%	95.83%	99.17%
Somme pondérée	99.17% w_1^*=0.62	100% w_1^*=0.44	98.33% w_1^*=0.66	99.17% w_1^*=0.38

Tableau V.8 : le taux de succès de l'identification des différents corpus de test pour les techniques de fusion des scores.

Au vu des résultats résumés dans le tableau V.11, nous constatons que la somme pondérée donne de meilleurs résultats

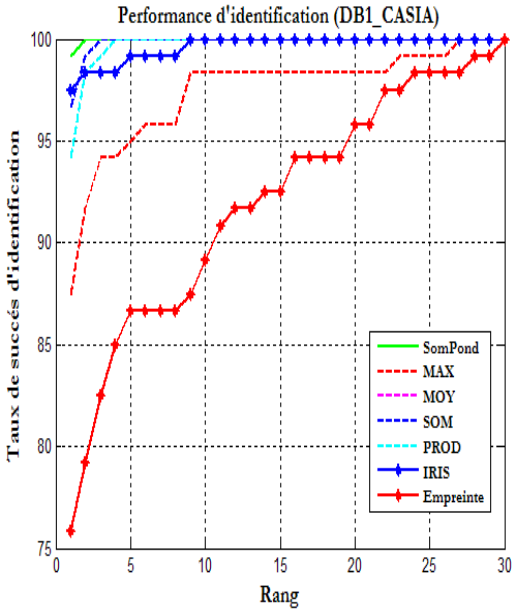


Figure V.30 : Courbes CMS pour les différentes méthodes de fusion des scores(DB1_CASIA).

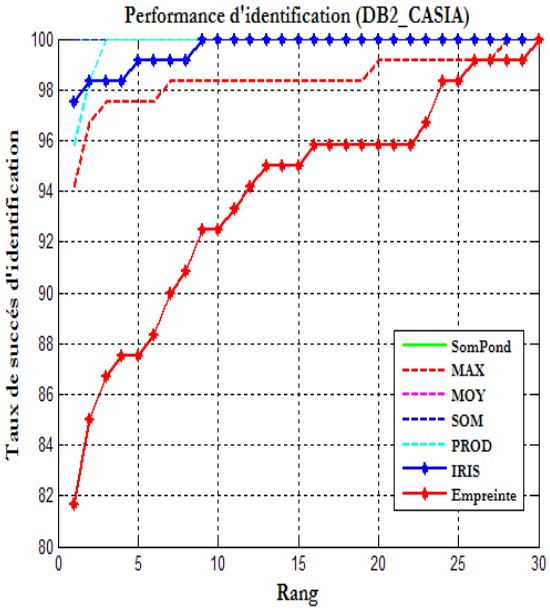


Figure V.31 : Courbes CMS pour les différentes méthodes de fusion des scores(DB2_CASIA).

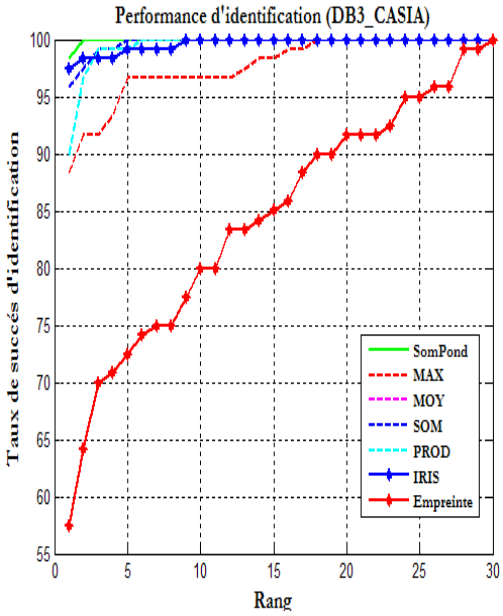


Figure V.32 : Courbes CMS pour les différentes méthodes de fusion des scores(DB3_CASIA).

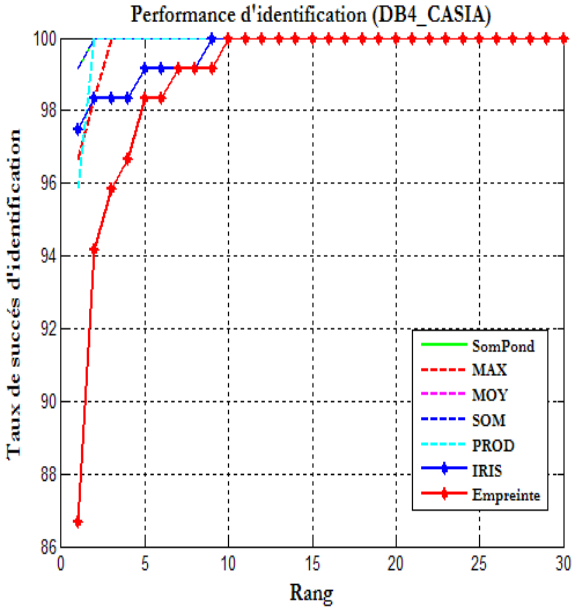


Figure V.33 : Courbes CMS pour les différentes méthodes de fusion des scores(DB4_CASIA).

Commentaires : les résultats résumés dans les figures précédentes montrent que les opérations de fusion : sommation, moyenne et la somme pondérée donnent des résultats satisfaisants .En revanche, le taux de succès d'identification de l'opération produit reste invariant dans les 4 multimodalités DBi-CASIA. D'autre part la qualité des résultats décroit pour la méthode maximum dans les trois corpus DBi ; i=1, 2,3.

Comparaison des systèmes (unimodal et multimodal) : Les résultats de l'identification des systèmes monomodaux (iris et empreinte digitale) et le système multimodal sont représentés par les courbes CMS suivantes :

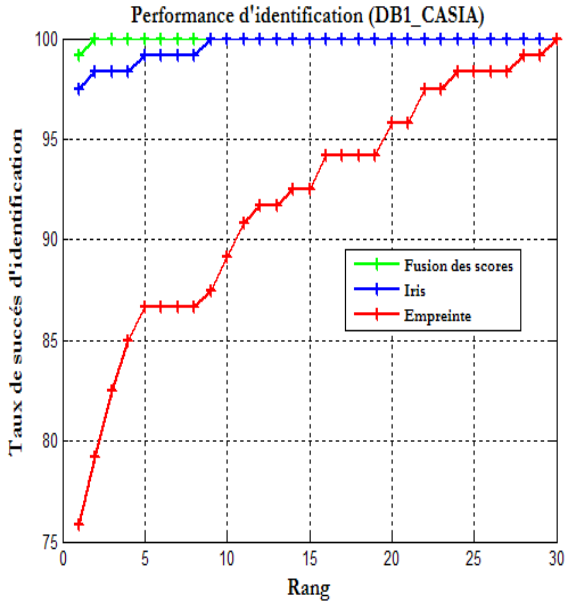


Figure V.34 : Courbes CMS pour les différents systèmes d'identification (DB1_CASIA).

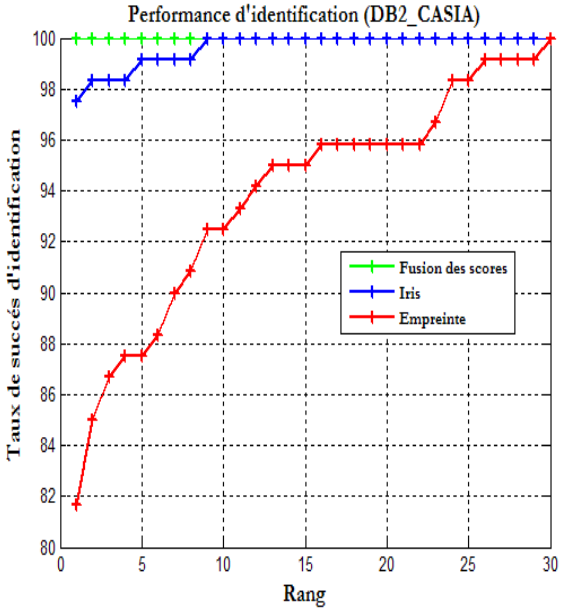


Figure V.35 : Courbes CMS pour les différents systèmes d'identification (DB2_CASIA).

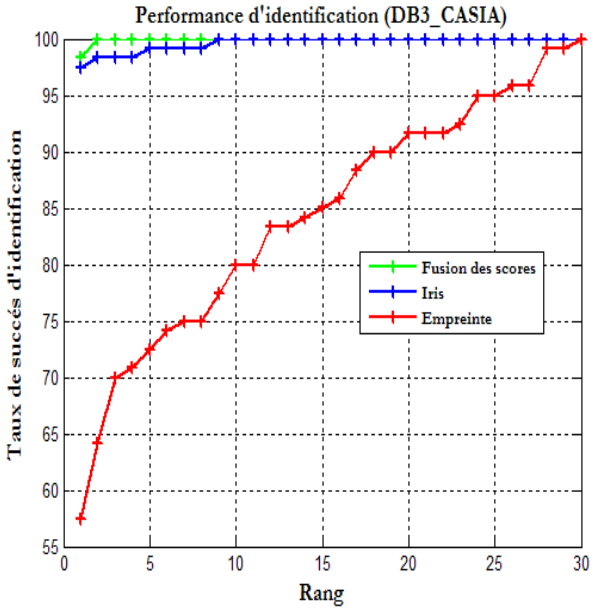


Figure V.36 : Courbes CMS pour les différents systèmes d'identification (DB3_CASIA).

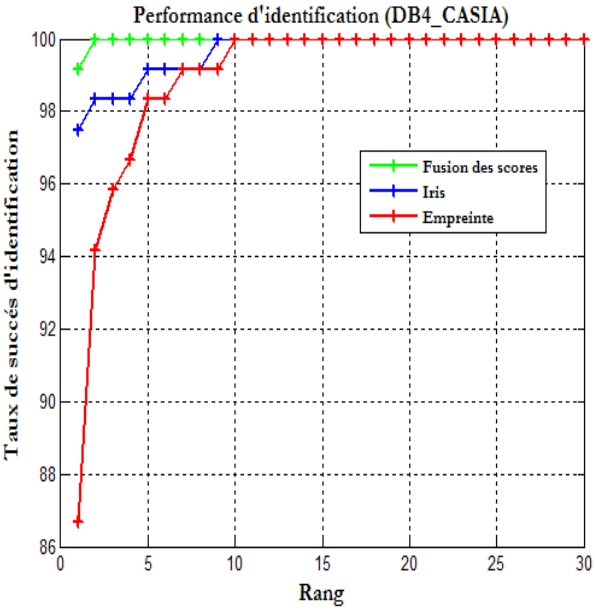


Figure V.37 : Courbes CMS pour les différents systèmes d'identification DB4_ASIA

V.11. Conclusion :

Nous avons appliqué la méthode de l'AIRS pour l'identification des modalités iris et empreintes digitales .Cette technique de l'intelligence artificielle a montré une fois de plus son efficacité.

Cependant, Les différentes étapes du système proposé nous obligent à prendre en considération les inconvénients de chaque opération comme l'omission des données au cours de l'extraction des paramètres pertinents, la position des doigts et leurs états, les différents capteurs utilisés pour la prise de l'image ,…

Enfin, nous remarquons à travers les expériences effectuées, que la fusion au niveau des scores des modalités de l'iris et des empreintes digitales donne un système bimodal performant comparé aux systèmes unimodaux.

CONCLUSION GENERALE

CONCLUSION GENERALE

Bien que les techniques de reconnaissance biométrique promettent d'être très performantes, on ne peut garantir actuellement un excellent taux de reconnaissance avec des systèmes biométriques unimodaux, basés sur une unique modalité biométrique. C'est pour cette raison que les systèmes multimodaux ont gagné une place importante dans différents domaines, notamment dans la reconnaissance des individus qui est de plus en plus présente pour accéder à certains endroits privés.

Dans cette thèse, nous avons mis en place un procédé biométrique bimodal pour l'identification des individus. Ce procédé est une fusion des scores de l'iris et des empreintes digitales.
Pour arriver à notre but, nous avons procédé de la manière suivante :

Après avoir décrit les technologies utilisées dans les systèmes biométriques pour l'identification des personnes et montré les différentes modalités biométriques tout en soulignant les avantages et les inconvénients de chacune. Nous avons constaté que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre. Pour palier à tous ces problèmes, nous avons conclu qu'il fallait combiner des modalités pour avoir des résultats plus fiables.

Ainsi, nous avons présenté la biométrie multimodale et présenté les différents types de combinaisons de modalités possibles, mais aussi les architectures et les niveaux de fusion pouvant être utilisés dans un système multimodal.

Parmi les modalités décrites, nous avons choisi l'iris et les empreintes digitales de part leur fiabilité et l'intérêt de plus en plus grandissant de la communauté scientifique.

Nous avons appliqué la méthode de l'AIRS pour l'identification des modalités iris et empreintes digitales .Cette technique de l'intelligence artificielle a montré une fois de plus son efficacité.

Cependant, Les différentes étapes du système multimodal proposé nous ont obligé à prendre en considération les inconvénients de chaque opération comme l'omission des données au cours de l'extraction des paramètres pertinents, la position des doigts et leurs états, les différents capteurs utilisés pour la prise de l'image ,…

Enfin, nous remarquons à travers les expériences effectuées, que la fusion au niveau des scores des modalités de l'iris et des empreintes digitales donne un système bimodal performant comparé aux systèmes unimodaux pris séparément

REFERENCES BIBLIOGRAPHIQUES

RÉFÉRENCES BIBLIOGRAPHIQUES:

[ABD10] A. Abdelhadi, L.H. Mouss et O. Kadri, “Algorithmes du système immunitaire artificiel pour la surveillance industrielle”, International Conference On Industrial Engineering and Manufacturing ICIEM’10, May, 9-10, Batna, Algeria, 2010.

[ADJ 06] R. Adjoudj, “Authentification Automatique par Identification & Reconnaissance dans un Système de Haute Sécurité”, Thèse de doctorat, université Djilali LIABES de Sidi Bel Abbes, 2006.

[AKR 11] S. Akrouf, “Une Approche Multimodale pour l’Identification du Locuteur”, Thèse de doctorat, université Ferhat Abbas Sétif, 2011.

[ALI 10] M. Alipoor, H. Ahopay et J. Haddadnia, “A Novel High Performance Iris and Pupil Localization Method”, IEEE, 2010.

[ALL 09] L. Allano, “La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles”, Thèse de doctorat, université d’Evry Val d’Essonne

[ANI00] Anil Jain et al.,"Automated Fingerprint Identification and imaging " Pattern Recognition. Vol. 11, N°.7, pp. 150–167, December 2000.

[ANT99] Anthony Lum,"Fingerprint Recognition"Pattern Recognition. Vol. 05, N° 2, pp. 72–85, June1999

[ALO 12] K. Aloui, “Caractérisation du Cerveau Humain : Étude de la Faisabilité en Biométrie”, Thèse de doctorat, École Nationale d’Ingénieurs de Tunis (ENIT), 2012.

[ARI 05] M. Arif, “Fusion de Données : Ultime Etape de Reconnaissance de Formes, Applications à l’Identification et à l’Authentification”, Thèse de doctorat, Université François Rabelais Tours, 2005.

[AZZ09] H. Azzag“ Un survol des algorithmes pour la classification ”Congrès Francophone de Vision par ordinateur. 2009

[BAI03] J .C Baillie, “Traitement d'Image et Vision Artificielle ”Congrès Francophone de Vision par ordinateur. 2003.

[BEL 06] N. Belguechi, “Contribution a la reconnaissance d’empreintes digitales par une approche hybride”, thèse de magister, Institut national de formation en informatique, 2006.

[BOL 98] W. Boles et B. Boashash, “A human identification technique using images of the iris and wavelet transform” ,IEEE Trans. on Signal Processing, Vol. 46, no. 4, pp. 1185-1188, Apr 1998.

[BEN08] I. Benchennane , A. Serrat , M. Benyettou , “Inverse Kinematic Using Artificial Immune System”, ACIT’2008

[BEN09] I. Benchennane "segmentation et classification des images par les systèmes immunitaires" Mémoire de Magister, Institut National des Télécommunications d’Oran, 2009

[BRU 95] R. Brunelli et D. Falavigna. “Person identification using multiple cues”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 17, pp. 955–966, 1995.

[CHA 09] A. Chaari, “Nouvelle approche d’identification dans les bases de données biométriques basée sur une classification non supervisée”, Thèse de doctorat, Université d’Evry Val d’Essonne, 2009.

[CHA 99] V. Chatzis, A. Bors et I. Pitas, “Multimodal decision-level fusion for person authentication”, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, Vol. 29, no. 6, pp. 674–681, November 1999.

[CHA98] P.A Chastanet,P.Wroblewski.“Performances comparées des filtre de Deriche et de Shen-Castan”. Ecole de télécommunication 1998.

[CHE 97] K. Chen, L. Wang et H. Chi, “Methods of combining multiple classifiers with different features and their applications to text-independent speaker identification”, International Journal of Pattern Recognition and Artificial Intelligence, Vol. 11, No. 3, pp. 417–445, 1997.

[CON 10] V. Conti, C. Militello, F. Sorbello et S. Vitabile, “A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems”, IEEE transaction on systems, man and, and cybernetics – part c: Applications and reviews, Vol. 40, no. 4, July 2010.

[DAU 06] J. Daugman, “Probing the Uniqueness and Randomness of Iris Codes: Results From 200 Billion Iris Pair Comparisons”. In: Proceedings of the IEEE, pp. 1927–1935, November 2006.

[DAU 04] J. Daugman, “How iris recognition works”, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, pp. 21–30, 2004.

[DAU 99] J. Daugman, “Recognizing persons by their iris pattern”, in: A. K. Jain, R. Bolle , S. Pankanti (Eds), Biometric: Personal identification in a Networked Society, Kluwer Academic Publishers, pp. 103-121, 1999.

[DAU 98] J. Daugman, “Combining Multiple Biometrics”, 1998. Available at http://www.cl.cam.ac.uk/~jgd1000/combine/combine.html.

[DAU 95] J. Daugman, “High confidence recognition of persons by rapid video analysis of iris texture”, European Convention on Security and Detection, pp. 244 -251, 16-18 May 1995.

[DAU 94] J. Daugman, “Biometric personal identification system based on iris analysis”, Patent N. 5,291,560 U.S, 1994.

[DAU 93] J. Daugman, “High confidence visual recognition of persons by a test of statistical independence,” IEEE Transactions on Pattern Analysis & Machine Intell., Vol. 15, no. 11, pp. 1148-1161, November 1993.

[DAS 03] D. Dasgupta, Z. Ji et F. Gonzalez, “Artificial Immune System (AIS) Research in the Last Five Years”, IEEE, 2003.

[DAS 99] D. Dasgupta, “Artificial Immune Systems and Their Application”, Springer-Verlag 1999.

[DEC 99] L. N. De Castro et F. J. Von Zuben, “Artificial immune systems: Part I-basic theory and applications”. Technical Report DCA-RT 01-99, School of Computing and Electrical Engineering, State University of Campinas, Brazil.

[DEC 00] L.N. De Castro et F.J. Von Zuben, “The clonal selection algorithm with engineering application” Proc of GECCO00, Workshop Proceeding, 36-37, 2000.

[DEC 01] L.N. De Castro, “An Introduction to the Artificial Immune Systems”, ICANNGA, April, 2001.

[DEV03] J.Devars et M.Milgram, Cours de Traitement d’images, par Catherine Achard, 2002/2003.

[DEN06] A.Deneche, “Approches bio inspirées pour la reconnaissance deFormes”, Mémoire présenté pour l’obtention du diplôme de Magistère en Informatique, Option: Information & Computation, Université Mentouri de Constantine, 2006.

[FON01] M.Fontaine“Segmentation non supervisée d’images couleur par analyse de La connexité des pixels”. Thèse de doctorat, LILLE, 2001.

[FOR10] E.M. Forgey. “Cluster analysis of multivarariate data: efficiency versus Interpretability of classification” International Journal of Computer Applications (0975 – 8887), Vol. 2, N°4, May 2010..

[FOR 96] S. Forrest, S. Hofmeyr, A. Somayaji et T. Longstaff, “A sense of self for Unix processes”, Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy, 120-128, 1996.

[FOR 94] S. Forrest, A. Perelson, L. Allen et R. Cherukuri, “Self-Nonself Discrimination in a computer”, Proc. Of the IEEE Symposium on research in Security and Privacy, pp. 202-212, 1994

[GAR 02] M.D. Garris, C.I. Watson, R.M. McCabe et C.L. Wilson. “Users Guide to Nist Fingerprint Image Software (nfis)”, Technical Report NISTIR 6813, National Institute of Standards and Technology, 2002.

[GEN02] Gendarmerie Royale du Canada, juin 2002, Les technologies biométriques : une évaluation d'applications pratiques

[GOM04] J.F. Gomes Da Costa, “Computational power of killers and helpers in the immune system”, Master en informatique Université de Lisboa, 2004.

[GON92] R.C. Gonzalez et R.E, Woods. “Digital image processing”.Edition -Wesley, 1992.

[GOV 04] A. Ross et R. Govinddarajan, “Feature level fusion using hand and face biometrics”, in proceedings of SPIE Conference on Biometric Technology for Human Identification, pp. 196-204, 2004.

[HAB 12] A. Haboussi, “Systèmes Immunitaires Artificiels pour le diagnostic des systèmes complexes”, thèse de magister, Université Hadj Lakhdar, Batna, Faculté de technologie, Département de génie industriel, 2012

[HAB03] .E. Kahloul&S.Fares. “Segmentation des images 3D ” Mémoire de PFE, USTO, département d'informatique, 2003.

[HAM 86] F. Hampel, P. Rousseeuw, E. Ronchetti et W. Stahel, “Robust Statistics: The Approach Based on Influence Functions”. John Wiley& Sons, 1986

[HEN 13] R. Hentati, “Implémentation d’algorithmes de reconnaissance biométrique par l’iris sur des architectures dédiées”, Thèse de doctorat, Université Evry Val d’Essonne, 2013.

[HO 94] T. Ho, J. Hull et S. Srihari, “DecisionCombination in Multiple Classifier Systems”, IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol. 16, no. 1, pp. 66–75, 1994.

[HOC 07]: S. Hocquet, “Authentification biométrique adaptative Application à la dynamique de frappe et à la signature manuscrite”, Thèse de doctorat, Université François Rabelais Tours, 2007.

[HOF 99] S. Hofmeyr “An immunological model of distributed detection and its application to computer security”, PhD thesis, University of New Mexico, 1999.

[HON 09] T. Hoang Van, H. Thai Le, “Adaptive Noisy Fingerprint Enhancement, Based on Orientation Consistency”, International Conference on Knowledge and Systems Engineering, 2009.

[JAI 05] A.K. Jain, K. Nandakumar et A. Ross, “Score normalization in multimodal biometric systems”. Pattern Recognition. Vol. 38, no. 12, pp. 2270–2285, December 2005.

[JAI 97] A.K. Jain, L. Hong, S. Pankanti et R. Bolle, “An identity authentication system using fingerprints”. Proceedings of the IEEE, Vol. 85, issue 9, pp. 1365-1388, 1997.

[JER 74] N. Jerne, “Towards a network theory of the immune system”, Annals of Immunology, (Inst. Pasteur), 125C, pp. 373–389, 1974.

[KIM 01] J. Kim, “Integrating Artificial Immune Algorithms for Intrusion Detection”, PhD Thesis, University College London, 2002.

[KHE 08] H. Khelil, A. Benyettou et A. Belaïd, “Application du système immunitaire artificiel pour la reconnaissance des chiffres”, MaghrebianConference on Software Engineering and Artificial Intelligence, April 28-30, Oran, Algeria, 2008.

[KOM 05] P. Komarinski, P.T. Higgins, K.M. Higgins et K. Fox Lisa, “Automated Fingerprint Identification Systems (AFIS)”, Elsevier Academic Press, pp. 1-118, 2005.

[KRI 07] E. Krichen, “Reconnaissance des personnes par l'iris en mode grade”, Thèse de doctorat, Institut National des Télécommunications, Paris, 4 octobre 2007.

[LAB 06] I. Labe, “Proposition d’un système immunitaire artificiel pour la détection d’intrusions”, Thèse de magister, Université Mentouri, Constantine, Faculté des sciences de l’ingénieur, département d’informatique, 2006.

[LEM 12] R. Lemouchi, “La Reconnaissance de l’iris basée sur l’orientation locale du signal monogène”, Mémoire de magister, Ecole nationale supérieure d’informatique, 2012.

[LIM 01] S. Lim, K. Lee, O. Byeon et T. Kim, “Efficient Iris Recognition through Improvement of Feature Vector and Classifier”, ETRI Journal, Vol. 23, no. 2, pp. 61–70, 2001.

[LIN97] Lin Hong et al." An identification system using fingerprints"Proceedings of the IEEE, Vol. 45, issue 3, pp. 1121-1145, 1997.

[LYD02] P.Lyddyard, Alex WHELAN et Michael FANGER “L’essentiel en immunologie", Port Royal Livres, 2002, Paris. BERTI Editions.

[LYE 95] S. Lyengar, L. Prasad et H. Min, “Advances in DistributedSensorTechnology”, 1995

[MA 02] L. Ma, Y. Wang et T. Tan. “Iris recognition using circular symmetric filters”, In: Proceedings of the 16th International Conference on Pattern Recognition, pp. 414–417, 2002.

[MAL03] D. Maltoni, D. Maio, Anil k. Salil Prabhakar, 2003, Fingerprint Handbook

[MAX02] Max Chasse- Juillet 2002, La biométrie au Québec : Les enjeux

[MIS 13] P. Mishra, A.K. Shrivastava, A. Saxena, “Enhanced Thinning Based FingerPrint Recognition”, International Journal on

Cybernetics & Informatics (IJCI), Vol.2, no.2, April 2013.

[MAI 97] D. Maio, D. Maltoni, “Direct Grey -Scale Minutiae Detection in Fingerprints”, IEEE Trans. Pattern Anal. Machin Intell., Vol. 19, no. 1, pp. 27-40, 1997.

[MOR 09] N. Morizet, “Reconnaissance Biométrique par Fusion Multimodale du Visage et de l’Iris”, Ecole Nationale Supérieure des Télécommunications, 2009.

[MUN 04] M.U. Munir et M.Y. Javed, “Fingerprint Matching using Gabor filters”, college of electronical and mechanical engineering, national university of sciences and technology Rawalpindi, Pakistan, 2004.

[MUR 00] A. Muron et J. Pospisil, “The human iris structure and its usages”, Acta Univ. Palacki, Phisica, Vol. 39, pages 87-95, Mars 2000.

[NAN 04] K. Nandakumar, A.K. Jain, “Local correlation-based fingerprint matching”, Indian Conference on Computer Vision, Graphics and Image Processing, pp. 503–508, 2004.

[OUA06] S. Ouadfel. “Contributions à la Segmentation d’images basées sur la résolution collective par colonies de fourmis artificielles ”, Thèse de doctorat, Batna, 2005-2006.

[OPP81] A. Oppenheim et J. Lim, “The importance of phase in signals”, Proceedings of the IEEE 69, 529-541, 1981.

[PRA 99] S. Prabhakar, A. Jain, L. Hong et S. Pankanti, “FingerCode: A Filterbank for Fingerprint Representation and Matching”, 1999.

[PET80] “Petit Larousse", dictionnaire encyclopédique pour tous, librairie Lar, Paris, 1980.

[Cas02] L. N. de Castro and J. Timmis, ” Artificial Immune System, A new computationalintelligence Approch ”, ISBN 1-85233-594-7, Edition Springer, 2002.

[RAJ 10] M. Rajinikannan, D.A. Kumar et R. Muthuraj, “Estimating the Impact of Fingerprint Image Enhancement Algorithms for Better Minutia Detection”, International Journal of Computer Applications (0975 – 8887),Vol. 2, no.1, May 2010.

[RAT 07] A. Rattani, D.R. Kisku, M. Bicego et M. Tistarelli, “Feature level fusion of face and fingerprint biometrics”, in of first IEEE International conference on biometrics: Theory, Applications and systems (BTAS-07), pp. 1-6, 2007.

[RAT 04] N. Ratha et R. Bolle, “Automatic Fingerprint Recognition Systems”, Springer-Verlag, ISBN# 0-387-95593-3, New York, Inc, USA, 2004.

[RED 06] R. Roujani, “Reconnaissance de visages”, Mémoire pour l’obtention du diplôme des études approfondies. Université Mohamed V – Agdal, Novembre 2006.

[RIM98] S.Rimmer, Les Bitmap, traduit de l’américain par François Pecheux, Cambridge UniversityPress, 1998.

[REV01] J.P. Revillard, “Immunologie ”, université De Bœck, 4 éme édition, page 137-151,2001.

[ROI 90] Roitt, “Immunologie”, Editions Pradel, 1990.

[ROS 11] E .VanajaRoselin, L.M. Waghmare et E.R.Chirchi, “Iris Biometric Recognition for Person Identification in Security Systems”, International Journal of Computer Applications (0975 8887), Vol. 24, no.9, June 2011.

[ROS 06] A. Ross, K. Nandakumar et A. Jain, “Handbook of Multibiometrics”. Springer-Verlag New York, Inc., 2006.

[ROS 03] A. Ross et A. Jain, “Information fusion in biometrics”. Pattern Recognition Letters, Vol. 24, no. 13, pp. 2115–2125, 2003.

[ROS 02] A.K. Jain et A. Ross, “Fingerprint Mosaicking”, IEEE Intentional Conference on ICASSP, Vol. 4, May 2002.

[RYD 04] E. Rydgren, T. Ea, F. Amiel, F. Rossant et A. Amara, “Iris features extraction usingwaveletpackets”. International Conference on Image Processing (ICIP), Vol. 2, pp. 861–864, October 2004.

[SAI 11] M. Saidi, “Traitement de données médicales par un système immunitaire artificiel : Reconnaissance Automatique du Diabète”, thèse de magister, université AboubakrBelkaid–Tlemcen, 2011.

[SAM 12] Y. Samai, “Reconnaissance de l’Iris humain en utilisant les méthodes de l’Intelligence Artificielle”, thèse de Magister, Université el Hadj Lakhdar, Batna, Faculté de Technologie, Département d’électronique, 2012.

[SAN 02] C. Sanderson et K. Paliwal, “Information fusion and person verification using speech and face information”, Tech.

Rep. IDIAP-RR 02-33, IDAIP, September 2002.

[SEO 02] B.C. Seow, S.K. Yeoh, S.L. Lai et N.A. Abu, “Image Based Fingerprint Verification”, Student Conference on Reseach and Development Proceedings, Malaysia, 2002.

[SHE 94] B.G. Sherlok, D.M. Monro et K. Millard, “Fingerprint Enhancement By Directional Fourier Filtering”, IEEE Proc. Vis. Image Signal Process, Vol. 141, no. 2, pp. 87-94, April 1994.

[SMI 93] R.E. Smith, S. Forrest et A.S. Perelson, “Searching for diverse, cooperative populations with genetic algorithms”. Evolutionary computation, Vol. 1, no. 2, pp. 127–149, 1993.

[SOM 00] A. Somayaji et S. Forrest, “Automated response using system-call delays”, Proceedings of the ninth USENIX Security Symposium, pp. 185-197, 2000.

[TIM 04] J. Timmis, T. Knight, L.N. De Castro et E.Hart, “An overview of Artificial immune Systems”, Natural computation series, pp. 51-86, Springer, 2004.

[TIM 03] J. Timmis et L.N. De Castro, “Artificial Immune System as a novel Soft Computing Paradigm”, Soft Computing Journal, Vol. 7, issue 7, July 2003.

[TIM 02] J. Timmis et L.N. De Castro, “Artificial immune Systems: A New computational Intelligence Approach”, Springer-Verglas, London, 2002.

[TIM 01] J. Timmis, “Artificial Immune Systems: A novel data analysis technique inspired by the immune network theory”, PhD Thesis, University of Wales, 2001.

[TIS 03] C. L. Tisse, “Contribution à la Vérification Biométrique de Personnes par Reconnaissance de l'Iris”, Montpellier, 2003.

[TIS 02] M. L. Tisse, C.-L., L. Torres et M. Robert, “Person identification technique usinghuman iris recognition”. In: Proceedings of Vision Interface, pp. 294–299, 2002.

[TON 07] W. Tong et H. Pi-Lian, “A Hidden Markov Model For Iris Recognition Method”, 2007 IEEE International Conference on Control and Automation. Guangzhou, CHINA - May 30 to June 1, 2007.

[TOU 04] H. Touati et N. Adlene, “Identification des empreintes digitales”, Mémoire de fin d’études, Ecole Militaire polytechnique, Alger, 2004.

[VAN03] P. Vandewalle. “Image Segmentation”. Projet en Digital Photography ,2003

[VAR 00] G.T.B. Verwaaijen, A.M. Baze, S.H. Garez, L.P.J. Veelunturf et B. J. van der Zwaag, “A Correlation-Based Fingerprint Verification System”, IEEE ProRISC2000 Workshops on Circuits, Systems and Signal Processing, Nov 2000.

[VER 99] P. Verlinde, P. Druyts, G. Cholet et M. Acheroy, “Applying Bayes based classifiers for decision fusion in a multi-modal identity verification system”, In: Proceedings of International Symposium on Pattern Recognition “In Memoriam Pierre Devijver”, Brussels, Belgium, February 1999.

[VIS 96] Viscaya et Gerhardt, “A Nonlinear Orientation Model for Global Description of Fingeprints”, Pattern Recognition, Vol. 29, no. 7, pp. 1221–1231, 1996.

[WAN 03] Y.Wang, T. Tan et A. Jain, “Combining face and iris biometrics for identity verification”. In: Proceedings of Fourth International Conference on Audio and Video-Based Authentication (AVBPA), pp. 805–813, Guildford, U.K., June 2003.

[WAT 01] A. Watkins, “AIRS : A resourcelimitedartificial immune classifier”, Thèse de l’université de Mississipi du département d’informatique, Mississipi, 2001.

[WHI 04] J. White, “Artificial Clonal Selection for Pattern Recognition”, PhD thesis, University of Wales, Aberystwyth, December 2004.

[WHI03] J. A. WHITE, S. M. GARRETT, “Improved pattern recognition with artificial clonal selection”. In Proceedings of ICARIS, 2003

[WHI02] “A model of Gene Library Evolution in the Dynamic Clonal SelectionAlgorithm”, ICARIS, pp.175-182, 2002.

[WIL 97] R.P. Wildes, “Iris recognition : An emerging biometric technology”, Proceedings of the IEEE , V. 85, issue 9, pp. 1348

-1363, September 1997.

[WOO 97] K. Woods, W. Kegelmeyer et K. Bowyer, “Combination of Multiple Classifiers Using Local Accuracy Estimates”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 19, no. 4, pp. 405–410, 1997.

[XU 92] L. Xu, A. Krzyzak et C. Suen, “Methods of combining multiple classifiers and their applications to handwriting recognition”, IEEE Transactions on Systems, Man and Cybernetics, Vol. 22, no. 3, pp. 418–435, 1992.

[YAM 02] C.Y. Yam, M.S. Nixon et J.N. Carter, “On the Relationship of Human Walking and Running: Automatic Person Identification by Gait” ICPR, pp. 1051-4651, 2002.

[YAN 05] P. Yan et K. Bowyer, “Empirical Evaluation of Advanced Ear Biometrics”, IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp. 41, 2005.

[ZHU 00] Y. Zhu, T. Tan et Y. Wang, “Biometric personal identification based on iris patterns”, In: Proceedings of the 15th International Conference on Pattern Recognition, pp. 801–804, 2000.

[ZOU06] ZOUAGHI Tarik, H.Benoit-Catin et C.Odet.“Une vision fonctionnelle de la segmentation d'images”, Congrès Francophone de Vision par ordinateur. 2006

[ZUB 01] F.J. Von Zuben et L.N. De Castro, “aiNet: An artificial Immune Network for Data analysis In Data Mining: A Heuristic Approach”, Idea Group publishing, USA, Chapter XII, pp.213-259, 2001.

WEBOGRAPHIE:

[WEB01] http://fr.wikipedia.org/wiki/S%C3%A9lection_n%C3%A9 gative_des_cellules_B.

[WEB02] http://magnin.plil.net/spip.php.article44.

[WEB03] http://www.recherche.enac.fr/opti/papers/thesis/HABIT/main002.html

[WEB04] http://biometrie-Online.net

[WEB05] http://biometrie.online.fr

[WEB06] http://www.biometricgroup.com

[WEB07] http://solutions.journaldunet.com/0208/020826_biometrie_1.shtml

[WEB08] http://biometrie.online.fr

[WEB09] http://www.biometricgroup.com

[WEB10] http://homepages.inf.ed.ac.uk/rbf/HIPR2/hitmiss.htm

[WEB11] http://matlabserver.cs.rug.nl/edgedetectionweb/web/edgedetection_params.htm

[WEB12] http://tpe-biometrie.fr

[WEB13] ums-riate.fr/ecoleyaounde2006/documents/fascicules/Classif_doc.pdf.

[WEB14] http://fr.wikipedia.org/wiki/Syst%C3%A8me_immunitaire_artificiel.