

UNIVERSITE KASDI MERBAH OUARGLA

Faculté des Nouvelles Technologis de l'Information et de la Communication

Département de l'Electronique et de la Télécommunication



Mémoire

MASTER ACADEMIQUE

Domaine : Sciences et technologies

Filière : Systèmes Embarqués

Spécialité : Systèmes Embarqués

Présenté par :

ADJAINÉ Elmechri

BENSLIMAN Abdelkarim

Thème

Authentification et Identification biométrique des personnes par les empreintes palmaires

Soutenu publiquement

Le : 07 /07 /2019

Devant le jury :

M. N.NASRI	MAA	Président	UKM Ouargla
M. A.G.MANSEUR	MAA	Examineur	UKM Ouargla
M. Z. TIDJANI	MAA	Encadreur	UKM Ouargla
M.K.BENSID	Docteur	Co- Encadreur	UKM Ouargla

Année Universitaire : 2018 /2019

Dédicace

Je dédie ce mémoire:

À mes très chers parents pour leur soutien durant toute ma vie d'étudiant et sans eux je ne serai jamais devenu ce que je suis.

mes frères et mes sœurs

A mes tantes et mes oncles

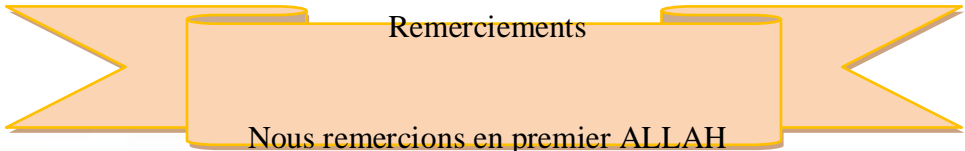
À mes amis d'enfance

À tous les professeurs et enseignants qui m'ont suivi durant tout mon cursus scolaire et qui m'ont permis de réussir dans mes études.

À mes amis d'étude

À toute personne ayant contribué à ce travail de près ou de loin.

ADJAINÉ ELMECHRI



Remerciements

Nous remercions en premier ALLAH

le tout puissant de nos avoir accordé la
volonté et le courage pour réaliser
notre mémoire.

Nous tenons à remercier Mr.TIDJANI ZAKARIA
et D.Ben Sid Khaled, qui a nous encadrer,
et nous lui exprimons particulièrement de toute
reconnaissance pour nous avoir fait bénéficié de ses
compétences scientifiques, ses qualités humaines et
sa constante disponibilité.

Nous remercions tous les professeurs
et les étudiants de spécialité « système embarqués »

Enfin, Nous remercions à tous ceux qui ont
contribué de près ou de loin à la réalisation de
ce travail.




Table des matières

Table des matières	I
Liste des figures	II
Liste des tableaux.....	III
Abstract	v
Résumé	vi
Liste des abréviations.....	iv
Introduction Générale.....	01
Chapitre I : Généralités Sur la Biométrie	
I.1 Introduction.....	03
I.2 la biométrie	03
I.2.1 définition de la biométrie.....	03
I.2.2 Domaines d'applications.....	03
I.3 Différentes modalités biométriques.....	04
I.3.1 Analyse biologique.....	05
I.3.2 Analyse comportementale.....	05
I.3.3 Analyse morphologique.....	06
I.4 Principe de fonctionnement.....	07
I.4.1 Module capteur biométrique	08
I.4.2 Module d'extraction des caractéristiques.....	08
I.4.3 Module comparaison.....	09
I.4.4 Module base de données.....	09
I.4.5 Module de décision	09
I.5 Architecture d'un système biométrique.....	09
I.5.1 mode d'enrôlement.....	09
I.5.2 Mode Vérification.....	10
I.5.3 Mode identification.....	10
I.6 La Multi modalité.....	11
I.7 Les niveaux de fusion.....	12
I.7.1 Fusion au niveau capteur.....	12
I.7.2 Fusion au niveau de données ou caractéristiques.....	13
I.7.3 Fusion au niveau score de comparaison.....	13
I.7.4 Fusion au niveau rang.....	13

I.7.5 Fusion au niveau de la prise de décision.....	13
I.8 Evaluation.....	14
I.9 Conclusion	15
 Chapitre II : Extraction des caractéristiques par la biais de modèle flou	
II.1 Introduction	17
II.2 les sous-ensemble flous	17
II.2.2 fonction d'appartenance	17
II.2.3 Variables linguistiques	18
II.3 Système d'inférence floue	18
II.3.1 Fuzzification	19
II.3.2 Inférence	19
II.3.3 Defuzzification	19
II.4 Modèle de Takagi-Sugeno.	19
II.5 La méthode gradient conjugué... ..	21
II. 6 Pré conditionnement de système	22
II.7 Algorithme du gradient conjugue Pré conditionnement	23
II.8 Conclusion	24
 Chapitre III : Résultats expérimentales et discussion	
III.1 Introduction	25
III.2 Amélioration de l'empreinte palmaire	25
III.3 Système biométrie proposé	26
III.3.1 Dispositif de capture des images de l'empreinte palmaire en ligne.....	26
III.3.2 La base de données des images palmaires	26
III.3.3 Séparation de la basse des données.....	27
III.4 L'extraction des caractéristiques	27
III.5 le module comparaison	28
III.6 L'adaptation des paramètres.....	29
III.6 .1 Nombre des fonctions d'appartenances du flou.....	29
III.6 .2 nombre d'itérations	29
III .7 Application uni-modale.....	30
III .8 Application Multimodale.....	32
III .9 Conclusion.....	33
Conclusion Générale.....	34

Liste des abréviations

ERR : Taux d'erreurs égales ("Equal Error Rate").

FAR : Taux de Fausses Acceptations ("False Acceptance Rate").

FRR : Taux de Faux Rejets ("False Reject Rate").

MAX : Maximum.

MIN : Minimum.

CMC : Cumulative Match Caractéristique.

ROC : Courbe représentant les taux d'erreur ("Receiver Operating Curve").

ADN : Acide Désoxyribose Nucléique.

NIR : Near Infra-Red.

Th : Threshold.

GCP l'algorithme du gradient conjugué pré conditionné.

Liste des figures

Chapitre I

Fig. I.1 : Modalités biométriques.....	4
Fig. I.2 : ADN	5
Fig. I.3 : Démarche.....	6
Fig. I.4 : signale de la voix	7
Fig. I.5 : La reconnaissance faciale (visage)	7
Fig. I.6 : le Principe de fonctionnement	8
Fig. I.7 : Capteur biométrique.....	8
Fig I. 8 Architecture d'un système biométrique.....	09
Fig. I.9 : Le mode de vérification ou authentification	10
fig. I.10 Niveaux de fusion.....	12
Fig. I.11 : Illustration du FRR et du FAR	14
Fig. I.12 : Courbe ROC	15

Chapitre II

Fig II.1 Fonctions caractéristiques d'un sous-ensemble classique pour l'exemple cité ci-dessus.....	18
Fig II.2 Fonctions caractéristiques d'un sous-ensemble flou (b) pour l'exemple cité ci-dessus.	18
Fig II.3. Système D'inférence Floue.....	19

Chapitre III

Fig III.1 L'empreinte palmaire.....	
Fig III.2 Dispositif de capture de palmaires en ligne.	25
Fig.III.3 Extraction des caractéristiques dans le système biométrique proposé (protocole).	26
Fig III.4 Système biométrique proposé.	28
Fig. III.5.: Performance de système uni-modal.....	31
Fig. III.6: Performance de système uni-modal (CMC)	31

Liste des tableaux

Tableau III.1 : Influence du nombre des fonctions d'appartenances	29
Tableau III.2 Résultat de l'EER, l'ROR et ROR en fonction du nombre d'itération.....	30
Tableau III.3 Résultats de l'EER, ROR et RPR pour différentes bandes uni-modal	31
Tableau III.4 Résultats de l'EER, ROR et RPR pour différentes bandes multimodale.....	32

Introduction Générale

Introduction générale

La sécurité des systèmes d'information (SSI) ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du système d'information[1].

Aujourd'hui, la sécurité est un enjeu majeur pour les entreprises ainsi que pour l'ensemble des acteurs qui l'entourent. Elle n'est plus confinée uniquement au rôle de l'informaticien. Sa finalité sur le long terme est de maintenir la confiance des utilisateurs et des clients. La finalité sur le moyen terme est la cohérence de l'ensemble du système d'information. Face à cette sollicitation grandissante, plusieurs systèmes de sécurité ont été proposés, reconnaissance palmaire, faciale, empreinte digitale et reconnaissance de l'iris...etc[1].

Le but de la biométrie dans le contrôle d'accès est de gérer les accès physiques ou logiques afin d'accroître la sécurisation des accès à des locaux de tous types mais aussi sécuriser l'accès à des stations informatiques et aux dossiers et fichiers présents sur ces dernières. La biométrie commence à être utilisée également afin d'authentifier un utilisateur lors de transactions bancaires pour sécuriser les paiements via des terminaux physiques ou encore pour des paiements en ligne. .

A ce projet, l'une des technologies étudiées est la biométrie via l'empreinte palmaire . Autant au niveau du contrôle des individus (passeport, carte d'identité et permis de conduire biométriques), qu'au niveau du contrôle d'accès.

Dans ce projet, nous définirons les notions de base de la logique floue. La logique floue (fuzzy logic, en anglais) est une logique multi-valuée où les valeurs de vérité des variables - au lieu d'être vrai ou faux - sont des réels entre 0 et 1. En ce sens, elle étend la logique booléenne classique avec des valeurs de vérités partielles. Elle consiste à tenir compte de divers facteurs numériques pour aboutir à une décision qu'on souhaite acceptable.

La logique floue est une technique largement utilisée dans le domaine de la commande des systèmes et processus industriels; notre contribution est d'utiliser cette technique pour la modélisation du vecteur de caractéristiques biométrique.

Dans ce travail nous allons proposer l'utilisation des système flous pour la conception d'un système biométrique de vérification et d'identification des personnes a partir de leurs empreintes palamires. ce mémoire est organisé comme suit:

Dans le premier chapitre, nous introduisons quelques définitions de la biométrie et différentes modalités biométriques

Dans le deuxième chapitre, nous allons aborder les notions de base et théorique de la logique floue, les différents modèles flous. Nous allons ensuite proposer une méthode d'apprentissage pour l'extraction de quelques caractéristiques discriminantes à partir de l'image palmaire .

Dans le troisième chapitre, nous allons appliquer la solution proposée à une base de données d'empreintes palmaires. Cela nous permettra de valider et d'analyser notre solution.

A la fin, nous terminons par une conclusion.



Chapitre I

Généralités Sur la Biométrie

I.1-Introduction

Il existe aujourd'hui une panoplie assez large de modalités biométriques et il en apparaît constamment de nouvelles. En fait, aucune modalité ne permet d'assurer à la fois une précision suffisante et un confort d'utilisation et cela dans toutes les situations d'usage. De plus, quelle que soit la modalité, il existe toujours des personnes réfractaires (mains usées de travailleurs manuels, visages voilés, voix enrrouées). [4] Nous ne décrivons ici que les modalités les plus communes, à savoir le visage, la parole, les empreintes digitales, le contour de la main et l'iris de l'œil, laissant de côté d'autres modalités moins classiques (veines de la main, ADN, odeur corporelle, forme de l'oreille, des lèvres, rythme de frappe sur le clavier, démarche...).

La biométrie est de plus en plus utilisée dans des applications de la vie courante. Si à ces débuts au 19ème siècle les données biométriques étaient traitées manuellement, aujourd'hui, avec les traitements informatiques, les systèmes biométriques sont automatisés. Dans ce chapitre, nous allons d'abord présenter le cadre général d'utilisation de la biométrie ainsi que la structure, les avantages des systèmes biométriques. Ensuite, nous présenterons la biométrie multimodale qui est le domaine d'étude de ce travail. La biométrie multimodale est la combinaison de plusieurs modalités biométriques.[2]

I.2 La biométrie

Avant de procéder aux détails de la biométrie, il y a lieu de définir ce terme comme suit :

I.2.1 Définition

La biométrie représente la mesure biologique ou les caractéristiques physiques qui peuvent être utilisées pour identifier les individus. Le mappage des empreintes digitales, la reconnaissance faciale et les empreintes rétinienne sont tous des formes de technologie biométrique, mais il ne s'agit là que des options les plus connues [3].

I.2.2 Domaines d'applications

Longtemps réservée aux grandes institutions de l'Armée et des Services Secrets du monde entier, la biométrie est aujourd'hui accessible à tous les professionnels et les particuliers [4].

De plus en plus d'entreprises, quelque soit leur taille et leur secteur d'activité viennent renforcer leur sécurité et optimiser leurs ressources humaines par l'installation de dispositifs biométriques. Parmi les secteurs d'application des systèmes biométriques, nous pouvons citer [5]:

Contrôle d'accès: Locaux professionnels ou commerciaux, lieux de stockage, laboratoires, banques, coffres-forts, hôpitaux,

Gestion du temps de travail et pointage en entreprise: Industries, PME, Associations, Ecoles, Magasins...la biométrie viendra s'interfacer aisément avec un logiciel de gestion de présences.

Gestion des adhérents de salles de sport: Centres de Fitness, Associations Sportives, Clubs de gym...La biométrie vient remplacer les badges coûteux et permet aux adhérents de se rendre dans leur club en toute simplicité!

Sécurité informatique: Sécurité des serveurs, des ordinateurs, des réseaux...etc. La sécurité des données est devenue un enjeu économique majeur au cours de ces dernières années, il est vital de les protéger.

Le mot « biométrie » est utilisé également dans le sens plus restrictif de l'« identification des personnes » en fonction de caractéristiques biologiques, telles que les empreintes digitales, les traits du visage, etc. ou de caractéristiques comportementales, telles que la reconnaissance vocale, la signature, la démarche, etc. Face à cette sollicitation il est nécessaire de citer les principales modalités biométriques.

I.3 Différentes modalités biométriques

Il existe plusieurs types de modalités biométriques qui peuvent être classées en deux grandes catégories : les biométries morphologiques et les biométries comportementales [1]. Les biométries morphologiques sont les biométries utilisant une partie du corps humain tel que l'empreinte digitale ou l'iris. Les biométries comportementales sont celles utilisant un trait personnel du comportement, comme par exemple la signature ou la démarche.

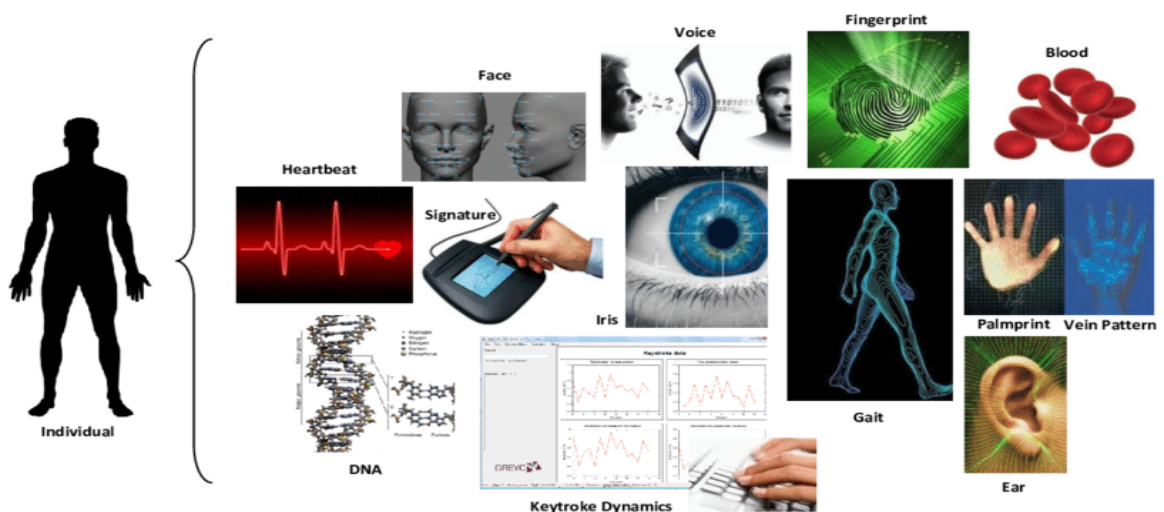


Fig. I.1: Modalités biométriques.

La figure I.1 illustre les différents empreintes biométriques. Nous pouvons les classer comme suit :

I.3.1 Analyse biologique

Cette analyse est basée sur les caractéristiques biologiques des individus (ADN, salive, Odeur...). Ce type de biométrie est très complexe à mettre en œuvre dans un système usuel de reconnaissance et n'est utilisé que dans un cas d'extrême nécessité (ex: Enquête criminelle, test de paternité...etc.) [4].

a-ADN L'empreinte génétique est la marque biologique la plus sûre du monde. Dans le cas des tests de paternité, on atteint une fiabilité de 99,999%. Mais les analyses d'ADN nécessitent des délais de plusieurs semaines, ce qui interdit toutes les applications d'identification en rapide.



Fig. I.2 : ADN

I.3.2 Analyse comportementale

La biométrie comportementale, quant à elle, 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 un clavier [4].

a) Voix

Un spectrogramme relève la tonalité, le rythme, l'intensité et la fréquence de la voix. Réputée peu fiable, c'est quand même la seule technique qui permet une authentification à distance. Elle ne peut cependant pas constituer une preuve suffisante pour la justice.

b) 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.



Fig. I.3 l'oreille

I.3.3 Analyse morphologique

L'analyse morphologique est basée sur l'identification des caractéristiques physiques particulières, ces derniers sont uniques et permanents, Elle sont classées en plusieurs tybes:

a-Empreintes digitales

Une empreinte est un dessin formé par les lignes de la peau. On en retrouve à différents endroits du corps. Lorsqu'on parle d'empreintes digitales, on fait référence aux lignes de la peau des doigts. La formation du dessin a lieu durant la période embryonnaire. Les lignes des doigts, ou crêtes papillaires, sont donc formées dans le ventre de la mère alors que la peau subie une pression interne. Chaque morphogenèse étant unique, les empreintes sont donc individuelles à chacun. La probabilité de trouver deux empreintes digitales similaires est extrêmement rare (1 sur 10^{24}).

D'autre part, les caractéristiques de la peau, laquelle est constituée de différentes couches lui permettant de se régénérer, lui confère son immuabilité. Ainsi, la pérennité du dessin s'explique par le fait qu'une blessure au doigt guérisse sans en altérer l'empreinte, à moins d'avoir affecté très profondément la peau. C'est donc dire qu'en plus d'être uniques, les empreintes se fixent avant même la naissance et perdurent jusqu'à la mort. Toutes ces caractéristiques rendent les empreintes digitales très attrayantes dans le domaine de la biométrie [5].

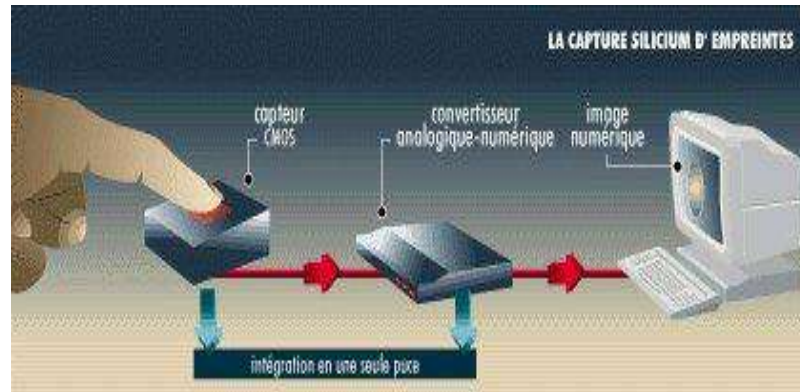


Fig. I.4: caractéristiques des Empreintes digitales.

b) Visage

La reconnaissance faciale (visage) permet d'adapter la vérification biométrique à toutes les situations. C'est une technologie très efficace qui est utilisée dans de nombreuses applications liées à la sécurité. Elle est par exemple un outil très fiable pour aider les forces de police à identifier des criminels, ou bien pour permettre aux services de douanes de vérifier l'identité des voyageurs. Actuellement, avec la numérisation des échanges, l'usage de cette technologie est en train de s'étendre au monde des entreprises. Utilisée dans des applications commerciales, la reconnaissance faciale permet par exemple de sécuriser des transactions en ligne. La reconnaissance faciale est sans contact et son utilisation ne nécessite aucun outil spécifique, ce qui en fait la solution idéale pour l'identification de personnes dans une foule ou dans des espaces publics[13].



Fig.I.5. La reconnaissance faciale (visage)

I.4 Principe de fonctionnement

Le système biométrique basée sur l'application des étapes suivantes :

1- Capture de l'information à analyser (image ou son). Traitement de l'information et création d'un fichier " signature/modèle " (éléments caractéristiques de l'image), puis mise en mémoire de ce fichier de référence sur un support (disque dur, carte à puce, code barre).

Dans la phase de vérification, l'on procède comme pour la création du fichier " signature/modèle " de référence, ensuite on compare les deux fichiers pour déterminer leur taux de similitude et prendre la décision qui s'impose.

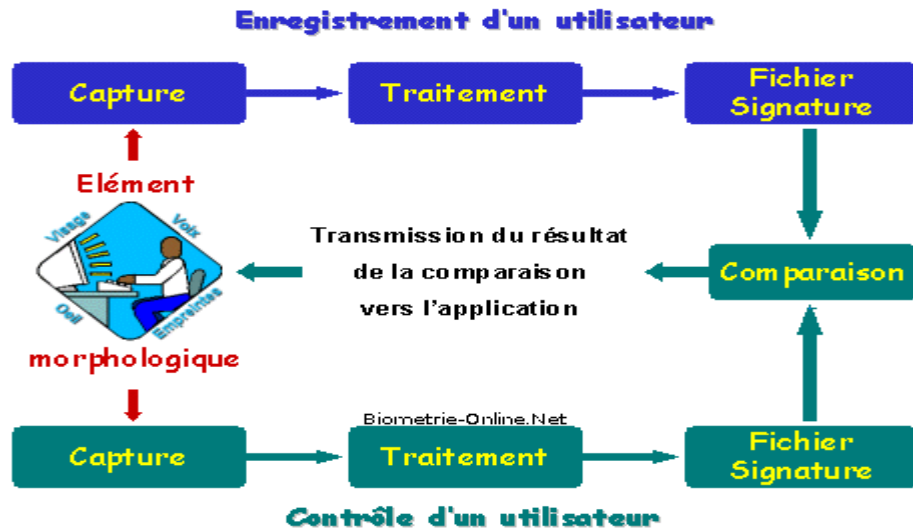


Fig. I.6 le Principe de fonctionnement d'un système biométrique

Au cours de cette phase, on distingue les principaux modules qui composent un système biométrique

I.4.1 Module capteur biométrique :

Responsable de l'acquisition des données biométriques d'un individu et la lecture de certaines caractéristiques morphologiques, et ou comportementales.



Fig. I.7 capteur biométrique

I.4.2 Module d'extraction des caractéristiques

Les caractéristiques biométriques sont une solution alternative aux anciens moyens de vérification d'identité. L'avantage de ces derniers est qu'elles doivent être universelles, uniques, permanentes, enregistrables et mesurables.

L'intérêt principal de la biométrie est donc de reconnaître et d'identifier automatiquement les identités des individus, en utilisant les caractéristiques physiologiques ou comportementales. L'extraction des caractéristiques clés de l'échantillon sont sélectionnées ou améliorées. Typiquement, le processus d'extraction de caractéristiques repose sur un ensemble d'algorithmes; le procédé varie en fonction du type d'identification biométrique utilisé [6].

I.4.3 Module comparaison

Ce module compare les caractéristiques biométriques d'une personne soumise à contrôle (volontairement ou à son insu) avec les « signatures » mémorisées. Ce module fonctionne soit en mode vérification (pour une identité proclamée) ou bien en mode identification (pour une identité recherchée) [4].

I.4.4 Module base de données:

Dans lequel on stocke les modèles biométriques des utilisateurs enrôlés.

I.4.5 Module de décision :

Il 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.5 Architecture d'un système biométrique

Il existe deux modes biométriques utilisés dans tout les systèmes biométriques , on peut en distinguer trois catégories :

I.5.1 Le mode d'enrôlement

C'est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier. Le système biométrique est un système de reconnaissance des personnes qui procède en premier pas à l'acquisition des données biométriques de l'individu à reconnaître, puis extrait un ensemble de caractéristiques à partir de celles-ci, enfin il compare ces caractéristiques avec les modèles de la base de données . L'architecture d'un système biométrique est illustrée sur la **Figure I.8**.

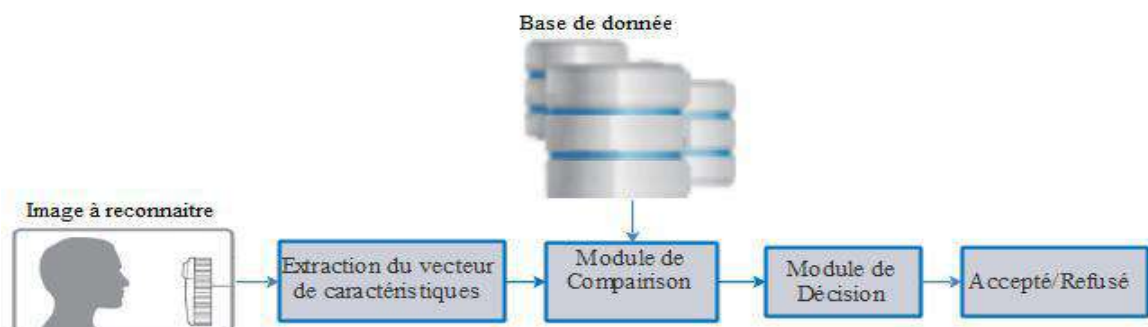


Fig I. 8 Architecture d'un système biométrique

I.5.2 Mode Vérification

Dans ce cas, le système compare la donnée de test (de la personne de test) avec la donnée biométrique stockée dans la base de données pour vérifier l'identité déclarée. Dans ce genre de système, la comparaison n'est faite qu'une fois et sert ensuite à prendre une décision à partir de la sortie du module de comparaison, appelée aussi **One-to-One (1:1)**

I.5.3 Mode identification

Dans ce cas, le système compare la donnée de test avec toutes les références stockées dans la base de données et sert ensuite à prendre une décision à partir de la sortie du module de comparaison (voir **Figure I.9**), appelée aussi **One-to-Many (1:N)**

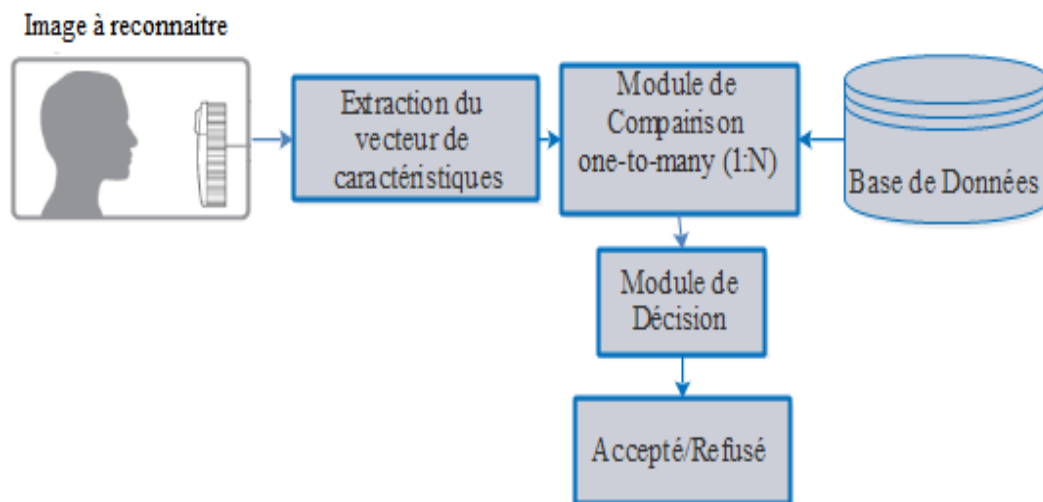


Fig. I.9 Mode Vérification. Identification

On distingue deux types d'identification :

a. Identification en ensemble fermé :

par exemple on utilise. Ce type d'identification afin d'enregistrer la présence de personnes dans certaine entreprise. Si l'échantillon possède un certain degré de similitude avec les échantillons dans le system, la personne sera acceptée.

b. Identification en ensemble ouvert :

Même s'il y'a une grande similitude entre l'échantillon biométrique testé et tous les modèles pré-enregistrés et si cette similitude est inférieure (ou supérieure) au seuil de sécurité, cette personne est rejetée. Cela signifie que la personne ne fait pas partie de celles enregistrées par le système [18].

I.6 La Multi modalité

Bien que certains systèmes mono modaux aient obtenu une amélioration considérable de la fiabilité et de la précision, ils souffrent souvent de problèmes d'inscription en raison de non universalité de leurs traits biométriques de bases, la susceptibilité à l'usurpation biométrique ou manque de précision causée par des données bruitées. Par conséquent, une seule modalité biométrique peut ne pas être en mesure d'atteindre l'exigence de performance souhaitée dans les applications du monde réel. Pour surmonter ces problèmes, les systèmes d'authentification biométrique multimodaux, combinant des informations issues de plusieurs modalités, semble une solution fiable pour arriver aux bons résultats d'authentification[2].

Des études ont démontré que les systèmes biométriques multimodaux peuvent atteindre une meilleure performance par rapport aux systèmes monomodaux. Ces systèmes abordent le problème de la non universalité, depuis plusieurs modalités pour assurer une couverture suffisante de la population. Ils ont également découragé la falsification d'identité car il serait difficile pour un imposteur de falsifier multiples modalités biométriques d'une personne. Ainsi, des études ont démontré que les systèmes biométriques multimodaux peuvent atteindre une meilleure performance par rapport aux systèmes monomodaux. Une variété de facteurs doit être prise en compte lors de la conception d'un système biométrique multimodal:

- Le choix des modalités biométriques de base ;
- Le niveau de fusion des informations fournies par multiple sources biométriques ;
- La méthodologie adoptée pour intégrer l'information ;
- compromis du coût correspondant par rapport à la performance.

Les différentes formes de multi modalité comme suit :

- **Multi-capteurs:**

lorsqu'ils associent plusieurs capteurs pour acquérir la même modalité.

- **Multi-instances:**

lorsqu'ils associent plusieurs instances de la même biométrie.

- **Multi-algorithmes:**

lorsque plusieurs algorithmes traitent la même image acquise.

- **Multi-échantillons:**

lorsqu'ils associent plusieurs échantillons de la même modalité.

- **Multi-biométries:** lorsque l'on considère plusieurs biométries différentes, par exemple visage et voix.

I.7 Les niveaux de fusion

La fusion biométrique multimodale combine des mesures de différents traits biométriques pour renforcer les points forts et réduire les points faibles des différents processus biométriques fusionnés. Ainsi, la fusion des informations biométriques peut se faire dans différents niveaux : niveau capteur, niveau caractéristiques, niveau score, niveau décision ou niveau rang. comme montre la fig (I.10).

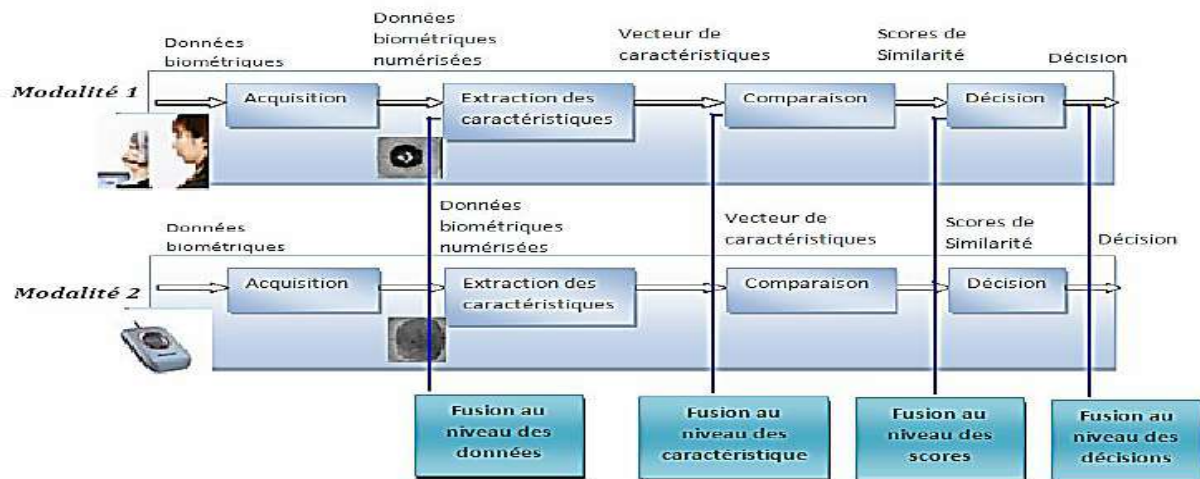


Fig. I.10 niveaux de fusion

I.7.1 Fusion au niveau du capteur

Dans la fusion de capteurs, les traits biométriques acquis à partir de capteurs tels que le scanner d'empreinte numérique, caméra vidéo, Iris Scanner, etc. Seront combinés pour former une caractéristique biométrique composite. Ce type de fusion peut se faire uniquement si les diverses captures sont des instances du même trait biométrique obtenu à partir de plusieurs capteurs compatibles entre eux ou plusieurs instances du même trait biométrique obtenu à partir d'un seul capteur [14].

De plus, les captures doivent être compatibles entre eux. Un exemple du niveau de fusion de capteurs consiste à détecter un signal de parole simultanément avec deux différents microphones. Un autre exemple de fusion au niveau capteur consiste à combiner plusieurs images d'empreintes digitales en les mettant en mosaïque afin de former une image d'empreinte digitale finale plus compliqué. Bien que la fusion à un tel niveau devrait améliorer la précision de la reconnaissance biométrique, il ne peut pas être utilisé pour d'autres biométries en raison de l'incompatibilité des données provenant de différentes modalités.

1.7.2 Fusion au niveau des caractéristiques

A ce niveau de fusion, les traits biométriques sont d'abord prétraités pour extraire séparément les vecteurs de caractéristiques, les combiner et générer un seul vecteur de caractéristiques composite. Ce vecteur sera utilisé par le processus de classification. La raison est que la fusion au niveau caractéristique est plus riche en informations sur les données biométriques brut. Cependant, un tel type de fusion n'est pas toujours possible. Par exemple, dans de nombreux cas, les caractéristiques pourraient ne pas être compatibles en raison de la différence dans la nature des modalités. Aussi tel enchaînement peut conduire à un vecteur de caractéristiques avec une très grande dimension. Cela augmente la charge de calcul. Il est rapporté qu'une conception complexe de classificateur pourrait être nécessaire pour opérer sur l'espace des caractéristiques à concaténer.

1.7.3 Fusion au niveau score

En fonction de la précision de chaque processus biométrique, nous pouvons fusionner les scores d'appariement résultants de ces processus biométriques pour trouver un appariement qui sera envoyé au module de décision. A ce niveau ; une étape de normalisation de scores est nécessaire. Actuellement, cela semble être le niveau de fusion le plus utilisé en raison de sa simplicité. Ce niveau de fusion peut être classé en deux catégories: combinaison et classification. Dans la première approche, un scalaire est obtenu en normalisant les scores dans un domaine commun, puis en combinant ces scores normalisés. Dans la deuxième approche, les scores sont considérés comme des caractéristiques d'entrée pour un deuxième problème de classification en deux classes de légitime et l'imposteur.

1.7.4 Fusion au niveau de décision

Chaque modalité est d'abord identifiée de façon indépendante. Puis, la décision finale est prise en se basant sur la fusion des décisions des différents processus biométriques. Les résultats finaux de plusieurs classificateurs sont consolidés par des techniques comme celle de la majorité de votes. Dans cette approche, une décision indépendante est prise pour chaque processus biométrique ce qui peut réduire la performance du processus de fusion. Ainsi, la fusion à un tel niveau est le moins puissant. La fusion au niveau décision est considérée, donc, comme rigide en raison de la disponibilité des informations limitées.

I.8 Evaluation de performance de système biométrique

Un système biométrique peut faire deux types d'erreurs. Il peut rejeter un utilisateur légitime et dans ce premier cas on parle de faux rejet (false rejection). Il peut aussi accepter un imposteur et on parle dans ce second cas de fausse acceptation (False Acceptance). La performance d'un système se mesure donc principalement avec son taux de faux rejet (False Rejection Rate ou FRR) et à son taux de fausse acceptation (False Acceptance Rate ou FAR).

Premier critère

« *False Reject Rate* » c'est le taux de Faux Rejetés indique le nombre de Faux Rejets (**FR**) divisé par le nombre de clients dans la base **Nc**. **FRR** est calculé par l'équation

$$FRR = FR/Nc \quad (I.1)$$

avec **FR** le nombre de faux rejet
NC le nombre de clients présents

Deuxième critère

« *False Accapte Rate* » c'est le taux d'erreur totale d'un système biométrique. Cette mesure est calculée par la relation suivante

$$FAR = FA/Ni \quad (I.2)$$

avec **FA** le nombre de fausse acceptation
Ni le nombre de imposteurs présentes

c) **Troisième critère** est connu sous le nom de taux d'égalé erreur ("Equal Error Rate" ou **EER**). Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où **FRR = FAR**, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations. A ce point, nous obtenons :

$$EER = FAR + FRR$$

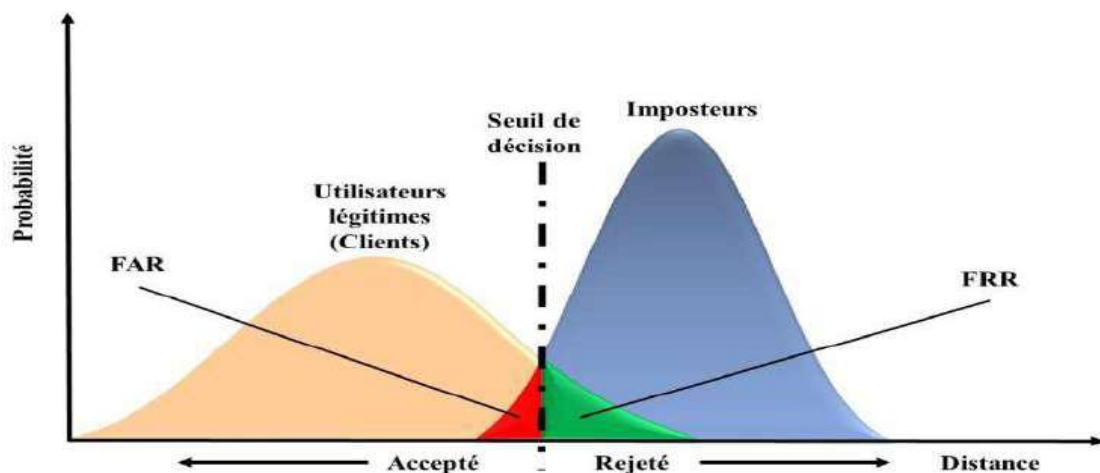


Fig. I.11 Illustration du FRR et du FAR

Les courbes est la liaison entre le FAR et le FRR pour différentes valeurs de seuil comme montre la **Figure I.11** La courbe ROC est la liaison entre le GAR et le FRR pour différentes valeurs de seuil comme le montre la **Figure I.12**.

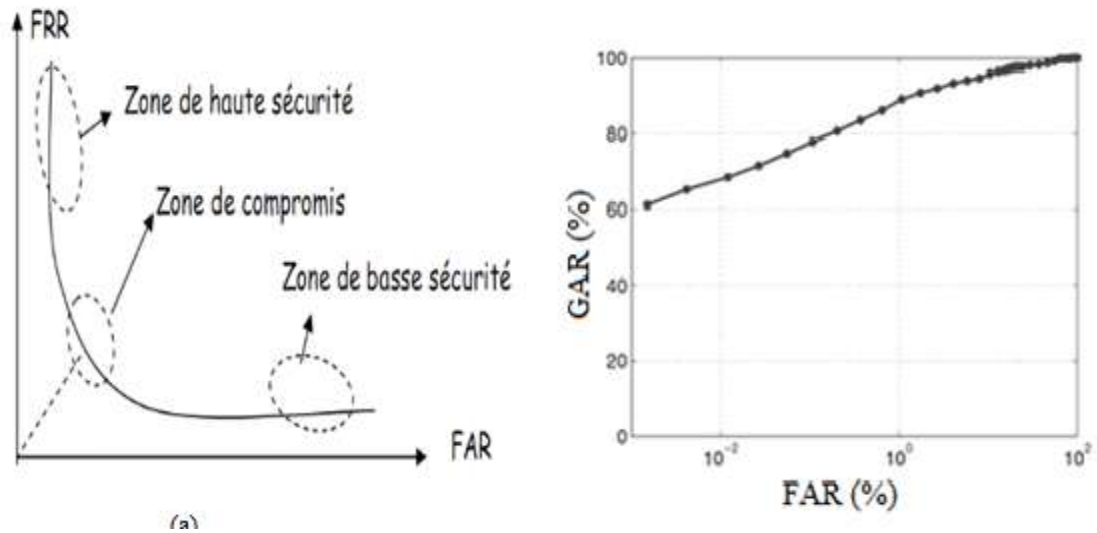


Fig I.12 Courbes ROC

I.9 Conclusion

Les systèmes biométriques utilisent différentes modalités pour authentifier ou identifier les personnes. La multimodalité offre meilleurs performances en matière FAR, FRR et ERR. Cependant l'implémentation d'un système biométrique nécessite tous d'abord l'extraction d'un vecteur de caractéristique fiable pour représenter l'empreintes. Dans le prochain chapitre, nous proposons un algorithme basé sur la modélisation par les systèmes flous.

Chapitre II

Modélisation à base de modèle flou

II.1 Introduction

La logique floue est une extension de la logique booléenne créée par Lotfi Zadeh en 1965 en se basant sur sa théorie mathématique des ensembles flous, qui est une généralisation de la théorie des ensembles classiques. En introduisant la notion de degré dans la vérification d'une condition, permettant ainsi à une condition d'être dans un autre état que vrai ou faux, la logique floue confère une flexibilité très appréciable aux raisonnements qui l'utilisent, ce qui rend possible la prise en compte des imprécisions et des incertitudes[10].

Dans ce chapitre, nous allons utiliser l'empreinte biométrique comme une fonction non linéaire à modéliser. Nous allons examiner les notions des systèmes flous ainsi que leurs utilisation pour la modélisation. Ensuite, la définition d'un problème d'optimisation, et sa formulation en critère quadratique, nous permettra d'exploiter l'algorithme d'optimisation le gradient conjugué pré conditionnel pour la détermination du vecteur caractéristique.

II.2 Théorie des sous-ensembles flous :

II.2.1 Les sous-ensembles flous

La logique floue repose sur la théorie des ensembles flous, qui est une généralisation de la théorie des ensembles classiques. nous utiliserons indifféremment les termes sous-ensembles flous et ensembles flous. Les ensembles classiques sont également appelés ensembles nets, par opposition à flou, et de même la logique classique est également appelée logique booléenne ou binaire[13].

II.2.2 fonction d'appartenance :

Definition : Soit X un ensemble. Un **sous-ensemble flou** A de X est caractérisé par une fonction d'appartenance $f_A : X \rightarrow [0,1]$. Cette fonction est l'équivalent de la fonction caractéristique d'un ensemble classique. La forme de la fonction d'appartenance est choisie arbitrairement en suivant les conseils de l'expert ou en faisant des études statistiques : formes sigmoïde, tangente hyperbolique, exponentielle, gaussienne ou de toute autre nature sont utilisables.

II.2.3 Variables linguistiques :

En logique floue, les concepts des systèmes sont normalement représentés par des variables linguistiques. Une variable linguistique est une variable dont les valeurs sont des mots ou des phrases utilisées couramment dans une langue naturelle ou un langage artificiel. Une variable linguistique est définie par [12]: $(X, U, T(X), \mu_x)$ Où X désigne le nom de la variable, U est l'univers du discours associé à la variable X (appelé aussi référentiel), $T(X) = \{T_1, T_2, \dots, T_n\}$ est l'ensemble des valeurs linguistiques de la variable X (appelé également termes linguistiques ou étiquettes linguistiques), et finalement μ_x sont les fonctions d'appartenance associées à l'ensemble de termes linguistiques.

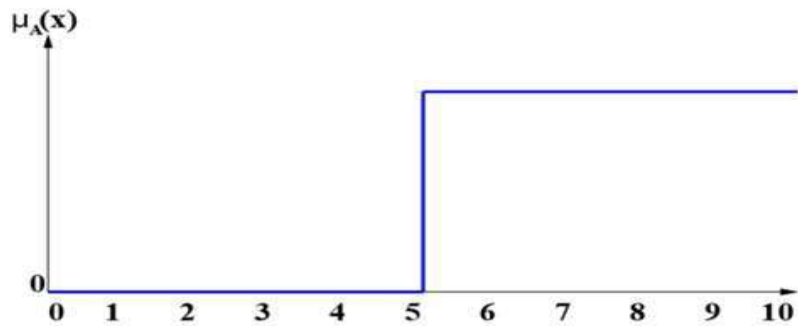


Fig II.1 Fonctions caractéristiques d'un sous-ensemble classique.

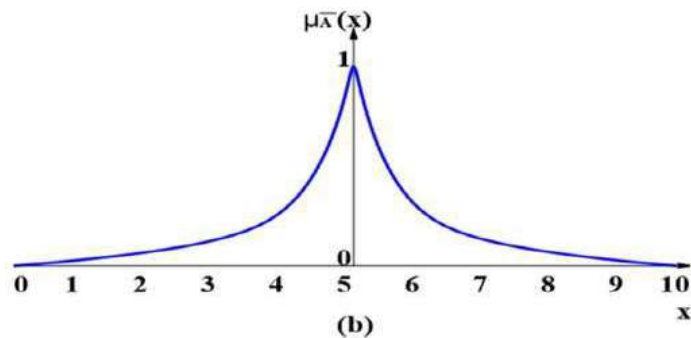


Fig II.2 Fonctions caractéristiques d'un sous-ensemble flou

II.3. Système d'inférence floue :

Un Système d'Inférence Floue (SIF) a comme but de transformer les données d'entrée en données de sortie à partir de l'évaluation d'un ensemble des règles. Les entrées sont issues du processus de fuzzification et l'ensemble de règles normalement sont définies par le savoir faire de l'expert [8].

II.3.1 Fuzzification :

Elle consiste à caractériser les variables linguistiques utilisées dans le système. Il s'agit donc d'une transformation des entrées réelles en une partie floue définie sur un espace de représentation lié à l'entrée. Cet espace de représentation est normalement un sous-ensemble flou. Durant l'étape de la fuzzification, chaque variable d'entrée et de sortie est associée à des sous-ensembles flous.

II.3.2 Inférence :

Elle consiste à utiliser le moteur d'inférence, qui est un mécanisme permettant de condenser l'information d'un système à travers un ensemble de règles définies pour la représentation d'un problème quelconque. Chaque règle délivre une conclusion partielle qui est ensuite agrégée aux autres règles pour fournir une conclusion (agrégation). Les règles constituent le système d'inférence floue, dans la suite de ce chapitre nous donnons une description des règles floues dans un cadre plus formel[23].

II.3.3 Defuzzification :

Elle consiste à caractériser les variables linguistiques utilisées dans le système. Il s'agit donc d'une transformation des entrées réelles en une partie floue définie sur un espace de représentation lié à l'entrée. Cet espace de représentation est normalement un sous-ensemble flou. Durant l'étape de la fuzzification, chaque variable d'entrée et de sortie est associée à des sous-ensembles flous

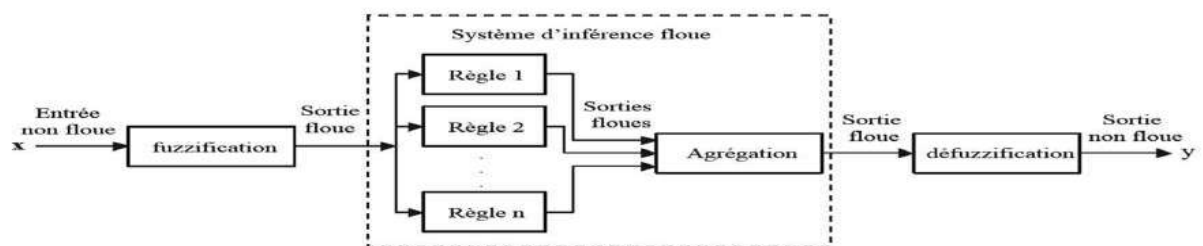


Fig II.3. Système D'inférence Floue

Quant aux systèmes flous, nous pouvons différencier les types des modèles suivants :

II.4 Modèle de Takagi-Sugeno :

Le modèle de raisonnement flou de Takagi-Sugeno (TS) qui est composé de règles de principe cause et effet. Souvent, les fonctions des conséquences sont choisies avec une expression polynomiale[5].

Dans le cas, de polynômes d'ordre zéro, l'expression de la sortie du système sera définie par[5]

$$\mathbf{I}(\mathbf{x}, \mathbf{y}) = \boldsymbol{\zeta}^T(\mathbf{x}, \mathbf{y}) \boldsymbol{\theta} \quad (\text{II.1})$$

Où le vecteur $\boldsymbol{\zeta} = [\zeta_1, \dots, \zeta_{nR}]^T$ est appelé vecteur d'activation, chaque terme ζ_i reflète le degré de considération de la règle dans la décision finale. Il est donné par [4] :

$$\zeta^t(\mathbf{x}, \mathbf{y}) = \frac{\mu_{A_{1i}}(x)\mu_{A_{2i}}(y)}{\sum_{i=1}^{nR} \mu_{A_{1i}}(x)\mu_{A_{2i}}(y)} \quad (\text{II.2})$$

Les termes A_{ij} sont des valeurs linguistiques avec nR le nombre de règles. Ici la conséquence est une fonction polynôme d'ordre zéro [13]. Ce modèle s'adapte bien à la description des systèmes à partir d'une expérience sous forme de règle de décision linguistique. Le vecteur des paramètres $\boldsymbol{\theta} = [a_{10}, \dots, a_{nR0}]^T$ regroupe les différents gains des fonctions polynômiales des conséquences.

En 1992 **Kosko** a prouvé que les systèmes flous sont des approximateurs universels. Ces systèmes sont capables d'approximer toute fonction suffisamment lisse avec une erreur bornée. Cette erreur peut être réduite considérablement avec un bon choix des paramètres du système flou (par exemple augmentation du nombre et de la distribution des fonctions d'appartenance) [15].

Problème

Nous considérons une fonction associée à une image biométrique donnée par $\mathbf{I}_{\text{image}}(\mathbf{x}, \mathbf{y})$ et un modèle flou d'approximation. Nous proposons la détermination du vecteur à travers la minimisation du critère suivant :

$$E^2 = \frac{1}{Np} \sum_{xy} [\mathbf{I}_{\text{image}}(\mathbf{x}, \mathbf{y}) - \hat{\mathbf{I}}(\mathbf{x}, \mathbf{y})]^2 \quad (\text{II.3})$$

Où Np est le nombre de pixel contenus dans l'image. Ce critère E^2 est la moyenne des carrées des erreurs d'approximation sur toute l'image appelé aussi Erreur Quadratique Moyenne (EQM). Cette dernière équation s'écrit :

$$E^2 = \frac{1}{Np} \sum_{xy} [\mathbf{I}_{\text{image}}(\mathbf{x}, \mathbf{y}) - \boldsymbol{\zeta}^T(\mathbf{x}, \mathbf{y}) \boldsymbol{\theta}]^2 \quad (\text{II.4})$$

Après développement, nous réécrivons l'EQM sous la forme matricielle [4]:

$$E^2 = \frac{1}{2} \boldsymbol{\theta}^T \mathbf{A} \boldsymbol{\theta} + \mathbf{b}^T \boldsymbol{\theta} + c \quad (\text{II.5})$$

avec

$$\mathbf{A} = 2 \sum_{xy} \frac{\boldsymbol{\zeta}(\mathbf{x}, \mathbf{y}) \boldsymbol{\zeta}^T(\mathbf{x}, \mathbf{y})}{Np} \quad (\text{II.6})$$

$$\mathbf{b}^T = \sum_{xy} \frac{2 \text{Image}(x,y) \zeta^T(x,y)}{Np} \quad (\text{II.7})$$

$$C = \sum_{xy} \frac{\text{Image}(x,y)^2}{Np} \quad (\text{II.8})$$

Puisque la matrice \mathbf{A} et les vecteur \mathbf{b} et \mathbf{c} peuvent être fixées par un choix arbitraires des fonction d'appartenance, il en reste le problème de détermination du vecteur. Il est possible de rechercher une méthode efficace permettant la détermination de ce vecteur tout en minimisant le critère EQM. En effet, cela assurera d'une part la qualité d'approximation et d'autre part sa considération comme vecteur caractéristique de l'empreinte biométrique.

II.5 La méthode du gradient conjugué :

Nous allons montrer dans cette section comment utiliser l'algorithme du gradient conjugué pré conditionné (GCP) pour la minimisation de l'EQM sachant que la matrice $\mathbf{A} \in \mathbf{R}^{n \times n}$ une matrice symétrique, définie positive.

Rappelons d'abord le principe et les principales caractéristiques de l'algorithme du gradient conjugué (GC) [21].

Considérons la fonctionnelle quadratique

$$\mathbf{E}: \mathbf{R}^n \rightarrow \mathbf{R}$$

$$E^2 = \frac{1}{2} \boldsymbol{\theta}^T \mathbf{A} \boldsymbol{\theta} + \mathbf{b}^T \boldsymbol{\theta} + \mathbf{c} \quad (\text{II.9})$$

dont le gradient vaut $\nabla E^2 = (\mathbf{A} \boldsymbol{\theta} - \mathbf{b})$. (II.10)

Le minimum de ce fonctionnel est atteint pour le point $\boldsymbol{\theta} \in \mathbf{R}^n$ qui annule ∇E^2 , donc vérifiant $\mathbf{A} \boldsymbol{\theta} = \mathbf{b}$. La méthode du gradient conjugué fait partie des méthodes de descente [1], qui ont comme principe commun la recherche de $\boldsymbol{\theta}$ suivant le processus itératif donné par :

$$\boldsymbol{\theta}_{i+1} = \boldsymbol{\theta}_i + \rho_i \mathbf{d}_i \quad (\text{II.11})$$

Avec, $\mathbf{d}_i \in \mathbf{R}^n$ la direction de descente et $\rho_i \in \mathbf{R}$ le pas de descente. la méthode simple de définition des paramètres de descente est le choix du pas de descente, une fois \mathbf{d}_i et $\boldsymbol{\theta}_i$ sont connues, on peut calculer facilement un pas de descente optimal [12] :

$$\rho_i = - \frac{(\mathbf{A} \boldsymbol{\theta}_i - \mathbf{b}, \mathbf{d}_i)}{(\mathbf{A} \mathbf{d}_i, \mathbf{d}_i)} \quad (\text{II.12})$$

qui réalise le minimum de la fonctionnelle E^2 dans la direction choisie.

Quant à la direction de descente, plusieurs choix sont possibles, ce qui nous permet de distinguer :

- la méthode du gradient : $\mathbf{d}_i = \mathbf{g}_i = \nabla E(\boldsymbol{\theta}_i)$

(basée sur l'observation que la valeur du fonctionnelle diminue le plus rapidement suivant la direction du gradient)

- la méthode du gradient conjuguée $\mathbf{d}_i = \mathbf{h}_i$

avec les directions de descente conjuguées par rapport à la matrice \mathbf{A} , c'est-à-dire $((\mathbf{A} \cdot \mathbf{h}_i), \mathbf{h}_j) = 0 \quad i \neq j$.

L'efficacité de la méthode du gradient conjuguée réside dans ses propriétés remarquables, énoncées ici pour l'itération i : les directions de descente \mathbf{h}_i sont construites de telle manière que les gradients $\mathbf{g}_i = \mathbf{A}\boldsymbol{\theta}_i - \mathbf{b}$ soient tous orthogonaux entre eux, $(\mathbf{g}_k, \mathbf{g}_j) = 0, \forall 0 \leq k < j \leq i$ (ce n'est pas le cas dans la méthode du gradient, où seulement deux gradients successifs sont

orthogonaux), $\boldsymbol{\theta}_i$ réalise le minimum de la fonctionnelle \mathbf{E} sur l'espace vectoriel $\boldsymbol{\theta}_0 + \text{Vect}\{\mathbf{g}_0, \mathbf{g}_1, \dots, \mathbf{g}_{i-1}\}$, de dimension i . D'un point de vue pratique, les directions de descente \mathbf{h}_i sont faciles à calculer, à partir des gradients \mathbf{g}_i , et la méthode nécessite le stockage de seulement trois vecteurs supplémentaires[12].

II. 6 Pré conditionnement de système :

Si l'algorithme (GC) peut être considéré comme une méthode exacte (la convergence étant assurée en N itérations au plus), il est généralement utilisée comme méthode itérative en s'attendant à ce qu'il converge plus rapidement. Pour accélérer la vitesse de convergence, on peut preconditionner le système linéaire[14]. L'idée ici est de multiplier le système initial par une matrice \mathbf{C} et résoudre le nouveau système $(\mathbf{C}^T \mathbf{A} \boldsymbol{\theta}^T = \mathbf{C} \cdot \mathbf{b}^T)$

En toute rigueur, pour appliquer le (GC), la matrice du système doit être symétrique. Cette observation nous amène à faire les manipulations algébriques suivantes pour trouver une formulation simple de l'algorithme Gradient Conjuguée Préconditionné (GCP).

Soit $\mathbf{U} \in \mathbf{R}^{n \times n}$ une matrice inversible et $\mathbf{z} = \mathbf{U}^T \boldsymbol{\theta}$ un changement de variable. La fonctionnelle \mathbf{E} donnée par (II.1) devient

$$\nabla E^2 = (\mathbf{A}\boldsymbol{\theta} - \mathbf{b}). \quad (\text{II.14})$$

Donc

$$\nabla E^2 = \frac{1}{2} (\mathbf{A}\mathbf{U}^{-1} \mathbf{z}, \mathbf{U}^{-1} \mathbf{z}) - (\mathbf{b}, \mathbf{U}^{-1} \mathbf{z}) = \frac{1}{2} (\mathbf{A}\mathbf{U}^{-T} \mathbf{z}, \mathbf{U}^{-T} \mathbf{z}) - (\mathbf{b}, \mathbf{U}^{-T} \mathbf{z}) \quad (\text{II.15})$$

II.7 Algorithme :

Cet algorithme après initialisation applique une procédure itérative (N itération au maximum) pour atteindre la valeur optimale des paramètres inconnus. Il est donné comme suit :

$\theta_0 \in R^n, \varepsilon, C$ donnés

$$A = 2 \sum_{xy} \frac{\zeta(x,y)\zeta^T(x,y)}{Np}$$

$$G_0 = (A\theta_0 - b).$$

$$H_0 = C G_0$$

pour $i=0$ à n

$$G_0 = A \theta_0 - b$$

$$G_{i+1} = G_i + \rho \cdot AH \quad (\text{II.15})$$

$$H_{i+1} = -CG_{i+1} + \Gamma H_i$$

$$\theta_{i+1} = \theta_i + \rho_i AH_i$$

$$\Gamma = \left(\frac{G_{i+1}CG_{i+1}}{G_iCG_i} \right)$$

Si $(G_{i+1}, G_{i+1}) < \varepsilon$ stop

Il est clair de ce qui précède que le choix «idéal» pour la matrice C, serait $C=A^{-1}$, l'inverse de A; dans ce cas, évidemment, l'utilisation de la méthode du gradient conjugué deviendrait inutile. En pratique, plus la matrice de préconditionnement est «proche» de A^{-1} , meilleure sera la convergence de l'algorithme. En même temps, la matrice C doit être la plus simple et la plus creuse possible, ce qui impose comme choix les plus faciles :

- $C=I$, la matrice identité (algorithme sans préconditionnement) ;
- $C=D^{-1}$, l'inverse de la partie diagonale de A.

I.8 Conclusion

Dans ce chapitre, nous avons présenté les outils nécessaires à la modélisation de l'image par un système flou de type Sugeno, cela nous a permis de formuler un critère quadratique à minimiser. L'algorithme du gradient conjugué préconditionné, tel que présenté, offre une procédure basée sur la récursivité. Dans le chapitre suivant, nous allons appliquer cet algorithme dans le cadre d'un système biométrique.

Chapitre III

Résultats expérimentaux et Interprétation

III.1 Introduction

L'application de la méthode du gradient conjuguée préconditionné (GCP), nous a permis de trouver un modèle flou équivalent à l'empreinte. L'optimisation a abouti à la détermination du vecteur inconnu dans le modèle flou. Cette méthode constitue la tâche d'extraction des caractéristiques dans un système biométrique.

Dans ce chapitre, nous allons développer un système biométrique pour l'identification des personnes à partir de leurs empreintes palmaires. Le modèle de chaque empreinte enregistrée dans la base de données est le vecteur obtenu par la méthode du GCP. Les différents tests, nous permettront de valider la méthode proposée et d'examiner ses performances.

Ce chapitre abordera le système biométrique proposé, la base des images empreintes d'expérimentation. Les différents résultats obtenus seront présentés et analysés.

III.2 Amélioration de l'empreinte palmaire

Pour améliorer la reconnaissance des empreintes palmaires il faut d'abord faire un traitement de l'empreinte, ce traitement prend l'empreinte palmaire comme une image numérique.

On peut représenter l'image numérique comme une interface divisée en un ensemble de cellules appelées pixels de tailles fixes et chaque pixel a une couleur correspond à l'image réelle[17].

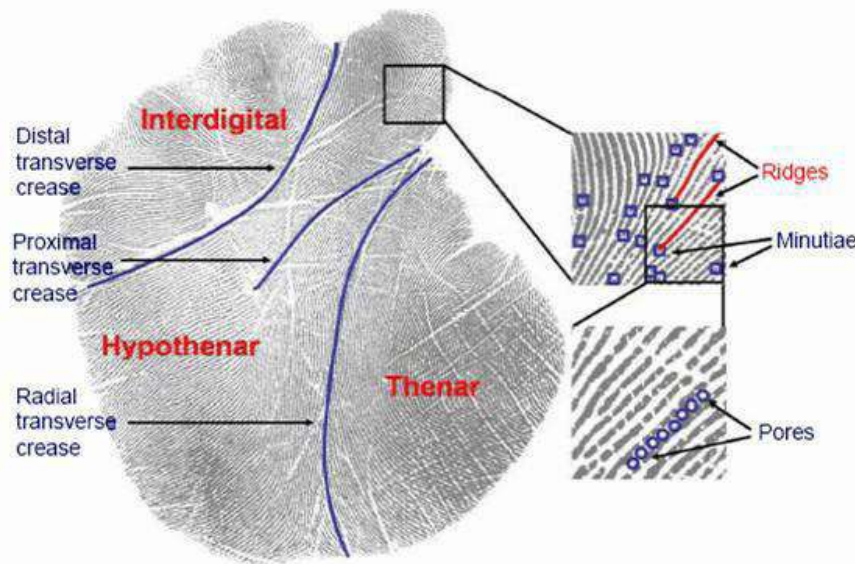


Fig III.1 L'empreinte palmaire

III.3 Système biométrie proposé le protocole

Nous proposons un système biométrie **Multi-échantillons** basé sur l'empreinte palmaire qui consiste en deux sous systèmes fusionnés au **niveau de score** (voir la ou est image Fig. III.2).

III.3.1 Dispositif de capture des images de l'empreinte palmaire en ligne

Pour accomplir une identification en ligne par les empreintes palmaires en temps réel, il faut un dispositif particulier qui doit être plus rapide dans l'acquisition d'empreintes palmaires. Un exemple d'un tel dispositif est présenté dans **la Figure III.2** [12].



Fig III.2 Dispositif de capture de palmaires en ligne.

Le système que nous avons développé contient quatre étapes essentielles qui sont : le prétraitement des images d'empreintes palmaires, extraction des paramètres ou codes pertinents, l'apprentissage des différentes classes de la base de données et la classification.

III.3.2 La base de données des images de palmaire

Les images palmaires que nous avons utilisées dans nos expérimentations sont issues de la base de données PolyUD[21] obtenu par un dispositif de capture multi-spectral en temps réel qui peut capturer des images de Palmprint sous des illuminations bleue, verte, rouge et infrarouge proche (NIR). Ces dernières sont utilisées pour construire une base des données multi-spectrales de Palmprint dans le but de fournir aux chercheurs qui travaillent dans le domaine de la reconnaissance multi-spectrale une plate-forme pour comparer l'efficacité de divers algorithmes multi-spectral de reconnaissance de palmprint.

La base de données Multi-spectral Palmprint a été recueillie auprès de 250 volontaires, dont 195 hommes et 55 femmes. La répartition par âge est de 20 à 60 ans. Les échantillons ont été recueillis en deux séances distinctes.

Dans chaque session, la personne a été invitée à fournir 6 images pour chaque paume. Par conséquent, 24 images de chaque illumination de 2 palmes ont été collectées de chaque personne. Au total, la base de données contient 6 000 images provenant de 500 paumes différentes pour un éclairage.

L'intervalle de temps moyen entre la première et la deuxième session était d'environ 9 jours.

Dans nos expériences, nous utilisons des bases des données a région d'intérêt (ROI) déjà extraite avec une taille 128×128 pixels pour évaluer nos méthodes d'extraction des fonctionnalités [5].

III.3.3 Séparation de la base de données

Il résulte souvent d'un compromis tenant compte du nombre de données dont on dispose et du temps pour effectuer l'apprentissage.

Dans les séries de tests que nous allons effectuer, la base a été segmentée de la façon suivante.

III.3.3.1 Image d'apprentissage Les images 1^{ère}, 5^{ème} et 9^{ème} chaque élément servent pour la phase d'apprentissage .

III.3.3.2 Image de test les image restantes de chaque élément nous ont servi pour la réalisation des différents tests (à savoir les images d'ordre 2, 3, 4, 6, 7, 8, 10, 11 et 12)

III.4 L'extraction des caractéristiques

Le choix que nous proposons dans ce chapitre est la méthode du «gradient conjugué préconditionnée » et la modification de la précondition avec matrice développée dans le chapitre (II) pour adapter les paramètres des vecteurs contenant les caractéristiques discriminantes.

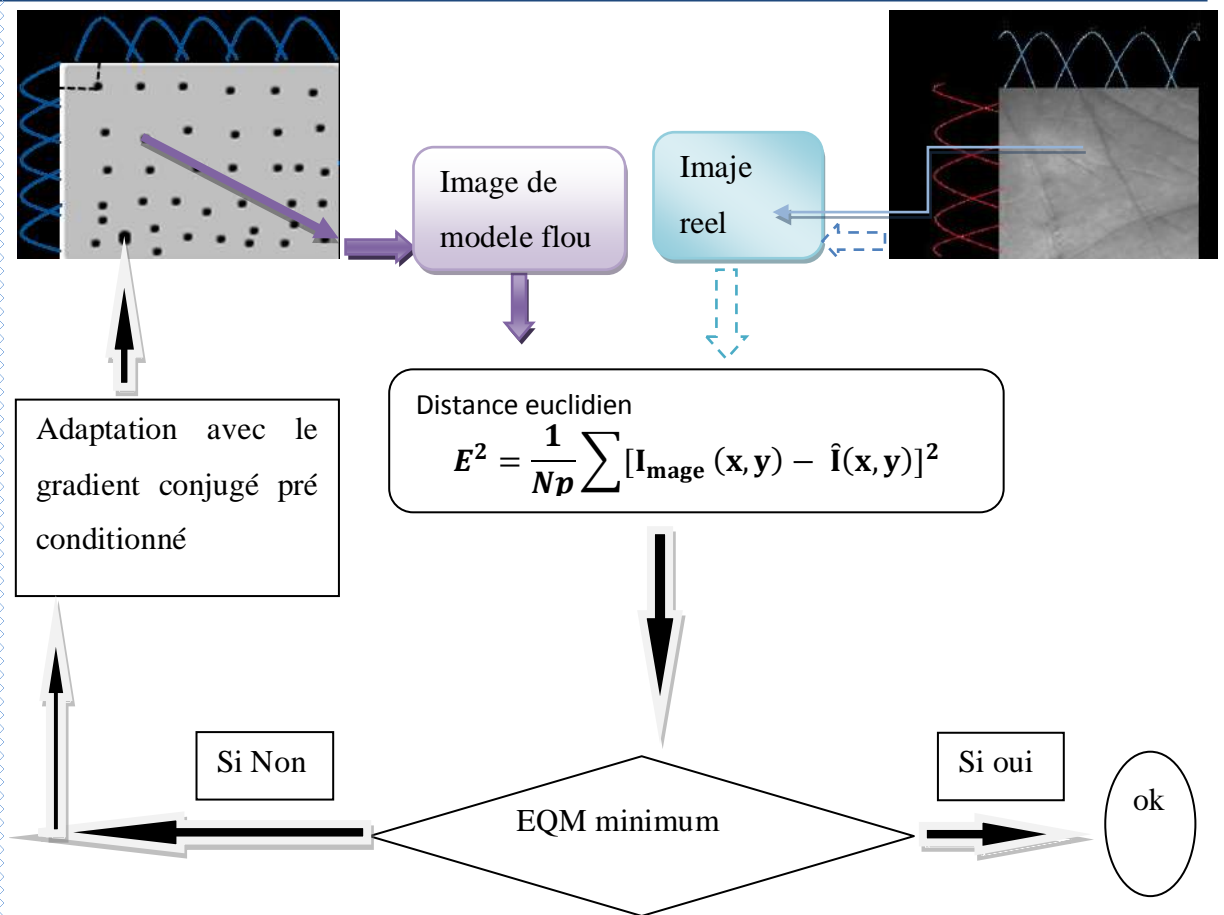


Fig.III.3 Extraction des caractéristiques dans le système biométrique proposé

Ainsi, cet algorithme est appliqué à tous les images de la modalités empreintes palmaires pour obtenir des modèles flou par l'optimisation de l'erreur qui a été calculée à l'étape de comparaison.

Une grande partie de la figure III.4, dans la page précédente, explique l'étape d'extraction des caractéristiques avec le système flou optimisé.

III.5 Le module comparaison

Nous avons vue dans le premier chapitre c'est quoi un module de comparaison et leur utilisation dans un système biométrique.

Il existe plusieurs travaux qui utilisent la méthode de « **Distance Euclidienne** », ainsi nous avons procédé à la comparaison de l'image de test approximé avec le modèle flou et les « signatures » (modèles) déjà mémorisés dans la base de données. La distance euclidienne est une distance géométrique dans cet espace multidimensionnel. Elle est calculée comme suit[1] :

$$d(\theta, \theta_j) = \sum_i ((\theta_{icpj} - \theta_{ji})^2)^{\frac{1}{2}}$$

θ_j : Vecteur caractéristique de l'empreinte de reconnaissance.

θ_{icpj} : Vecteur caractéristique dans la base de données (le modèle de comparaison).

Tandis que « i » est l'indice de la composante dans le vecteur.

Cette distance sera ensuite normalisée entre 0 et 1. Le schéma de principe du système biométrique proposé est comme suit :

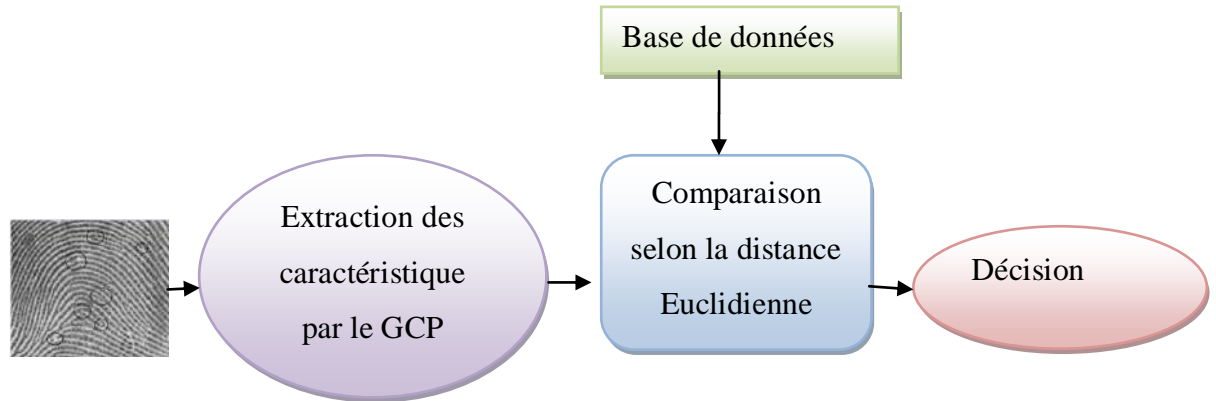


Fig III.4 Système biométrique proposé.

III.6 L'adaptation des paramètres

Le but de cette section est l'estimation des paramètres qui assure des meilleures performances. Pour cela, nous suivons les étapes suivantes:

III.6.1 Nombre des fonctions d'appartenances du système

Nous fixons le nombre des itérations à 20, et nous varions Nfa, le nombre des fonctions d'appartenances du système flou. Les résultats sont regroupés dans le tableau suivant.

Tableau III.1: Influence du nombre des fonctions d'appartenances.

Nfa	ROR	EER
5	94.33	0.841
10	97.80	0.355
15	97.44	0.442
20	97.11	0.525
25	96.86	0.625
30	96.75	0.644

➤ **Analyse des resultants**

Le tableau résume la variation du nombre des fonctions d'appartenances du flou **Nfa** en tenant compte des valeurs de l'**EER** et du **ROR**, nous obtenons des meilleures résultats (**EER=0.355**) puisque c'est la plus petite valeur.

Concernant le (**ROR =97.80%**) est la plus grande valeur **ROR**. Nous pouvons dire que **Nfa =10** réalise le meilleur résultat. .

III.6 .2 nombre d'itérations :

Nous fixons le nombre des fonctions d'appartenance à 10, et nous faisons varier le nombre d'itération de l'algorithme GCP entre 5 et 10 avec un pas de 5.

Les resultants obtenus sont illustrés dans le tableau III.2 dans la page suivante.

Tableau III.2: Résultat de l'EER, l'ROR et ROR en fonction du nombre d'itération

Niter	ROR	EER
5	98.00	0.280
10	98.13	0.266
15	97.91	0.338
20	97.80	0.355
25	97.11	0.346

➤ **Analyse des resultants**

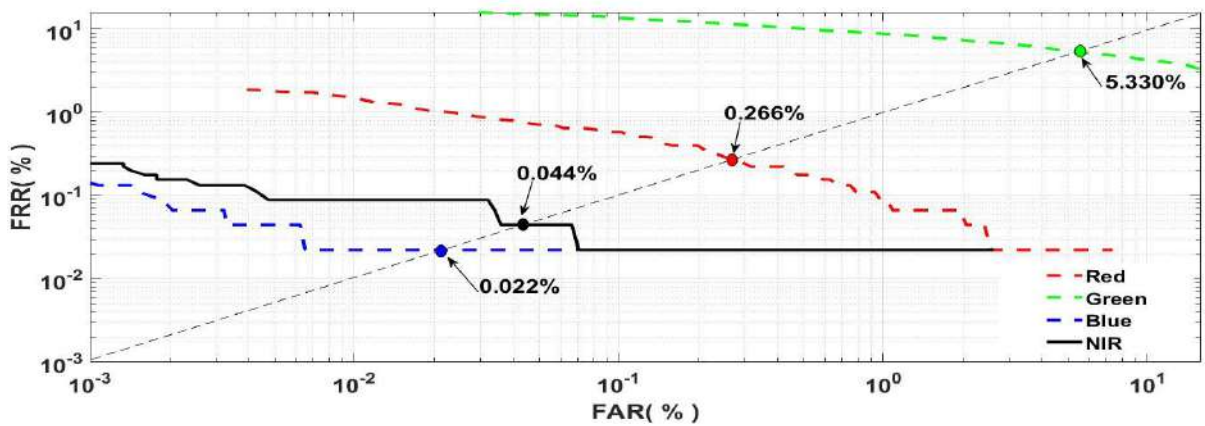
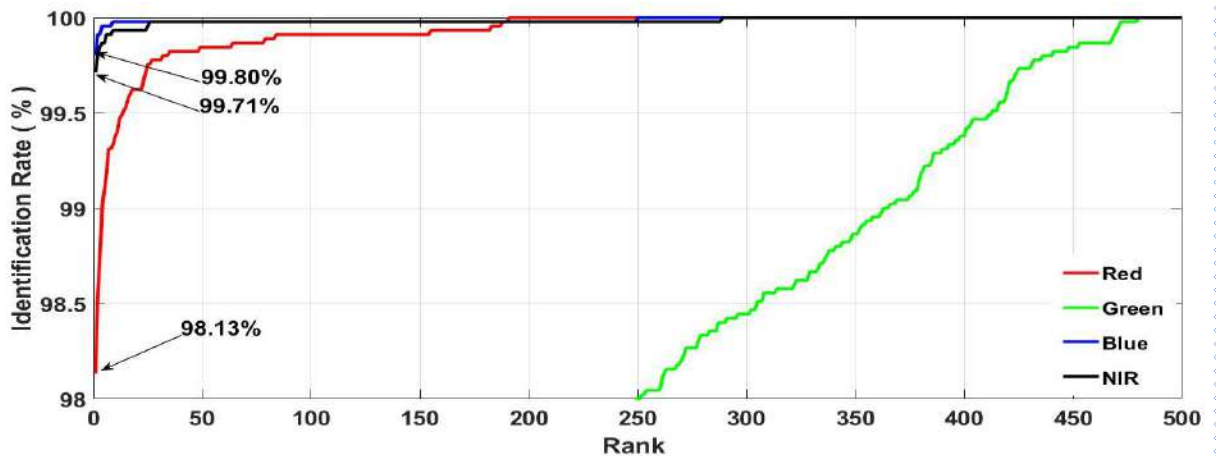
nous obtenons des meilleures résultats avec (**EER=0.266**) et (**ROR =97.80**), on peut dire que **Niter =10** réalise le meilleur résultat.

III.7 Application uni-modale

Le système biométrique peut fonctionner en deux modes ; mode ouvert ou mode fermé. Les résultats donnés au tableau III.3 ainsi que les figures III.5 et III.6 illustrent les valeurs des paramètres relatifs au mode ouvert et mode fermé pour les variétés des bandes d'images.

Tableau III.3 : Résultats de l'EER, ROR et RPR pour différentes bandes uni-modal

UN modale system résultats				
Bands	Open-set		Closed-set	
	T ₀	EER	ROR	RPR
Red	0.1338	0.266	98.13	191
Green	0.1398	5.331	84.06	480
Blue	0.1440	0.022	99.80	250
Nir	0.1570	0.044	99.71	289

**Fig. III.5.:Performance du système uni-modale (ROC)****Fig. III.6: Performance du système uni-modale (CMC)**

➤ Analyse des résultats

La figure III.5 montre les courbes caractéristiques (*Receiver Operating Characteristic* (ROC)) du test de performances du système d'identification opérant en mode fermé. La figure

III.6, montre les courbes des scores cumulés (*Cumulative Match Curve (CMC)*) du système basé sur les différentes bandes d'images du système.

La lecture de ce tableau nous permis de conclure sur la qualité des résultats pour les différentes bandes comme suit : La bande bleue est la meilleure puisque son **EER = 0.022** est le minimum ; et son **ROR=98.13%** est le maximum. Concernant la bande **NIR**, nous remarquons que son **EER=0.044** , et son **ROR=99.71%** enregistrés sont en deuxième position. La bande **RED** enregistre **des résultats RPR et ROR** en troisième position. Tandis que la bande **GREEN** possède les plus mauvais résultats (EER important et un ROR le plus grand).

III.8 Application Multimodale

Dans cette section, nous effectuons des expérimentations sur un système multimodale de type multi-échantillons, nous avons procédé à l'ensemble des tests de fusions selon la méthode suivante :

- Nous avons fusionné les deux bandes

la BLEU, la RED et la GREEN.

Avec l'enregistrement des valeurs de **EER**, le seuil (treeshold), le **ROR** et le **RPR**

- . Dans la deuxième étape de la même manière. nous fusionnons les bandes :

la RED , le BLEU, la NIR et la GREEN

avec les paramètres l'**EER**, le seuil, le **ROR** et le **RPR**.

Le tableau ci-après résume les résultats

Tableau III.4 : Résultats de l'EER, ROR et RPR pour différentes bandes multimodale

Multimodal system results								
	R+G+B				R+G+B+NIR			
	Open-Set		Closed-Set		Open-Set		Closed-Set	
Rules	T0	EER	ROR	RPR	T0	EER	ROR	RPR
Sum	0.1561	0.066	99.80	03	0.1835	0.032	100	01
Mul	0.022	0.083	88.20	03	0.011	0.039	88.20	03
Min	0.024	0.088	88.20	03	0.083	0.044	88.20	03
Max	0.2141	0.133	99.20	124	0.2666	0.088	99.80	02
W Sum	0.1517	0.026	100	01	0.1639	0.022	100	01

A partir des résultats, nous constatons que les deux systèmes multimodales conservent les mêmes performances en matière de l'erreur EER (maintenu à 0.22 avec la méthode de fusion par multiplication dans le cas de trois bandes et la méthode de fusion sommation pondérée dans le cas de quatre bandes.

Cependant, en ensemble fermé (Closed-set), les deux méthode peuvent atteindrent un taux de reconnaissance ROR idéale qui est égale à 100% qui est supérieur au taux de reconnaissance ROR en uni-modale qui était au maximum 99.80% dans le cas de la bande BLEU.

III.9 Conclusion

Nous concluons la validité de la méthode proposée. L'optimisation a permis la création de vecteur caractéristique de l'empreinte identifiée. Les résultats expérimentaux montrent l'efficacité de l'algorithme du gradient conjuguée et une très bonne reconnaissance en ensemble fermé avec un système multimodale.

Conclusion Générale

Conclusion générale

L'objectif générale de ce mémoire est l'identification biométrique des personnes basée sur la modélisation par les systèmes flous.

Nous avons développé l'application de l'algorithme du gradient conjugué pré conditionné (GCP) pour l'optimisation du modèle flou de Sugeno dans le sens d'approximer l'image numérique de l'empreinte palmaire.

Nous avons proposé une méthode assurant la convergence avec une amélioration de la vitesse de convergence par le biais d'optimisation avec l'algorithme du GCP.

L'ensemble des paramètres du modèle flou est déterminé par optimisation de l'erreur quadratique moyenne d'approximation de l'image numérique de l'empreinte par un modèle flou de Sugeno.

Nous avons proposé de considérer le vecteur des paramètres du modèle flou comme vecteur caractéristique du système biométrique d'identification.

L'application de cet algorithme au cas d'une base de donnée palmaires a montrés des bonnes performances en matière d'erreur EER et du taux de reconnaissance ROR.

En système biométrique uni-modal l'erreur EER est réduite à une valeur de l'ordre de 0.022 avec un taux de reconnaissance 99.88% obtenu particulièrement avec la bande BLEU.

L'utilisation d'un système biométrique multi-modal, nous a permis l'amélioration du taux ROR pour atteindre un niveau idéal (100%

Bibliographies

- [1] <http://biometrie.online.fr/> 01-04-2019
- [2] Lorène ALLANO La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles 2009
- [3] Ibtissam Benchennane, "Etude et mise au point d'un procédé biométrique
- [4] HADJAIDJI .Khaled MAHDADI Modélisation d'empreinte biométrique par un modèle 2017
- [5] BARKA .BOUKHRIS Système d'identification biométrique à base d'un modèle flou 2016 multimodale pour la reconnaissance des individus ". Université Oran Mohamed Boudiaf, thèse Doctorat 2016.
- [6] Abderahmane BENAGGA, Lina TELIB, "Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt ".UKM Ouargla, Master Académique ,2016.
- [7] Mr. SAMAI Yacine. "Reconnaissance de l'Iris humain en utilisant les méthodes de l'Intelligence Artificielle. "Uni ELHADJ LAKHDAR Batna .diplôme de Magister 2012
- [8] GUERFI ABABSA " Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D ". Université Evry Val d'Essonne ,2008.
- [9] flou de Sugeno optimisé Jain et *al.*, 2003
- [10] Boukhari Wassila Identification Biométrique des Individus par leurs Empreintes Palmaires « Palmprints » : Classification par la Méthode des Séparateurs à Vaste Marge (SVM)
- [11] Hanène Guesmi Identification de personnes par fusion de différentes modalités biométriques 2015
- Lorène ALLANO La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles 2009
- [12] I. Danaïla, F. Hecht, O. Pironneau, Simulation numérique en C++, Dunod, 2003 Algorithmes et techniques avancées de programmation
- [13] adjaine .lamri stady and design of bagstping aberver 2010
- [14] Max CHASSE," La biométrie au Québec ". Les enjeux Préparé Analyste en

informatique, 2002.

[15] Mohamed SANDELI, "Traitement d'images par des approches bio-inspirées Application à la segmentation d'images" Université Constantine 2, Magister en informatique,2014.

[16] Chérif TAOUCHE," Implémentation d'un Environnement Parallèle pour la Compression d'Images à l'aide des Fractales ". Uni Mentouri Constantine diplôme de magister 2005.

[17] Sarra BENFRIHA et Asma HAMEL," Segmentation d'image par Coopération région-contours". UKM Ouargla, Master Professionnel,2015/2016.

[18] Abderahmane BENAGGA, Lina TELIB, "Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt ".UKM Ouargla, Master Académique ,2016.

[19] S. K. Panigraphy, Jena, D. & Jena, S. K. A Rotational- and Translational-Invariant Palmprint Recognition System. Tiruchirapalli, s.n., pp. 380-383. 2008

[20] D. D. Zhang, Line features extraction and representation. Dans: Palmprint Authentification. s.l.:Springer. 2004

[21] R. Belguechi, Contribution à la reconnaissance d'empreinte digitales par une approche hybride, s.l.: s.n. 2006

[22] Rapport technique Tour d'horizon des technologies biométriques Projet CCT – PFPDT – juin 2012.

[23] <http://www-asim.lip6.fr/~marzouki/perso/publi/cnil-biometrie01.html> a 22-05-2019

ملخص

تعد التقنيات البيومترية القاعدة الأساسية للتعرف الآمن على الأشخاص التي تعرف انتشارا واسعا في كل المجالات خاصة الأمنية منها, لما تتسم به من سهولة في الاستخدام. حيث تعتمد هذه الأنظمة في التعرف على مختلف السمات المميزة للجسم البشري من بينها: بصمات الأصابع، الوجه، بصمة راحة اليد، شبكية العين... الخ. حيث تتبوأ بصمة راحة اليد مكانة متميزة بين المحددات البيومترية المتنوعة نظراً لما تتمتع به من مزايا، وقد تم اعتمادها في تصميم النظام المقترح كنظام عام الاستخدام. يركز العمل الذي نقوم به كجزء من هذه المذكرة على التعرف على الأشخاص انطلاقاً من بصمة راحة اليد و هذا باستخدام نظام التعرف أحادي الوسيطة و متعدد الوسائط.

Abstract

Biometric technologies constituted the basic rule for the identification of the identity. These systems have known a spread particularly in the areas of security, due to its convenient and easy to use. To identify persons, they rely on different distinguishing features of the human body such as fingerprints, face, the palm print and retina, etc. Where palmprint occupies a privileged position among the various biometric technologies because of its benefits, it was adopted in the proposed biometric system. The work that we propose as part of this memory is within the scope of the verification and 'identification of persons by multispectral palmprints based on a uni-modal and multimodal recognition system.

Résumé

Les technologies biométriques constituées la règle de base pour l'identification de l'identité. Ces systèmes également ont connu une propagation en particulier dans les tout les domaines, en raison de sa pratique et facile à utiliser. Pour identifier les personnes, ils s'appuient sur les différents traits distinctifs du corps humain tels que : les empreintes digitales, le visage, l'empreinte palmaire et la rétine, etc. Là où l'empreinte palmaire occupe une position privilégiée entre les divers techniques biométriques en raison de ses avantages, elle a été adoptée dans le système biométrique proposé. Le travail que nous proposons dans le cadre de ce mémoire rentre dans le cadre de la vérification et l'identification des personnes par les empreintes palmaires multi-spectrales à base d'un système de reconnaissance uni-modal et multimodal.