République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Ferhat Abbas Sétif 1

THÈSE

Présentée à la Faculté des Sciences

Département d'Informatique

En vue de l'obtention du diplôme de

Doctorat en science

Option : Informatique

Par

Houda Benaliouche

Thème

Multimodalité Biométrique dans le cadre d'une Application d'Authentification

Soutenue le : 21 février 2016 devant la commission d'examen :

Président :	**Khababa Abdallah**	**Professeur**	**Université Sétif -1-**
Examinateur :	**Amirat Abdelkrim**	**Professeur**	**Université de Souk Ahras**
Examinateur :	**Boubetra Abdelhak**	**Professeur**	**Université de BBA**
Examinateur :	**Kazar Okba**	**Professeur**	**Université de Biskra**
Rapporteur :	**Touahria Mohamed**	**Professeur**	**Université Sétif -1-**

ملخص

في هذه الأطروحة نتعرض الى ثلاث تقنيات جديدة خاصة بالتشخيص البيومتري باستعمال دمج ومطابقة الشفرة البيومترية .

اولا داخل نظام تشخيص بيومتري عن طريق دمج عدة بصمات لعدة أصابع على مستوى مرحلة استخراج النقاط المميزة.

ثانيا داخل نظام تشخيص بيومتري عن طريق دمج عدة خوارزمات خاصة بتشخيص حدقة العين على مستوى مرحلة حساب نتيجة قرار التشخيص.

ثالثا وأخيرا داخل نظام تشخيص بيومتري عن طريق دمج عدة خوارزمات خاصة بتشخيص حدقة العين و بصمة الأصابع على مستوى ثلاث مراحل؛ مرحلة استخراج النقاط المميزة و مرحلة حساب نتيجة قرار التشخيص ومرحلة القرار.

خوارزم الدمج المستعمل يعتمد على فكرة المنطق الغامض الملائم للصور البيومترية الغير واضحة وبذلك تتحسن درجة التشخيص وتقل نسبة الخطأ.

Résumé

La biométrie multimodale consiste à combiner plusieurs modalités biométriques, ou plusieurs échantillons ou instances biométriques du même trait, ou encore utiliser plusieurs capteurs ou appliquer plusieurs extracteurs au même trait biométrique. Elle est de plus en plus utilisée de nos jours. En effet, elle permet de pallier les limites observées dans les systèmes biométriques uni-modaux comme le manque d'individualité et la sensibilité aux attaques, tout en améliorant l'efficacité et la performance de la reconnaissance.

Dans ce travail nous présentons trois éléments de contribution, montrant chacun un type de la biométrie multimodale.

- La première contribution concerne la proposition d'un algorithme d'identification par l'iris à base de deux algorithmes d'appariement. Dans cette proposition nous utilisons la fuzzification des résultats de la reconnaissance marquée par le degré d'appartenance aux ensembles flous modélisant les décisions du système, ce qui offre un intervalle intermédiaire entre la décision d'accepter le client et la décision de le rejeter. Le système peut donc, par exemple, déclarer une authentification comme « *fortement accepter* », ou bien « *fortement rejeter* ». Nous agissons au niveau de la phase d'appariement en appliquant deux algorithmes d'appariement différents et en essayant de voir l'influence et l'apport de la fusion par l'inférence floue sur les résultats de la reconnaissance du système.
- La deuxième contribution concerne La proposition d'un nouvel algorithme de la reconnaissance par empreinte digitale assurant l'identification par instances répétées (plusieurs impressions du même doigt) et multiples (plusieurs doigts) d'empreintes digitales. La fusion est établie au niveau *caractéristique* (*feature level*). A ce niveau de fusion, Choisir de combiner les informations biométriques provenant d'instances répétées et/ou multiples engendre un ensemble de caractéristique (*feature set*) plus riche en information biométrique que d'utiliser la fusion au niveau *Score* ou bien au niveau de *Décision*. En plus, il assure la détection des points de caractéristiques biométriques redondants qui seront supprimés avant l'appariement. Cet avantage n'est pas offert par la fusion au niveau *Score* ou bien au niveau de D*écision*, ensuite, Choisir la fusion au niveau caractéristique est idéal quand les codes à fusionner sont homogènes (dans notre cas les codes sont tous des codes d'instances d'empreinte). Nous avons mesuré la *Spécificité* et la *Sensibilité* de l'algorithme proposé en utilisant une instance, trois instances puis huit instances de l'empreinte et on a déduit à propos de la meilleure combinaison. Le critère de la *Spécificité* mesure la pertinence du système à éviter les fausses détections, le critère de la *Sensibilité* mesure la pertinence du système à détecter les vraies minuties. Les résultats expérimentaux ont montrés que la précision de la reconnaissance est améliorée chaque fois on fusionne plus d'instances.
- La troisième contribution concerne La proposition d'un nouvel algorithme de fusion multimodale d'iris et d'empreinte digitale à base de la logique floue. Nous avons tenu à Concevoir plusieurs scénarios de fusion et les comparer afin d'en tirer conclusion à propos du meilleur scénario de fusion. Les méthodes de fusion utilisés sont *la Règle Somme*, *la règle somme pondérée* et *l'inférence floue*. La méthode de la fusion multimodale par *inférence floue* a réalisée un meilleur compromis entre le taux de fasse acceptation TFA et le taux de faux rejet TFR par rapport aux travaux de recherche sur l'identification par fusion d'iris et d'empreinte.

Abstract

Multimodal biometrics, which is defined as the use of several sensors or instances of the same biometric trait, or even applying several extractors to the same biometric modality, or simply fusing different biometrics, is widely used today. It can overcome the limitation possessed by single biometric trait like the lack of individuality and sensitivity to attacks and give better classification accuracy.

In this work we present three contributions each showing one facet of multimodal biometrics:

- The first contribution is the proposition of a new matching algorithm for iris recognition based on *fuzzy inference*. Two matching algorithms are applied to the biometric data and their decisions are fused following a series of fuzzy if-then rules. The experimental results were conducted on the public CASIA-Iris V1 database and showed that the system accuracy of the proposed scheme is enhanced compared to those of the monomodal iris recognition works reported from the current literature.
- The second contribution is the proposition of a new recognition algorithm for fingerprint modality based on the concatenation of fingerprint codes at *feature extraction* level. Repeated impressions of the same finger are fused. Three experiments were carried out using respectively one fingerprint instance, three fingerprint instances and eight fingerprint instances per finger. The database used to measure the performance of our system is FVC2000. *Specificity* and *Sensitivity* evaluation metrics are calculated and then compared; error rates are calculated for each experiment, tests indicates that specificity and sensitivity metrics reach high percentages as well as the number of fingerprint instances per finger increase. An equal error rate of 0.025 is achieved. The approach is compared to the most known fingerprint recognition systems in the current literature.
- The third contribution investigates the comparative performance from three different approaches for multimodal recognition of combined iris and fingerprints: *Classical Sum Rule*, *Weighted Sum Rule*, and *Fuzzy Logic Method*. The scores from the different biometric traits of iris and fingerprint are fused at the matching *Score* and the *Decision* levels. The scores combination approach is used after normalization of both scores using the M*in-Max Rule*. Our experimental results suggest that the *Fuzzy Logic method* for the matching scores combinations at the *Decision* level is the best followed by the C*lassical Weighted Sum rule* and the C*lassical Sum rule* in order. The performance evaluation of each method is reported in terms of matching time, error rates, and accuracy after doing exhaustive tests on the public CASIA-Iris databases V1 and V2 and the FVC 2004 fingerprint database. Experimental results prior to fusion and after fusion are presented followed by their comparison with related works in the current literature. The fusion by fuzzy logic decision mimics the human reasoning in a soft and simple way and gives enhanced results.

Remerciements

Je tiens tout d'abord à remercier Dieu le tout Puissant et Miséricordieux, qui m'a donné la force et la patience d'accomplir ce Modeste travail.

En second lieu, je tiens à remercier mon directeur de thèse Monsieur le Professeur THOUAHRIA Mohamed, pour son précieux conseil et son aide durant toute la période de la thèse. Je le remercie également pour l'orientation, la confiance et la patience qui ont constitués un apport considérable sans lequel ce travail n'aurait pas pu être mené au bon port.

Je remercie le Professeur KHABABA Abdallah d'avoir accepter de présider ce jury, qu'il trouve toute ma gratitude. Je remercie le Professeur AMIRAT Abdelkrim de l'université de Souk Ahras, pour l'honneur qu'il me fait, en acceptant d'évaluer ce travail. Que le Professeur BOUBETRA Abdelhak de l'université de BBA trouve également toute ma gratitude en acceptant de faire partie de ce jury, je tiens à présenter tous mes remerciements au Professeur KAZAR Okba de l'université de Biskra pour le temps consentis à l'évaluation de cette thèse.

Je remercie également Monsieur le Professeur Benmohamed Mohamed qui a su me faire confiance dès ma première année de Magister et qui a toujours été d'excellents conseils, qui s'est toujours montré à l'écoute et très disponible, ainsi pour l'inspiration, l'aide et le temps qu'ils a bien voulu me consacrer.

Je tiens également à remercier mon frère Docteur Benaliouche Fouad pour son aide précieuse concernant la correction des articles.

Enfin, Je remercie Monsieur Bouriche Houssem pour son aide précieuse concernant la partie implémentation de la fusion bimodale d'iris et d'empreinte. Je remercie également Monsieur Meziani Hamza pour son aide précieuse concernant la partie implémentation de la reconnaissance par empreinte.

SOMMAIRE

INTRODUCTION GÉNÉRALE

PARTIE I : LA RECONNAISSANCE BIOMÉTRIQUE

CHAPITRE 1 : LA BIOMÉTRIE MULTIMODALE

CHAPITRE 2 : LA RECONNAISSANCE PAR L'EMPREINTE DIGITALE

CHAPITRE 3 : LA RECONNAISSANCE PAR L'IRIS

PARTIE II : PARADIGMES DE RAISONNEMENT INTELLIGENT

CHAPITRE 4 : L'INTELLIGENCE ARTIFICIELLE

CHAPITRE 5 : LA LOGIQUE FLOUE

PARTIE III : LA BIOMÉTRIE MULTIMODALE : APPROCHES PROPOSÉES

CHAPITRE 6 : LA RECONNAISSANCE D'IRIS PAR FUSION DE DÉCISIONS

CHAPITRE 7 : FUSION D'EMPREINTES AU NIVEAU CARACTÉRISTIQUE

CHAPITRE 8 : RECONNAISSANCE PAR FUSION D'IRIS ET D'EMPREINTE

LISTE DES FIGURES

LISTE DES TABLES

LEXIQUE DE LA BIOMÉTRIE

Authentification	Procédé permettant de vérifier l'identité d'une personne selon deux étapes : 1. L'utilisateur fournit un identifiant « Id » au système de reconnaissance (par exemple un numéro d'utilisateur) 2. L'utilisateur fournit ensuite un échantillon biométrique qui va être comparé à l'échantillon biométrique correspondant à l'utilisateur « Id » contenu dans la base de données biométrique du système. Si la comparaison correspond, l'utilisateur est authentifié.
Identification	Procédé permettant de déterminer l'identité d'une personne. Il ne comprend qu'une étape. L'utilisateur fournit un échantillon biométrique qui va être comparé à tous les échantillons biométriques contenus dans la base de données biométriques du système. Si l'échantillon correspond à celui d'une personne de la base, on renvoie son numéro d'utilisateur. Sinon l'identification échoue.
Biométrie comportementale	Il s'agit d'un type de biométrie caractérisée par un trait d'attitude qui est appris et acquis au fil du temps (par exemple sa façon de signer un document, de marcher, d'utiliser un clavier...) plutôt que par une caractéristique physiologique
Capteur biométrique	Dispositif d'acquisition permettant d'obtenir une représentation numérique d'un élément du corps humain.
Capture	Méthode de collecte d'un échantillon biométrique d'un utilisateur.
Caractéristique Biométrique	La plupart des systèmes biométriques ne comparent pas directement les données acquises (image, son, etc.). On utilise plutôt différentes méthodes mathématiques pour extraire une quantité de données moins importante, mais contenant l'essentiel de l'information permettant de différencier deux individus (par exemple les minuties dans le cas de l'empreinte digitale). Ces données sont des éléments caractéristiques.
Classification	Ce procédé permet d'affecter une donnée biométrique à une classe donnée. La classification est utilisée par exemple par certains systèmes de reconnaissance d'empreintes digitales (avec des classes telles que : boucles, arches ou tourbillons), dans le but d'accélérer les identifications. En effet, la séparation des données en plusieurs classes permet de réduire la taille de la base de recherche et donc d'accélérer le processus
Comparaison	Processus d'évaluation de correspondance d'un échantillon biométrique avec un ou plusieurs modèle(s) de référence précédemment stocké(s).

Correspondance	Processus de comparaison d'un échantillon biométrique avec une référence déjà stockée et évaluation du degré de similarité. Une décision d'acceptation ou de rejet est fondée sur le dépassement ou non du seuil par le score.
Critère-de performance	Critère prédéterminé établi pour évaluer la performance d'un système biométrique et tester le degré de liberté.
Degrés de liberté	Nombre de données statistiquement indépendantes contenues dans un échantillon biométrique. Cela exprime la complexité d'une donnée en terme de quantité d'information.
Donnée biométrique	Information extraite d'un échantillon biométrique et utilisé soit pour construire un *modèle de référence* ou pour comparer à des modèles existants
Échantillon biométrique	Représentation sous forme numérique d'un élément du corps humain. On obtient un échantillon biométrique à l'aide d'un capteur biométrique
Échec à l'enrôlement	Événement ayant lieu lorsqu'une personne ne réussit pas à s'enrôler. Ceci inclut les cas où la personne ne peut pas fournir l'échantillon biométrique demandé, les cas où la qualité de l'échantillon est insuffisante, etc
Taux d'échec à l'enrôlement	Evaluation statistique de la partie de la population ne pouvant pas être enrôlée sur un système donné. Ce taux dépend de la méthode de capture, du capteur et de l'algorithme utilisé ainsi que des caractéristiques de la population étudiée
Empreinte digitale	Motif formé par les crêtes et les vallées du relief cutané
Empreinte latente	Trace d'empreinte laissée sur un objet après contact entre celui-ci et un doigt. C'est ce type d'empreintes qui est relevé sur les scènes de crime
Enrôlement	Étape initiale au cours de laquelle sont capturées les données biométriques qui serviront de références lors des authentifications ou identifications futures. C'est aussi lors de cette étape qu'un identifiant est associé aux données biométriques de chaque personne. Un soin tout particulier doit être apporté à cette première capture, car c'est sa qualité qui déterminera les performances futures du système
Extraction	Processus de conversion d'un échantillon biométrique capturé en donnée biométrique pouvant être comparée au modèle de référence
Fausse Acceptation	Événement ayant lieu lorsqu'un système biométrique accepte une personne alors qu'elle n'est pas dans sa base d'utilisateurs. Cet événement doit être le plus rare possible pour assurer la sécurité d'un système biométrique
Faux Rejet	Événement ayant lieu lorsqu'un système biométrique refuse une personne alors qu'elle est dans sa base d'utilisateurs. Cet événement est souvent dû à une mauvaise acquisition des données biométriques et est perçu comme une gène par l'utilisateur

TFA	Taux de Fausse Acceptation : Indique la probabilité qu'un utilisateur inconnu soit identifié comme étant un utilisateur connu. Ce taux définit la sécurité du système biométrique.
TFR	Taux de faux rejet : Indique la probabilité qu'un utilisateur connu soit rejeté par le système biométrique. Ce taux définit en partie le confort d'utilisation du système biométrique.
TEE	Taux d'égale erreur : Donne un point pour lequel le TFA est égal au TFR.
Gabarit	En anglais : Template. Modèle initial créé au cours de l'enrôlement. Modèle mathématique décrivant certaines caractéristiques physiques ou comportementales d'un individu. On comparera par la suite les demandes de reconnaissance à ce modèle.
Iris	Partie colorée de l'œil, percée en son centre par la pupille. L'iris se contracte en fonction de la luminosité ambiante pour laisser passer plus ou moins de lumière à travers la pupille. La couleur de l'iris est déterminée par la quantité de mélanine qu'elle contient. L'iris est bleu quand la mélanine est peu concentrée, elle devient plus foncée quand sa concentration augmente. Lors d'une analyse biométrique de l'iris, la couleur de celle-ci n'est pas prise en compte. Seul le motif complexe formé par sa texture est pris en compte.
Appariement (*Matching*)	Procédé mathématique permettant d'effectuer la comparaison de deux échantillons biométriques.
Minuties	Petites imperfections dans le flot des lignes cutanées d'une empreinte digitale. Il en existe différents types (îlot, lacs, etc.) mais seules deux sont utilisées dans les applications informatiques de reconnaissance. les fins de lignes et les bifurcations
Reconnaissance d'empreintes	Les minuties ne sont qu'un type d'élément caractéristique utilisé par les systèmes de reconnaissance. Certains systèmes utilisent d'autres méthodes pour effectuer la reconnaissance (analyse de texture par exemple).
Modèle de référence	Donnée représentant une caractéristique biométrique d'un individu utilisée par un système biométrique pour permettre la comparaison avec des échantillons soumis a posteriori
Moteur biométrique	Ensemble d'algorithmes permettant l'enrôlement, le matching, ainsi que toutes les étapes intermédiaires du procédé de reconnaissance d'un élément biométrique (amélioration des images, détermination de la qualité, extraction des caractéristiques discriminantes, etc).

Prétendant	Personne soumettant un échantillon biométrique pour vérification d'une identité.
ROC Curve (*Receiver Operating Caracteristics curve*)	Dans le cadre biométrique, cette courbe représente l'évolution du FRR en fonction du FAR. L'étude de cette courbe permet de déterminer les performances d'un système biométrique.
Seuil de décision	L'acceptation ou rejet d'une donnée biométrique dépend du passage du score de correspondance au-dessus ou au-dessous du seuil. Ce dernier est ajustable pour rendre le système biométrique plus ou moins strict, cela dépend des éléments requis par tout système application biométrique.
Seuil de rejet	Score minimum en dessous duquel un algorithme biométrique rejettera une authentification / identification
Seuil d'acceptation	Score au dessus duquel un algorithme biométrique acceptera une authentification/identification.
Système Biométrique	Dispositif automatisé permettant de : 1. Acquérir des données biométriques 2. Extraire des informations discriminantes à partir de données 3. Comparer ces informations avec celles contenues dans un ou plusieurs gabarits servant de référence. 4. Décider s'ils correspondent 5. Indiquer à l'utilisateur si l'authentification ou l'identification a réussi ou échoué.
Système multimodal	Système utilisant différents moyens d'authentification (biométriques ou non) pour vérifier l'identité d'une personne.
Taux d'erreur égal	Quand le seuil de décision d'un système est établi pour que la proportion de faux rejet soit approximativement égale à la proportion de fausse acceptation on a un taux d'erreur égal.
Temps de réponse	Période temporelle requise par un système biométrique pour retourner une décision sur l'authentification d'un échantillon biométrique

INTRODUCTION GENERALE

Introduction

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. D'autre part, les caractéristiques physiques sont loin d'être si parfaites et si précises, et l'on atteint très vite des limites pour ces techniques.

La biométrie trouve ses origines dans des procédés de reconnaissance *anthropométrique*, le plus ancien étant l'analyse des empreintes digitales. L'empreinte du pouce servait déjà de signature lors d'échanges commerciaux à Babylone dans l'Antiquité et en Chine au 7 ème siècle. Dans une époque beaucoup plus proche, au 19ème siècle, *Alphonse Bertillon*, grand criminologiste français, invente une méthode Scientifique appelée "anthropologie judiciaire" permettant l'identification de malfrats d'après leurs mesures physiologiques. De nos jours, la puissance de calcul grandissante des ordinateurs peut être mise à contribution pour reconnaître des individus, grâce à des appareils couplés à des programmes informatiques complexes [Wikipédia, 2013].

Depuis plusieurs années, des efforts importants sont fournis dans le domaine de la recherche en biométrie. Ce constat s'explique par la présence d'un contexte mondial dans lequel les besoins en sécurité deviennent de plus en plus importants et où les enjeux économiques sont colossaux. Les applications biométriques sont nombreuses et 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, casinos, etc.).

La biométrie est un domaine de recherche actuel, qui connait des progrès rapides et intéressants où les différentes inventions technologiques améliorent la capacité de l'être humain à identifier une personne.

Les buts de la biométrie sont multiples :

- Remplacer des méthodes anciennes susceptibles à l'oubli, la fraude, le vol, etc.
- Protéger les systèmes, les individus, contre la fraude et le vol.
- Assurer la haute sécurité dans les applications : comme par exemple l'association de la biométrie aux techniques de la cryptographie, les cartes à puces, etc.
- Assurer le confort dans l'utilisation, comme par exemple le remplacement des mots de passe par l'authentification biométrique, la biométrie évite aux administrateurs de réseaux d'avoir à répondre aux nombreux appels pour perte de mot de passe (que l'on donne parfois au téléphone, donc sans sécurité).
- Changer le comportement des consommateurs pour gagner leur confiance, surtout dans le domaine du commerce électronique.

Positionnement du travail de recherche

Le travail de recherche mené dans cette thèse porte sur *la reconnaissance biométrique par fusion multimodale*. Les points suivants sont étudiés :

- Apport de la logique floue lors de son introduction dans un système biométrique.
- Apport de l'introduction d'information supplémentaire relative principalement à la qualité du trait biométrique dans un système de reconnaissance biométrique.
- Etude d'une nouvelle alternative de classification des scores d'appariement et la comparer avec l'approche classique de normalisation des scores.

Nous nous sommes intéressés à la théorie des sous ensembles flous afin de représenter l'imprécision des données, mais également d'autoriser l'expression de préférence dans les critères de sélection de l'identité biométrique. L'utilisateur peut donc exprimer des requêtes larges fournissant des résultats classés par ordre de préférence.

Cadre de la thèse

Le cadre de ce travail est présenté par la figure 1.1. La biométrie multimodale, et plus particulièrement le traitement de l'iris et de l'empreinte digitale, peut être vue comme un croisement de trois domaines de l'Intelligence Artificielle : la reconnaissance des formes, l'apprentissage automatique et la fusion d'information.

La biométrie fait appel aux notions de l'intelligence artificielle, l'objectif principale des méthodes biométriques est d'essayer au maximum de mimer la perception et le raisonnement de l'être humain, qui décide génieusement si un prétendant est authentique ou imposteur. Ceci est expliqué clairement, par exemple, dans la reconnaissance faciale chez l'être humain.

Un système biométrique est essentiellement un système de reconnaissance des formes, produisant une décision sur l'identification de personne par la détermination de certaines caractéristiques biologiques, morphologiques ou comportementales.

Un système de reconnaissance biométrique comporte essentiellement une phase d'apprentissage, dans laquelle le modèle est constuit.

La biométrie multimodale fait appel aux techniques de fusion d'information. Ces techniques sont multiples (opérations mathématiques, règles logiques, logique floue etc). elles présentent des point forts et des limitation, sans oublié l'adéquation à l'application biométrique et à la représentation des informations biométriques à fusionner. L'étude précieuse de ces méthodes mène à des contributions et des suggestions de nouvelles pistes de recherche dans la biométrie multimodale.

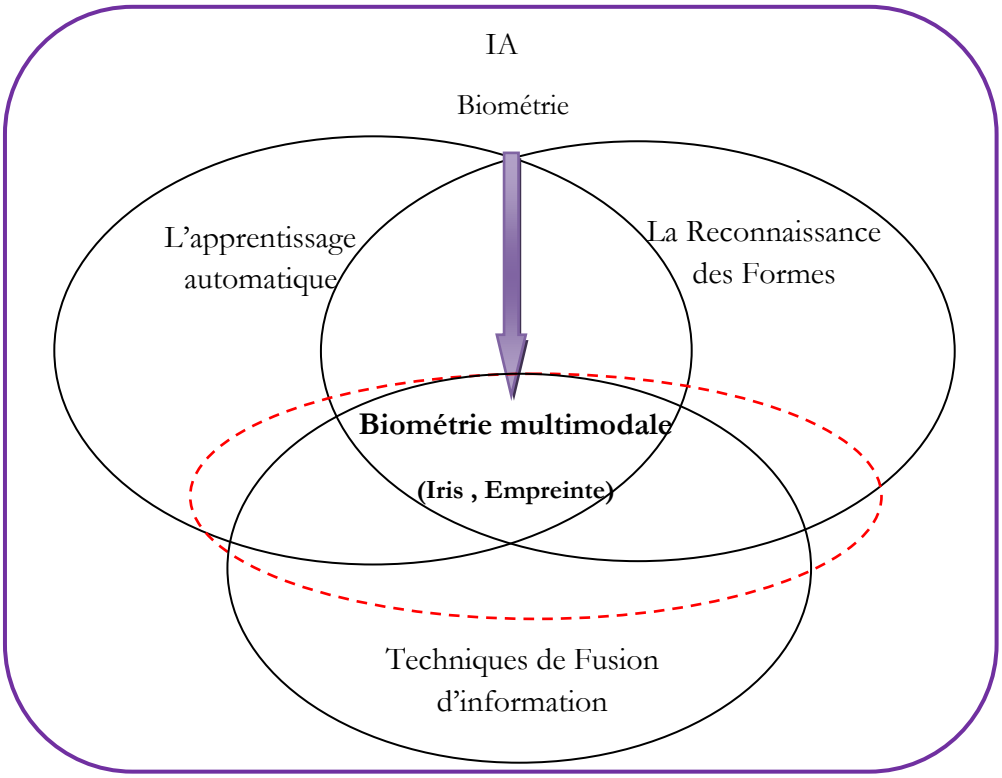


Figure 1.1. Le cadre de la thèse

Problématique

Les systèmes biométriques monomodaux soufrent de plusieurs problèmes qui les rendent inappropriés aux applications actuelles de la biométrie, exigeants de hauts degrés de fiabilité et de sécurité. Ces problèmes sont à l'origine de l'utilisation d'un seul trait biométrique susceptible au bruit, à la mauvaise capture, à la pauvreté en matière de points biométriques confidents ou encore à la détérioration de la qualité de l'entrée biométrique. L'introduction de la biométrie multimodale s'avère une solution à ces problèmes.

Objectif et Motivation du travail

Notre travail consiste à étudier, concevoir puis implémenter des systèmes de reconnaissance biométrique d'individus basés sur la fusion multimodale, en explorant plusieurs facettes de la multi-modalité (Cf. figure 1.2), à savoir :

- la multi-modalité biométrique par utilisation de plusieurs algorithmes appliqués sur le même trait biométrique (l'iris).
- La fusion d'instances répétées et multiples du même trait biométrique (l'empreinte digitale).
- et enfin réaliser la fusion de deux traits biométriques différents: l'iris qui est un trait biométrique pertinent, et l'empreinte qui est un trait biométrique bien accepté par les individus lors de l'authentification.

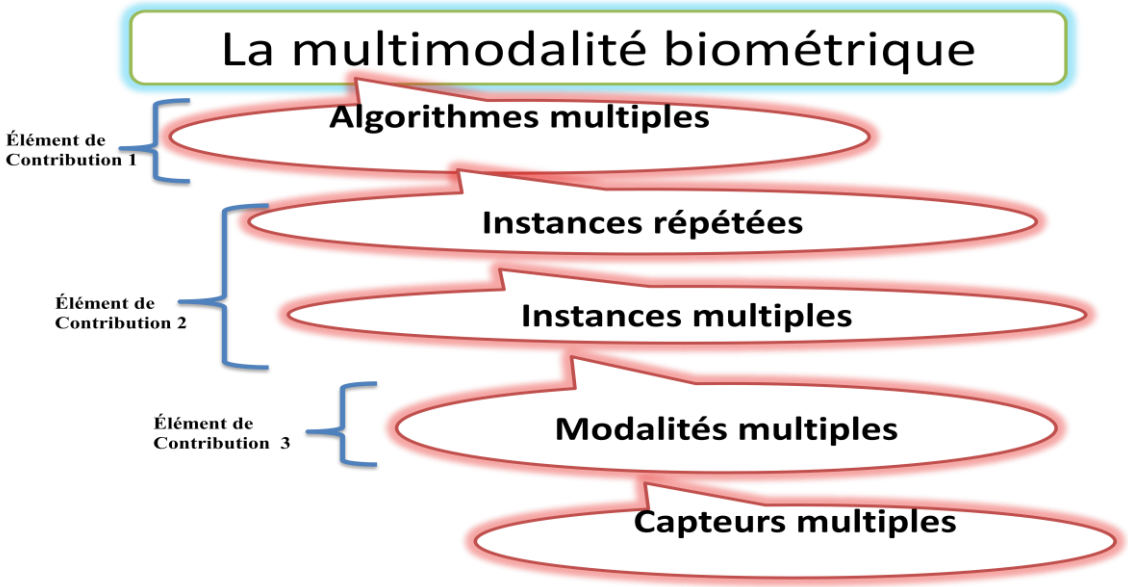


Figure 1.2: Correspondance entre les éléments de contribution et les formes de la multi-modalité.

L'union des deux traits biométrique (l'iris et l'empreinte digitale) présente l'avantage de bénéficier des avantages combinés des deux traits qui sont :

- L'acceptation de l'opération d'identification par les individus.
- La diminution des taux d'erreurs de la reconnaissance.
- La diminution des cas où le système de reconnaissance biométrique ne produit pas de résultats (cas des images très bruités, ou des empreintes à bas nombre confident de minuties, ou des images mal captées par le dispositif d'acquisition).

L'utilisation conjointe de deux traits biométriques ou plus est une tendance actuelle pour renforcer les systèmes biométriques sur les plans de sécurité, fiabilité et pertinence.

Plan de la thèse

Cette thèse est organisée en trois grandes parties : la première, porte sur la reconnaissance biométrique, la seconde partie s'intéresse aux concepts liés au domaine de l'intelligence artificielle et de la logique floue, et en fin la troisième est dédiée à l'étude expérimentale des approches développées.

Partie I : La reconnaissance biométrique.

Cette partie présente le domaine d'investigation de notre étude. Elle est constituée de trois chapitres :

Chapitre 1 : la biométrie multimodale.

Le premier chapitre est dédié aux notions de bases de la biométrie multimodale. Nous commencerons tout naturellement par introduire quelques définitions de base, puis nous présenterons quelques techniques biométriques physiologiques et comportementales, suivi par des exemples d'application de la biométrie dans la vie courante. La multi-modalité biométrique sera par la suite introduite, définit et détaillée avec des exemples, le point sera

mis sur les avantages offerts par l'utilisation de la multi-modalité par rapport aux systèmes biométriques unimodaux, les différentes stratégies de fusion multimodale et les niveaux de fusion sont définit et détaillés. Le chapitre est conclu par la présentation des critères d'évaluation des performances d'un système biométrique.

Chapitre 2 : la reconnaissance par l'empreinte digitale.

Le deuxième chapitre présente l'état de l'art de la reconnaissance par empreinte digitale, nous donnerons un historique de l'utilisation de cette technique, ensuite nous définirons les caractéristiques de l'empreinte qui la rendent unique par individu, nous détaillerons l'approche par extraction de minuties que nous choisissons pour implémenter le module monomodal de reconnaissance d'empreinte de nos implémentations, et enfin, nous présenterons les différentes méthodes d'appariements d'empreintes digitales.

Chapitre 3 : la reconnaissance par l'iris.

Le troisième chapitre présente la reconnaissance biométrique basée sur l'extraction de caractéristiques liée à l'iris. Tout d'abord nous commencerons par définir l'iris, ensuite le système biométrique de traitement d'iris et ses modes opératoires, par la suite nous présenterons un historique sur les travaux de recherche liés à la reconnaissance d'iris suivi par les principales méthodes de la reconnaissance d'iris connues dans monde de la biométrie. Nous conclurons le chapitre par citer les bases de données d'iris les plus connues et utilisées par les travaux de recherche.

Partie II : Paradigmes de raisonnement intelligent.

La seconde partie présente les notions fondamentales de l'intelligence artificielle et de la logique floue. Elle comporte deux chapitres :

Chapitre 4 : l'Intelligence Artificielle.

Ce chapitre présente une introduction au domaine de l'Intelligence Artificielle, sa définition, son fondement théorique, ses domaines d'application. Des notions de ce domaine seront présentées et expliquées (l'intelligence artificielle expérimentale, l'information, la connaissance, l'apprentissage, la reconnaissance). Le point sera mis sur les notions de l'apprentissage automatique et la reconnaissance des formes.

Chapitre 5 : La Logique Floue.

Ce chapitre présente un état de l'art sur la logique floue. Tout d'abord, nous présenterons les définitions mathématiques des sous-ensembles flous, des opérateurs flous, des valeurs linguistiques, ensuite nous détaillerons le système d'inférence flou, l'étape de *Fuzzification* et les notions de l'imprécision et de l'incertitude. Nous tenons à donner l'essentiel de cette théorie ce qui nous aide dans la conception du module d'appariement flou du système biométrique multimodal proposé. Les données pourront être également de type *imparfait* (imprécis, incertain et incomplet). C'est le cas qui nous concerne, notre problématique traite des informations imparfaites extraites des échantillons biométriques de l'iris et de l'empreinte digitale. C'est pourquoi nous discuterons en détail cette notion.

Partie III : Multimodalité biométrique : Approches proposées.

Cette partie est constituée de trois chapitres.

Chapitre 6 : Reconnaissance d'iris par fusion de décisions.

Le sixième chapitre présente un système de reconnaissance biométrique d'iris basé sur la fusion de décisions provenant de deux appariements différents sur les mêmes données biométriques. En intégrant l'information sur la qualité d'image de l'iris à la fois dans le processus d'appariement, et en second lieu dans la classification de la base de donnée, afin d'arriver à une meilleure séparabilité entre les distributions de scores de la reconnaissance.

Chapitre 7 : Fusion d'empreintes au niveau caractéristique.

Le septième chapitre montre l'application d'une approche de reconnaissance par empreinte basée sur la concaténation de codes d'empreintes au niveau *caractéristique*. Le but principal de ce travail est de trouver une solution simple, rapide et précise concernant la reconnaissance par empreintes digitales lorsque celles-ci sont de qualité détériorée. Les impressions répétées de l'empreinte sont sujettes à la variation d'inclinaison, de déformation (écrasement) ou de déplacement du doigt. Ces variations existent dans les acquisitions différentes d'une même empreinte, l'analyse de ces dernières ne donnera jamais 100% de similitudes, mais on obtiendra néanmoins toujours un pourcentage très élevé. Dans ce cadre, nous présenterons une étude quantitative visant à évaluer la pertinence de l'algorithme de fusion proposé. Les mesures de performance du matcher (l'algorithme de fusion des vecteurs de caractéristiques) sont la Spécificité P et la Sensibilité S.

Chapitre 8 : Reconnaissance par fusion d'iris et d'empreinte digitale.

Le huitième chapitre est consacré à la conception et l'implémentation d'un système de reconnaissance biométrique bimodal, utilisant comme données biométriques l'iris et l'empreinte digitale. Tout d'abord, nous commencerons par citer les motivations et les objectifs de l'approche, ensuite nous présenterons une synthèse des travaux de recherche voisins, par la suite, nous présenterons la conception détaillée du système de reconnaissance par fusion multimodale, suivi de sa validation et des résultats expérimentaux. Enfin, nous comparons ce travail avec des travaux similaires pour montrer sa valeur ajoutée

Enfin, nous dresserons une conclusion générale. Dans laquelle on reprendra les diverses contributions apportées tout au long de cette thèse et on suggèrera de nouvelles pistes de réflexion utiles dans la perspective de recherche.

Première partie

La reconnaissance biométrique

Chapitre 1

LA BIOMETRIE MULTIMODALE

1.1. Introduction

La biométrie, définit comme l'étude quantitative des caractéristiques biologiques, morphologiques ou comportementales de l'humain, constitue à l'heure actuelle une véritable alternative aux mots de passe, aux signatures, et autre identifiants. Plusieurs types de biométrie existent, comme l'empreinte digitale, l'iris, la voix, le visage, la dynamique de frappe au clavier, l'ADN, etc. Cependant, aucune biométrie n'est fiable à 100 %. C'est un fait qui, dans le cas d'applications de haute sécurité, demeure contraignant.

La biométrie multimodale consiste à combiner plusieurs systèmes biométriques monomodaux. En effet, elle permet de réduire certaines limitations de la reconnaissance monomodale, liées à l'efficacité de la reconnaissance, l'acceptabilité de l'opération d'authentification, et la fraude intentionnelle.

La multimodalité biométrique peut aussi être vue sous un autre angle; il s'agit soit de combiner des technologies hétérogènes (biométrie + badge + clavier codé, par exemple), soit d'associer plusieurs échantillons d'une même biométrie (plusieurs empreintes digitales d'un même individu, par exemple). On parle alors de « *multibiométrie* », soit d'exploiter plusieurs technologies biométriques pour l'identification (empreinte digitale + réseau veineux ou iris + forme du visage). On parle alors de *biométrie multimodale*. Ces avantages apportés par la multimodalité aux systèmes biométriques "monomodaux" sont obtenus en fusionnant plusieurs systèmes biométriques.

Dans ce chapitre nous présenterons un état de l'art sur la biométrie. Le point sera mis sur les difficultés observées dans les systèmes biométriques unimodaux tels que le degré d'erreur élevé et la mauvaise précision. L'introduction de systèmes biométriques multimodaux s'avère une solution à ces problèmes.

Nous présenterons par la suite un état de l'art sur la multimodalité biométrique. Ensuite, nous analyserons plus en détail la fusion multimodale et les systèmes multimodaux avant d'expliquer les différents niveaux de fusion possibles. Nous insisterons sur deux niveaux de fusion qui seront utilisé dans la conception du système multimodale proposé: le niveau *score* et le niveau *décision*.

1.2. Définition de la biométrie

Le mot biométrie signifie "mesure + vivant" ou "mesure du vivant", et désigne dans un sens très large l'étude quantitative des êtres vivants [Wikipédia, 2013].

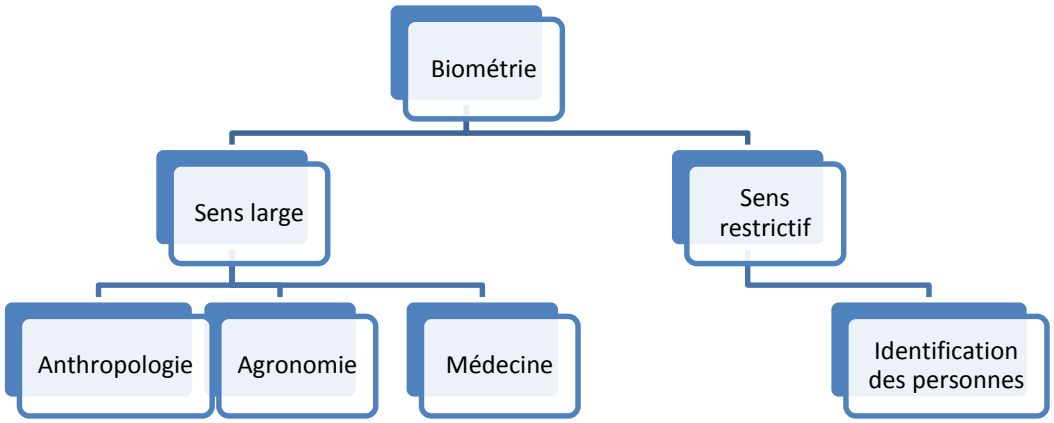


Figure 1.3 : Différents domaines d'applications de la biométrie.

La biométrie est aussi un système qui permet d'identifier automatiquement une personne en analysant (Cf. Figure 1.4) :

- Ses caractéristiques comportementales.
- Ses caractéristiques morphologiques.
- Ses traces biologiques.

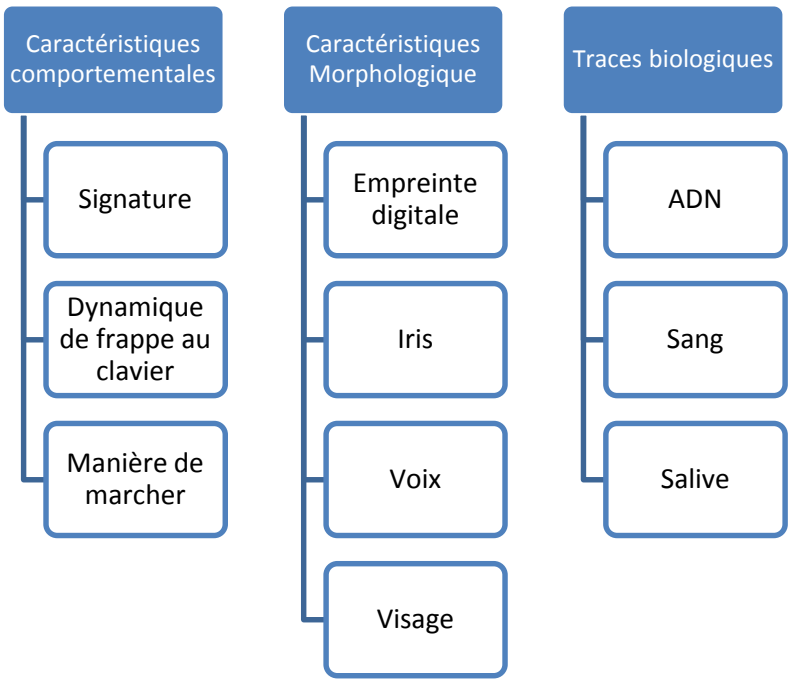


Figure 1.4 : Différentes facettes de la biométrie : biométrie comportementale, morphologique et biologique avec quelques exemples.

Les données biométriques ont la particularité d'être uniques et permanentes. Elles permettent de ce fait une identification certaine des individus. Les moyens de confirmation de l'identité comme les badges, les clés et les pièces d'identité, les mots de passe et les codes d'accès ne peuvent pas assurer l'identification d'une personne à 100%. Ils peuvent facilement être oubliés, volés, copiés ou contrefaits.
On peut constater que la biométrie est une véritable alternative aux mots de passe et autres identifiants pour sécuriser les contrôles d'accès. Elle permet de vérifier que l'usager est bien la personne qu'il prétend être.
Il existe plusieurs techniques en cours de développement à l'heure actuelle; parmi celles-ci, citons :

- La biométrie basée sur la géométrie de l'oreille.
- les odeurs.
- les pores de la peau.
- les tests ADN.

Le test ADN est une technique biométrique qui peut se révéler comme exact et sûr à 100%, autorisant des FRR et FAR nuls. Il est également reconnu de façon universelle et permettrait très facilement d'effectuer des recoupements entre bases de données.

1.3. Domaines d'applications de la biométrie

Les applications peuvent être grossièrement classées sous deux catégories [Ailsto et al, 2006]:

- Le contrôle d'accès physique.
- Le contrôle d'accès aux ressources virtuelles ou numériques.

Des exemples de la première catégorie comprennent le contrôle des frontières et de l'identification dans les aéroports, tandis que les cas typiques de ce dernier comprennent l'accès aux postes de travail, réseaux et l'authentification des transactions financières.

Figure 1.5 : Exemples de domaines d'application de la biométrie.

La Biométrie trouve ses applications dans plusieurs domaines comme le contrôle d'accès aux installations et aux ordinateurs, l'identification des criminels, la sécurité des frontières, l'accès à la centrale nucléaire, l'authentification de l'identité dans un environnement réseau, la sécurité de l'aéroport et la délivrance des passeports ou des permis de conduire, des bases de données médico-légales et médicales (Cf. Figure 1.5). Comme la biométrie trouve ses applications dans plusieurs zones de haute sécurité, assurer la sécurité du gabarit biométrique est de la plus haute importance. [Meenakshi & Padmabathi, 2010].

1.4. Comparaison des méthodes biométriques

Il existe plusieurs traits biométriques utilisés dans la reconnaissance d'individus (Cf. Figure 1.6). L'iris est considéré comme l'un des traits biométriques les plus fiables [Bowyer et al, 2008], [Radman et al, 2012], Le système d'identification par l'iris est très coûteux mais très efficace. C'est pourquoi on ne l'utilise que dans des bâtiments nécessitant une haute sécurité comme des prisons ou des agences bancaires. La reconnaissance par empreintes est la méthode de la reconnaissance biométrique la plus ancienne [Nanni & Lumini, 2009]. Elle est caractérisée par son acceptabilité par les utilisateurs comme c'est le cas avec d'autres méthodes biométriques utilisant la signature, la voix et la géométrie de la main.

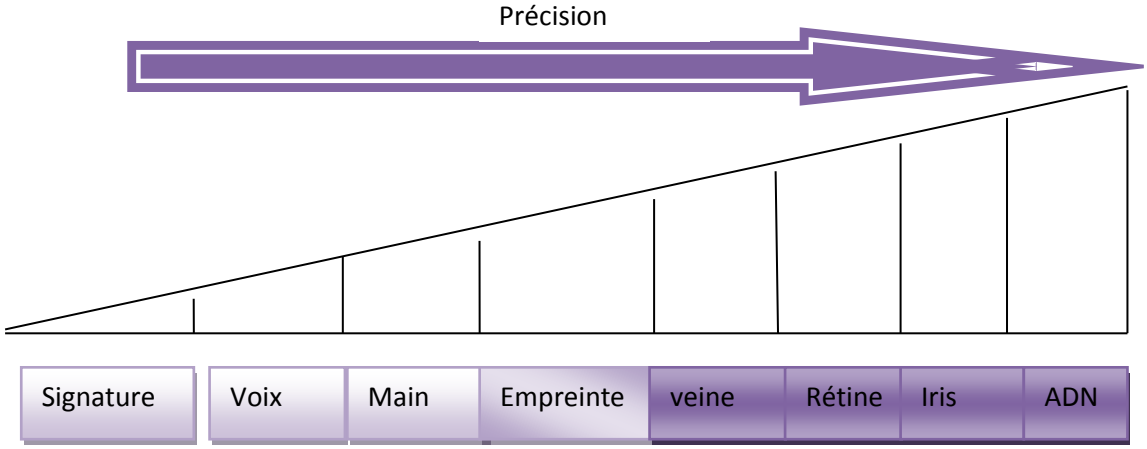


Figure 1.6 : Comparaison des méthodes biométrique selon le critère de précision.

Il est important de noter que l'utilisation d'une technique biométrique spécifique dépend fortement des conditions du domaine d'application et pas nécessairement de son taux de fiabilité et de précision. 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.

Chaque modalité présente des avantages et des inconvénients. Toutefois, le choix d'une modalité particulière dépend d'un certain nombre de paramètres comme le type de l'application visée, le coût envisagé pour le système, les performances attendues du système, l'acceptation de la modalité par l'utilisateur, la simplicité d'utilisation, etc.

Quelques points de comparaison

Le tableau 1.1 présente quelques points de comparaison de quelques méthodes biométriques (l'empreinte, l'iris, la main, la voix et le visage).

Tableau 1.1. : Quelques points de comparaison de quelques méthodes biométriques les plus utilisées.

	Points forts	Points faibles
Empreintes digitales	Faible coût, encombrement minimal	Exige un environnement propre.
Iris	Excellente fiabilité, faible taux de rejet.	Matériel plus coûteux
Forme de la main	Simplicité d'utilisation.	Encombrement de l'appareil
Voix	Facilité de mise en œuvre.	Nécessité de lire une phrase au hasard.
Visage	Simplicité, efficace sur un flux de personnes.	Nécessité d'une mise en œuvre rigoureuse.

1.5. La multimodalité biométrique

Les systèmes biométriques unimodaux souffrent de plusieurs problèmes qui sont à l'origine de l'utilisation d'un seul trait biométrique susceptible au bruit, à la mauvaise capture, à la pauvreté en matière de points biométriques confidents ou encore à la détérioration de la qualité de l'entrée biométrique, l'introduction de systèmes biométriques multimodaux est une solution à ces problèmes.

La biométrie donne lieu à plusieurs applications de fusion de données avec les différents indicateurs de biométrie et les systèmes multi indicateurs [Salicetti et al., 2003], [Toh et al., 2003], [Feng et al., 2004], [Kumar et al., 2003], [Ong et al., 2003], identification de visages [Achermann & Bunke, 1996], [Brunelli & Falavigna, 1995], vérification de signatures [Zois & Anatassopoulos, 1999], [Sabourin & Genest, 1994], [Bajaj & Chaudhury, 1997], reconnaissance de la parôle [Chibelushi et al., 1993], [Yu et al., 2000], [Chen et al., 1997].

1.5.1. Motivation de la fusion multimodale

Selon les références [Meenakshi & Padmabathi, 2010], [Liau & Isa, 2011], [Yang & Zhang, 2012], les systèmes biométriques unimodaux souffrent de plusieurs anomalies, nous présentons dans ce qui suit un résumé des différents problèmes affectant ses systèmes :

1. ***Bruit introduit par le capteur*** :

Du bruit peut être présent dans les données biométriques acquises, ceci étant principalement dû à un capteur défaillant ou mal entretenu. Par exemple, l'accumulation de poussière sur un capteur d'empreintes digitales, un mauvais focus de caméra entraînant du flou dans des images de visage ou d'iris, etc. Le taux de reconnaissance d'un système biométrique est très sensible à la qualité de l'échantillon biométrique et des données bruitées peuvent sérieusement compromettre la précision du système [Chen et al., 2005].

2. Non-universalité

Le principe d'universalité constitue une des conditions nécessaires de base pour un module de reconnaissance biométrique. Cependant, toutes les modalités biométriques ne sont pas vraiment universelles.

Le *National Institute of Standards and Technologies* (NIST) [NIST] a rapporté qu'il n'était pas possible d'obtenir une bonne qualité d'empreinte digitale pour environ 2% de la population (personnes avec des handicaps liés à la main, individus effectuant de nombreux travaux manuels répétés, etc.) [NIST, 2002]. Ainsi, de telles personnes ne peuvent pas être enrôlées dans un système de vérification par empreinte digitale.

De la même manière, des personnes ayant de très longs cils et celles souffrant d'anormalités des yeux ou de maladies oculaires (comme certains glaucomes et cataractes) ne peuvent fournir des images d'iris, ou de rétine, de bonne qualité pour une reconnaissance automatique. La non-universalité entraîne des erreurs d'enrôlement ("*Failure to Enroll*" ou FTE) et/ou des erreurs de capture ("*Failure to Capture*" ou FTC) dans un système biométrique.

3. Manque d'individualité

Les caractéristiques extraites à partir de données biométriques d'individus différents peuvent être relativement similaires. Par exemple, une certaine partie de la population peut avoir une apparence faciale pratiquement identique due à des facteurs génétiques (père et fils, vrais jumeaux, etc.). Ce manque d'unicité augmente le taux de fausse acceptation ("*False Accept Rate*" ou FAR) d'un système biométrique.

4. Manque de représentation invariante

Les données biométriques acquises à partir d'un utilisateur lors de la phase de reconnaissance ne sont pas identiques aux données qui ont été utilisées pour générer le modèle de ce même utilisateur lors de la phase d'enrôlement. Ceci est connu sous le nom de "*variations intra-classe*". Ces variations peuvent être dues à :

- Une mauvaise interaction de l'utilisateur avec le capteur (par exemple, changements de pose et d'expression faciale lorsque l'utilisateur se tient devant une caméra).
- L'utilisation de capteurs différents lors de l'enrôlement et de la vérification.
- Des changements de conditions de l'environnement ambiant (par exemple, changements en éclairement pour un système de reconnaissance faciale).
- Des changements inhérents à la modalité biométrique (par exemple, apparition de rides dues à la vieillesse, présence de cheveux dans l'image de visage, présence de cicatrices dans une empreinte digitale, etc.).

Idéalement, les caractéristiques extraites à partir des données biométriques doivent être relativement invariantes à ces changements. Cependant, dans la plupart des systèmes biométriques, ces caractéristiques ne sont pas invariantes et, par conséquent, des algorithmes complexes sont requis pour prendre en compte ces variations. De grandes variations intra-classe augmentent généralement le taux de faux rejet ("*False Reject Rate*" ou FRR) d'un système biométrique.

5. Sensibilité aux attaques

Les modalités biométriques sont uniques par personne mais elles peuvent être sujettes à différentes attaques. La fabrication de fausses empreintes ou l'imitation de la voix ou de la signature sont des exemples d'attaques aux systèmes biométriques. Les modalités biométriques comportementales telles que la signature et la voix sont plus sensibles à ce genre d'attaque que les modalités biométriques physiologiques.

1.5.2. Les scénarios de fusion

Dans ce paragraphe nous présentons les différents scénarios de fusion utilisés par les systèmes biométriques dites multimodaux, il est à noter que la multimodalité n'implique pas l'utilisation de plusieurs modalités biométriques au sens stricte du terme (comme le fait de combiner l'iris et l'empreinte), mais son sens est plus large comme définit dans ce qui suit par les différents scénarios de fusion.

- Capteurs multiples (multiple sensors).
- Algorithmes multiples (multiple algorithms).
- Instances multiples (multiple instances).
- Instances répétées (repeated instances).
- Modalités multiples (multiple modalities).

Dans les références [Jain & Ross, 2004] [Ross & Jain,2004] [Ross et al, 2006] on parle de « *multimodals biometrics* » qui entraine l'utilisation de plusieurs traits biométriques, et « *multibiometrics* » expliqué par les quatre premiers scénarios de fusion cités plus haut.

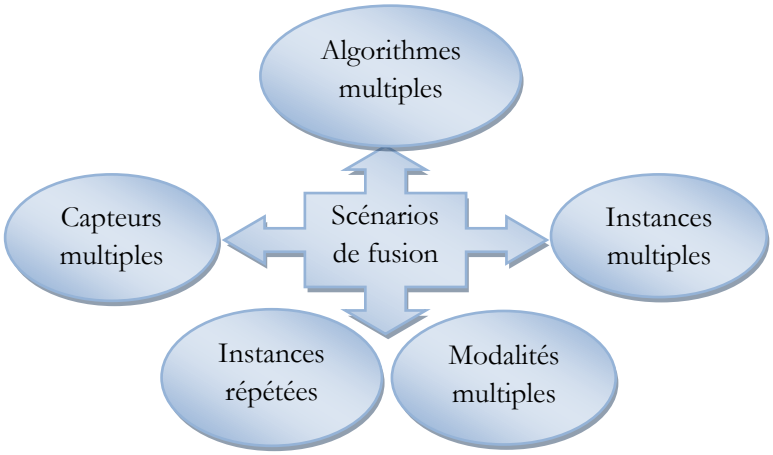


Figure 1.7 : Les différents scénarios de la fusion biométrique multimodale.

1.5.3. Les différents niveaux de fusion

Différents niveaux de fusion multimodale ont été introduit dans la littérature (Cf. Figure 1.8), communément retenu, est une division en cinq niveaux qui sont :

1.5.3.1. Niveau Capteur (*Sensor Level*)

Des données biométriques du même trait provenant de différents appareils et capteurs sont utilisées afin d'accroitre le nombre de points biométriques servant à identifier

l'individu. La fusion au niveau capteur 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. De plus, les captures doivent être compatibles entre elles et la correspondance entre les points dans les données brutes doit être connue par avance.

Par exemple, les images de visage obtenues à partir de plusieurs caméras peuvent être combinées pour former un modèle 3D du visage. Un autre exemple de fusion au niveau capteur consiste à mettre en mosaïque plusieurs images d'empreintes digitales afin de former une image d'empreinte digitale finale plus complexe [Ross & Jain, 2002] [Moon et al., 2004].

1.5.3.2. Niveau Caractéristique (*Feature Level*) :

La fusion au niveau caractéristique consiste à combiner différents vecteurs de caractéristiques ("*feature vectors*") qui sont obtenus à partir d'une des sources suivantes :

1. Plusieurs capteurs du même trait biométrique.
2. Plusieurs instances du même trait biométrique.
3. Plusieurs unités du même trait biométrique.
4. Plusieurs traits biométriques.

Les techniques basées sur la fusion au niveau d'extraction de caractéristiques sont meilleures par apport aux autres techniques à cause de la préservation des caractéristiques biométriques discriminantes des différents traits fusionnés. [Yang & Zhang, 2012]. Cependant, l'opération de la fusion multimodale à ce niveau est difficile.

1.5.3.3. Niveau Décision (*Decision Level*)

La fusion d'information au niveau *décision* peut être mis en place lorsque chaque matcher biométrique décide individuellement de la meilleure correspondance possible selon l'entrée qui lui est présentée.

La fusion au niveau de *décision* est utilisée selon différents algorithmes, les plus connus sont l'algorithme de « *Majority voting* » [Lam & Suen, 1997] et les règles logiques « *ET* » et « *OU* » [Daugman, 1998]. Cette fusion est souvent utilisée pour sa simplicité.

1.5.3.4. Niveau Rang (*Rank Level*)

Quand la sortie de chaque "matcher" biométrique est un sous-ensemble de correspondances possibles triées dans un ordre décroissant de confiance, la fusion peut se faire au niveau rang.

La décision est réalisée à l'aide de différents rangs de systèmes d'identification biométrique.[Giot & Rosenberger, 2012], la méthode la plus connue est la « *majority voting* »[Zuev & Inavov, 1999]. Dans cette méthode, on assigne à chaque correspondance possible le meilleur (minimum) rang calculé par différents matchers. En cas d'égalité, on en retient un seul au hasard afin d'arriver à un ordre de rang strict et la décision finale est prise selon les rangs combinés. D'autres méthodes de fusion au niveau rang existent :

- **La méthode *Borda count***

Les rangs combinés sont calculés en utilisant la somme des rangs assignés par les *matchers* individuels.

- ***La* méthode *de régression logistique***

C'est une généralisation de la méthode de *Borda count* ou une somme des rangs individuels est calculée et les poids sont déterminés par *régression logistique*.

1.5.3.5. Niveau Score (*Score Level*)

Ce niveau de fusion est le plus utilisé par les systèmes biométriques. Plus de détails sont donnés dans le paragraphe qui suit.

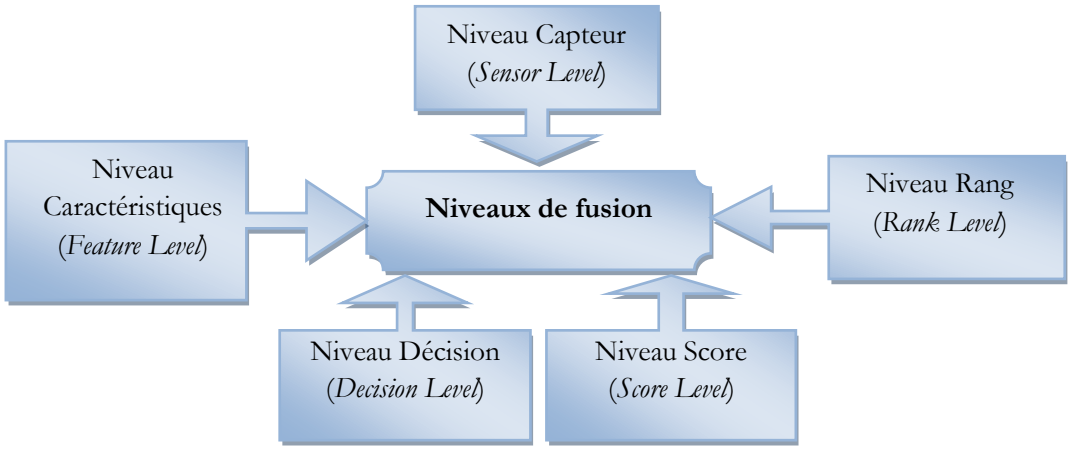


Figure 1.8 : Les cinq niveaux de la fusion biométrique multimodale.

1.5.4. La fusion au niveau score

La fusion au niveau score est l'approche la plus utilisée dans les systèmes biométriques multimodaux [Giot,2012][Park & Park, 2007][[Kumar & Passi, 2010][Sasidhar et al, 2010] ce choix est motivé par les points suivants :

- Les scores de données contiennent l'information la lus riche à propos du modèle d'entrée.
- la fusion au niveau score donne le meilleur compromis entre la richesse d'information et la facilité d'implémentation.
- il est facile d'accéder et de combiner les scores générés par les différents classificateurs (matchers).

De ce fait, nous avons choisi d'utiliser les scores générés par les classificateurs (matchers) de l'iris et de l'empreinte au sein du système de fusion multimodale proposé.

1.5.4.1. Normalisation de score

Il existe deux approches pour combiner les scores obtenus par différents classificateurs (matchers). La première approche permet de voir cela comme un problème de *classification*, tandis que 'autre approche permet de traiter le sujet comme un problème de *combinaison*. Dans les références [jain & Ross, 2004] et [Ross et al., 2006], les auteurs ont montré que les approches par combinaison sont plus performantes que la plupart des méthodes de classification (Cf. Figure 1.9).

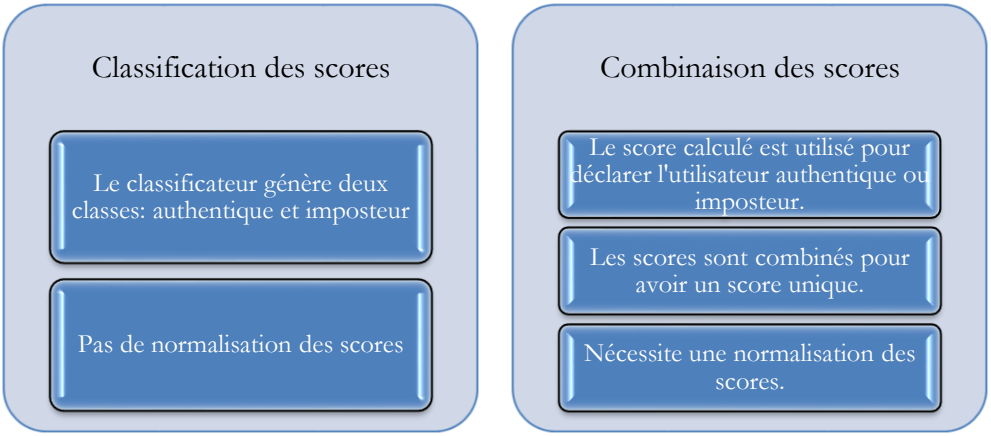


Figure 1.9: Comparaison entre l'approche de *classification des scores* et l'approche de *combinaison des scores*.

1.5.4.2. Les différentes techniques de normalisation de scores

A partir des références [Sasidhar et al, 2010][Ross et Jain,2004][Kittler et al, 1998] [Ross et al, 2006] [Kumar & Passi, 2010] [Tax et al, 2000] nous avons pu résumer les techniques de normalisation de scores des systèmes de fusion multimodales.

Tableau 1.2 : Résumé des techniques de normalisation de scores.

Technique	Utilisation	Fonction mathématique
MinMax	scores min max connus. Les scores imposteurs seront proches de 0 et les scores clients seront proches de 1.	s'=(s-min)/(max-min)
Z-Score	Moyenne et déviation standard connues, les scores client seront plutôt positifs et les scores imposteurs seront plutôt négatifs.	s'=(s-Moyenne)/(déviation standard)
Médiane et MAD	Médiane connu.	s'=(s-median)/constant(median l- median i)
Double Sigmoïde	Les fonctions logistiques	$S(t) = \frac{1}{1+e^{-t}}$
Tanh	Met chaque score normalisé s' dans l'intervalle [0.1]	s'=0.5[Tanh(0.1(s-Moyenne)/ déviation standard))+1]

S' est le score de fusion.

I.5.4.3. Les différentes techniques de fusion de scores

La règle minimum et la règle produit sont considérées comme des règles reliées aux statistiques des scores (*statistical based rules*), leur utilisation déponds de quelques conditions reliées aux scores des classificateurs [Toh et al , 2004].

- **La règle minimum : « *the min rule* »**

Cette règle donne de meilleurs résultats lorsque les scores d'appariement présentent des erreurs de type très haut « *outlier type error* » [Tax et al, 2000].

$$S' = Min\ (S^1..S^n) \qquad (1.1)$$

- **La règle produit : « *the product rule* »**

Cette règle est recommandée lorsque les classificateurs sont indépendants « *independant matchers* » [Tax et al, 2000]

$$S' = \prod_{k=1}^{n} S \qquad (1.2)$$

- **La règle somme : "*the sum rule*"**

Cette règle est recommandée lorsque les classificateurs sont corrélés « *correlated matchers* » [Tax et al, 2000].

$$S' = \sum_{k=1}^{n} S \qquad (1.3)$$

- **La somme linéaire pondérée "*Wheigted sum rule*"**

La pondération par des poids de scores provenant de traits biométriques différents indique l'importance de chaque score par rapport à la précision du trait biométrique et par conséquent la décision sera meilleure.

Par exemple si on fusionne deux scores $\mathbf{S_1}$ et $\mathbf{S_2}$ pondérés respectivement par les valeurs $\boldsymbol{\alpha}$ et $\mathbf{1 - \alpha}$ alors le score de fusion **S'** sera calculé comme suit

$$S' = \alpha S_1 + (1 - \alpha) S_2 \qquad (1.4)$$

1.5.5. La fusion au niveau décision

L'intégration d'information au niveau abstrait ou au niveau décision peut être mis en place lorsque chaque matcher biométrique décide individuellement de la meilleure correspondance possible selon l'entrée qui lui est présentée.

On site quelques méthodes de fusion de décisions :

- Méthode de "*majority voting*" ,
- Méthode de "*behavior knowledge space*" ,
- Method de "*weighted voting*" basé sur la théorie Dempster-Shafer ,
- les règles *ET* et *OU*.

Ces méthodes peuvent être utilisées afin d'arriver à la décision finale.

1.6. Critères d'évaluation des systèmes biométriques

Tout d'abord on présente les types d'erreurs d'un système biométrique, ensuite on présentera les courbes de performance et les différents points de fonctionnement.

1.6.1. Les erreurs

- **Erreurs liées au module d'acquisition**

Impossibilité d'acquisition du trait biométrique par le capteur de la donnée biométrique (*Failure to enroll*). Ces erreurs ne sont pas traitées par le système. Elles sont recensées et les données sont supprimées en général.

- **Erreurs liées au module d'extraction**

Impossibilité de comparaison (*failure to match*), ce type d'erreur est dû au module d'extraction de caractéristique et de comparaison.

- **Erreurs de classification**

Il existe deux types d'erreurs de classification liés aux mauvaises décisions des deux classes client et imposteur. Ces erreurs sont le résultat de la non-correspondance exacte entre deux échantillons biométriques d'une personne et permettent donc d'évaluer le niveau de fiabilité de la décision du système. Ces erreurs sont :

Fausses acceptations FA : si le système déclare l'individu comme étant le client alors que c'est un imposteur.

Faux rejets FR: si le système rejette l'individu alors que c'est le client.

Les fausses acceptations sont mesurées par le taux de fausse acceptation **TFA** (en Anglais False Rejection Rate **FRR**). Ce taux est égal au nombre de fausses acceptations FA divisé par le nombre de tests imposteur dans la base Ni.

$$TFA = \frac{FA}{Ni} \qquad (1.5)$$

Le taux de faux rejet **TFR** (en Anglais False Rejection Rate **FRR**) est égal au nombre de faux rejets FR divisé par le nombre de tests clients dans la base Nc.

$$TFR = \frac{FR}{Nc} \qquad (1.6)$$

Le taux d'erreur égal **TEE** (en Anglais **EER)**

Les taux d'erreurs de décision des systèmes de reconnaissance biométrique dépondent du seuil de décision fixé dans le module de décision (Cf. Figure 1.10).

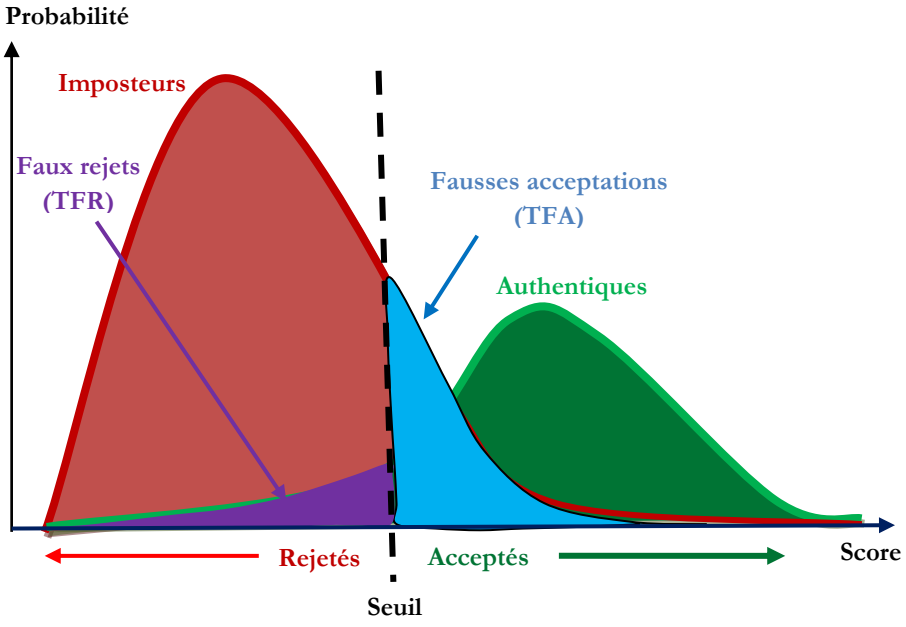


Figure 1.10 : Illustration des Taux d'erreurs TFA et TFR.

1.6.2. Les courbes de performances

1.6.2.1. Courbes ROC

Les courbes ROC ont été créées dans les années 1950 et utilisées afin d'optimiser des signaux radio bruités. On les utilise maintenant dans bien d'autres domaines, et notamment dans la biométrie ou elles se sont révélées très performantes [Metz, 1978], [Hanley & McNeil, 1982], [Langdon & Buxton, 2001].

L'aire sous la courbe ROC est une autre valeur susceptible de permettre d'´evaluer les performances d'une méthode de classification. Les courbes ROC (*Receiver Operating Characteristic* ou courbe de caractéristiques d'efficacité) permettent d'´étudier les variations de la spécificité et de la sensibilité d'un test pour différentes valeurs du seuil de discrimination.

La construction d'une courbe ROC se fait de la manière suivante :
- on porte sur l'axe des abscisses la variable "1- spécificité " (taux de faux positifs).
- sur l'axe des ordonnées, on retrouve la sensibilité (taux de vrais positifs).

La courbe se construit de façon empirique en calculant la sensibilité puis la spécificité d'un test pour différents niveaux de seuils de discrimination (Cf. Figure 1.11).

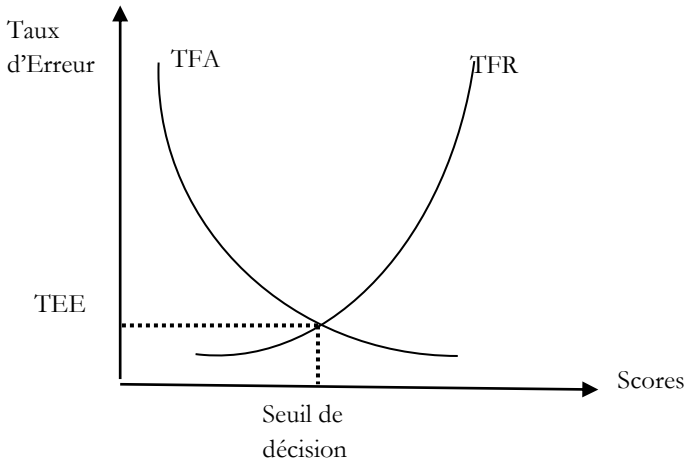


Figure 1.11 : Exemple de courbe ROC.

1.6.2.2. Courbe DET

Une deuxième courbe permettant d'illustrer la relation entre le FRR et le FAR est le DET (*Detection Error Trade-off*) [Martin et al., 1997]. Dans cette courbe, le FAR est tracé en fonction du FRR. Afin de focaliser la représentation sur les valeurs proches de l'EER, les valeurs du FAR et FRR sont normalisées de façon à rendre la courbe plus linéaire à l'intervalle autour de l'EER. L'EER est obtenu par l'intersection de la courbe avec la droite passant par les points dont les coordonnées sont (0,0) et (100,100).

Le DET facilite la comparaison de plusieurs systèmes dessinés sur un même graphique. Plus la courbe est proche de l'origine, plus le système est performant. La figure 1.12 montre un exemple de courbe DET.

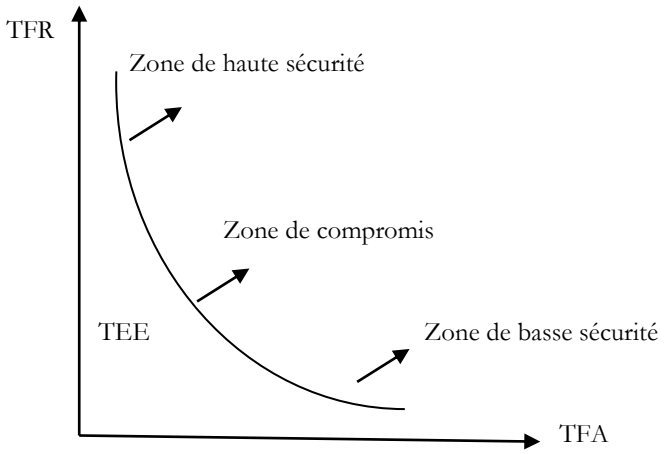


Figure 1.12 : Exemple de courbe DET.

1.6.3. Les points de fonctionnement

Les points de fonctionnement les plus utilisés sont :

TEE Taux d'Erreur Egal ou **EER** Equal Error Rate en Anglais. Ce point de fonctionnement correspond au seuil qui donne des taux de fausses acceptation et des taux de faux rejets égaux.

TEP Taux d'Erreur Pondéré ou **WER** Weighted Error Rate en Anglais. Ce point de fonctionnement correspond au seuil tel que le **TFR** est proportionnel au **TFA** avec un coefficient qui dépond de l'application. Le seuil du TEP est égal au seuil de l'TEE lorsque ce coefficient est égal à 1.

TFA fixé Ce point de fonctionnement correspond au seuil tel que le **TFA** est égal à un taux fixé par l'application (par exemple 1% ou 0.1%). La performance du système est donnée par le taux de **TFR** pour cette valeur de **TFA** fixée.

TFR fixé Ce point de fonctionnement correspond au seuil tel que le **TFR** est égal à un taux fixé par l'application (par exemple 1% ou 0.1%). La performance du système est donnée par le taux de **TFA** pour cette valeur de **TFR** fixée.

Zéro-TFR Ce point de fonctionnement correspond au seuil tel que le **TFR** est égal à 0. La performance du système est donnée par le taux de **TFA** pour cette valeur de **TFR** fixée.

Zéro-TFA Ce point de fonctionnement correspond au seuil tel que le **TFA** est égal à 0. La performance du système est donnée par le taux de **TFR** pour cette valeur de **TFA** fixée.

Le point de fonctionnement qui définit le choix du seuil de décision dépond de l'application visée. En général, le TEE est le plus utilisé car c'est un point de fonctionnement assez neutre qui ne favorise aucun des deux types d'erreurs (TFA et TFR). En revanche, lorsqu'une application est définie avec des objectifs de performance, on peut utiliser les autres points de fonctionnement, et le plus souvent, les points de fonctionnement correspondant à des niveaux fixés pour l'un des deux types d'erreurs.

I.7. Conclusion

Nous considérons ce chapitre comme le plus important dans notre thèse. Introductif, il présente un recadrage de la littérature sur les différentes facettes de la multimodalité biométrique, à savoir :

- Les différentes définitions de la multimodalité.
- Les niveaux de fusion.
- Les scénarios de fusion.
- La normalisation de scores comme une nécessité avant la combinaison des scores.
- La classification des scores comme une autre alternative de décision multimodale.

Nous avons tenu à présenter l'utile de la multimodalité en résumant l'information à partir de sources multiples sous formes de tableaux et figures pour bien expliciter ces notions.

Nous avons choisi le niveau fusion de score et le niveau décision avec plusieurs méthodes de combinaison de score qui nous servirons dans les chapitres suivants, afin de renforcer la comparaison des résultats des différents tests effectués.

Chapitre 2

LA RECONNAISSANCE PAR L'EMPREINTE DIGITALE

2.1. Introduction

Technologie mature, peu encombrante et abordable, la lecture de l'empreinte digitale a conquis de nombreux terrains et se présente comme la modalité biométrique dominante en contrôle d'accès.

Les empreintes digitales se forment dès le développement du fœtus et restent uniques et identiques durant toute la vie. Pendant près de 150 ans, les analyses des empreintes digitales ont été une partie importante des investigations criminelles et de l'identification des individus. Mais jusque récemment, la capture des empreintes digitales était plus un art qu'une science, et leur comparaison était un travail réservé à des spécialistes très qualifiés. De nos jours, les empreintes digitales peuvent être capturées, enregistrées et comparées par de petits capteurs de plus en plus performants : il est donc possible de les intégrer à toutes sortes d'appareils et d'applications comme les contrôles d'accès physiques et informatiques, les passeports et cartes d'identité, les terminaux de retrait d'argent ou de paiement ou encore diverses applications policières... Et tout ceci en temps réel.

Nous tenons à présenter dans ce chapitre un survol sur la reconnaissance d'individus basée sur l'extraction des caractéristiques biométriques liées à l'empreinte. Nous commençons par donner un historique de l'utilisation de cette technique si ancienne, ensuite nous définissons l'empreinte digitale en citant ses caractéristiques qui la rendent unique par individu, nous détaillons l'approche par extraction de minuties que nous choisissons pour implémenter le module monomodal de reconnaissance d'empreinte de notre application, et enfin, nous présentons les différentes méthodes d'appariements d'empreintes digitales.

2.2. Historique

Les premières traces d'utilisation d'empreintes digitales ont été découvertes en Egypte et datent de l'époque des pyramides il y a plus de 4000 ans. Les Chinois ont aussi utilisé très tôt ce moyen pour signer les documents officiels (le plus vieux document signé date du troisième siècle avant Jésus Christ) mais ils ne savaient sûrement pas que les empreintes étaient uniques pour chaque personne et permettaient ainsi une identification fiable. C'est en 1856 que l'anglais William Herschel, après avoir utilisé les empreintes en guise de signature sur la population indienne qu'il dirigeait, commença à comprendre que les empreintes étaient uniques et constantes dans le temps. En 1888 le britannique Francis Galton publia une étude sur les empreintes digitales où il établit leurs caractéristiques (unicité, invariance, minuties, classification) et en 1901 la technique d'identification au moyen des empreintes fut adoptée officiellement en Angleterre dans le système judiciaire. Cette technique fut ensuite largement développée dans les enquêtes criminelles et permit de résoudre un bon nombre d'affaires. De nos jours les empreintes sont toujours largement utilisées et reconnues comme méthode d'identification fiable [Wikipédia, 2013].

2.3. Caractéristiques d'une empreinte digitale

Une empreinte digitale est constituée d'un ensemble de lignes localement parallèles formant un motif unique pour chaque individu (Figure 2.1), on distingue les stries (ou crêtes, ce sont les lignes en contact avec une surface au toucher) et les sillons (ce sont les creux entre deux stries). Les stries contiennent en leur centre un ensemble de pores régulièrement espacés.

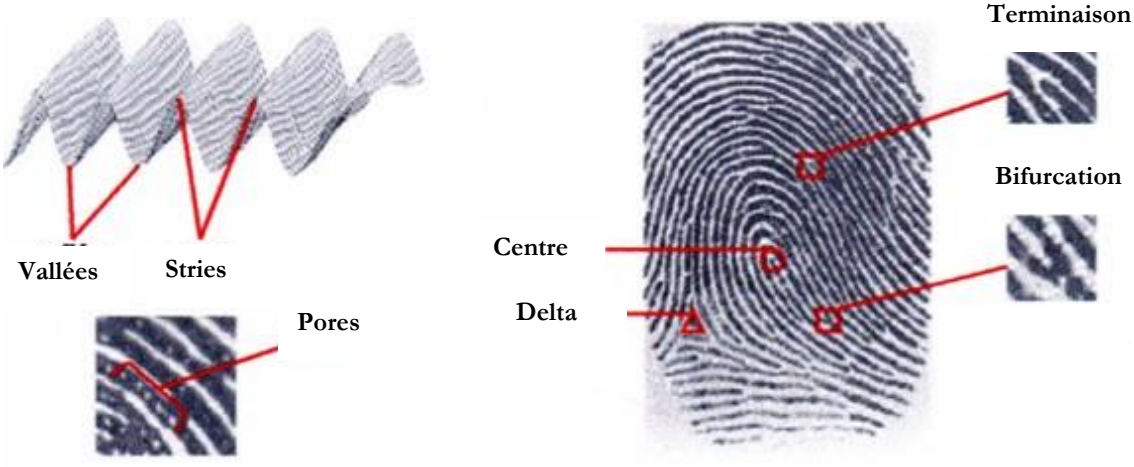


Figure 2.1 : Les caractéristiques de l'empreinte digitale.

Chaque empreinte possède un ensemble de points singuliers globaux (les centres et les deltas) et locaux (les minuties). Les centres correspondent à des lieux de convergences des stries tandis que les deltas correspondent à des lieux de divergence. Une étude a montré l'existence de seize types de minuties différentes mais en général les algorithmes ne s'intéressent qu'aux bifurcations et terminaisons qui permettent d'obtenir les autres types par combinaison (Cf. Figure 2.2).

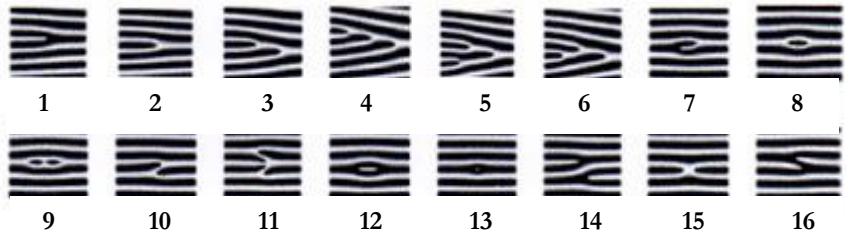


Figure 2.2 : Les différents types de minuties.

1. terminaison	9. boucle double
2. bifurcation simple	10. pont simple
3. bifurcation double	11. pont jumea
4. bifurcation triple I	12. intervalle
5. bifurcation triple II	13. point isolé
6. bifurcation triple III	14. traversée
7. crochet	15croisement
8. boucle simple	16. tête bêche

La position et le nombre de centres et de deltas permettent de classifier les empreintes en catégories, selon leur motif général on distingue principalement trois grandes familles (voir Figure 2.3):

Les boucles (*loop*) représentent 65% des empreintes rencontrées. Les spires (*whorl*) représentent 30% des empreintes rencontrées. Les arches (*arch*) représentent 5% des empreintes rencontrées.

Figure 2.3 : Les trois principales classes d'empreintes digitales.

L'ensemble formé par la disposition des points singuliers constitue un motif unique pour chaque individu.

En effet il a été montré que l'empreinte digitale se forme au cours du troisième mois de la vie fatale [Babler, 1991], le motif général est influencé par les gènes héréditaires mais l'apparition des détails (minuties) est créée de manière accidentelle par des pressions variables aléatoires sur les surfaces tactiles. Ainsi l'empreinte est unique pour tout individu, y compris pour des vrais jumeaux, et il a été montré que les méthodes de reconnaissance actuelles permettent d'identifier efficacement les jumeaux [Jain et al., 2001].

De plus, les empreintes une fois formées ne changent plus au cours de la vie d'une personne, ces deux caractéristiques en font un moyen de reconnaissance très efficace.

Selon la référence [Vasta et al., 2009], les caractéristiques d'empreintes sont divisées en trois niveaux :

- **Caractéristiques d'empreinte de niveau 1** : (*level 1 fingerprint features*) représentent le flux de crête et des informations morphologiques générales. Ces caractéristiques ne sont pas unique pour établir l'identité mais sont utilisés pour une large classification des empreintes digitales dans différentes catégories telles que : boucle gauche, boucle droite, spirale, arc, arc et tentes.
- **Caractéristiques d'empreinte de niveau 2** : (*level 2 fingerprint features*) représentent les informations de minuties telles que les terminaisons de crêtes et les bifurcations.
- **Caractéristiques d'empreinte de niveau 3** : (*level 3 fingerprint features*) Ces caractéristiques représentent les détails complexes d'une empreinte digitale comme les attributs de dimension et la structure des pores et des crêtes qui sont les plus discriminant entre les trois niveaux de fonctionnalités. Ce niveau de caractéristique n'est pas utilisé par les systèmes automatiques de reconnaissance d'empreinte car il est applicable seulement sur les images de haute résolution.

2.4. Traitement de l'empreinte digitale

Il existe trois approches différentes d'algorithmes du traitement des empreintes digitales pour reconnaissance biométriques [Lumini and Nanni, 2008] :

- l'approche basée sur l'extraction des minuties.
- L'approche basée sur la corrélation.
- L'approche basée sur la texture de l'image d'empreinte.

L'approche par détection de minuties est la plus utilisée par les travaux de recherche, cela est dû principalement aux résultats de reconnaissance obtenus qui sont meilleurs que ceux des approches basées sur l'image de l'empreinte. Ces dernières sont utilisées surtout lorsque l'image de l'empreinte est assez mauvaise pour ne pas détecter un nombre confident de minuties dans l'image. Dans ce qui suit nous détaillons l'approche basée sur l'extraction de minutie que nous choisissons pour concevoir et implémenter le module monomodale de reconnaissance d'empreinte du système multimodale proposé. La motivation de ce choix est la simplicité d'implémentation de l'algorithme d'extraction de minuties. Cf. Figure 2.4.

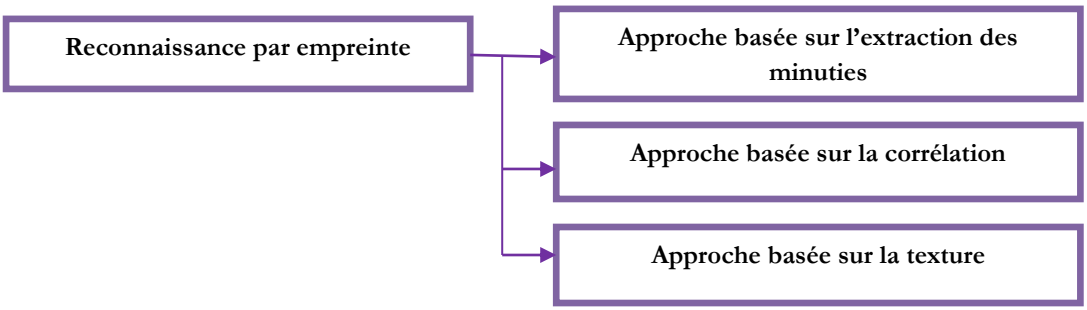


Figure 2.4 : Les approches de la reconnaissance par empreinte digitales.

2.5. L'approche basée sur l'extraction de minuties

Selon la référence [Bansal et al., 2011], plusieurs algorithmes d'extraction de minuties ont été proposés dans la littérature (Cf. Figure 2.5). Il y a ceux qui agissent sur les images binaires, et ceux qui s'appliquent directement sur les images à niveau de gris. Des travaux ont été proposés en appliquant la squelettisation sur l'image d'empreinte binaire ensuite les minuties sont extraites en se basant sur les valeurs de la connectivité (*Crossing Number* CN) ; d'autres travaux utilise la morphologie de l'image pour extraire les minuties à partie de l'image binarisée et squelettisée [Humbe et al., 2007][Bansal et al. ; 2010].

Une autre direction de recherche est basée sur l'extraction des minuties en utilisant le code chaine (*chaincode*) à partir de l'image binarisé [Shi & Govindaraju, 2006]. Ou bien en utilisant la représentation *Run* (*Run representation*) appliquée sur l'image binarisé [Zenzo et al., 1996]. D'autres travaux ont proposés le traitement des empreintes à partir des images à niveaux de gris présentant plus d'informations. Les textes encadrés dans la figure 2.5 seront détaillés dans les paragraphes suivants.

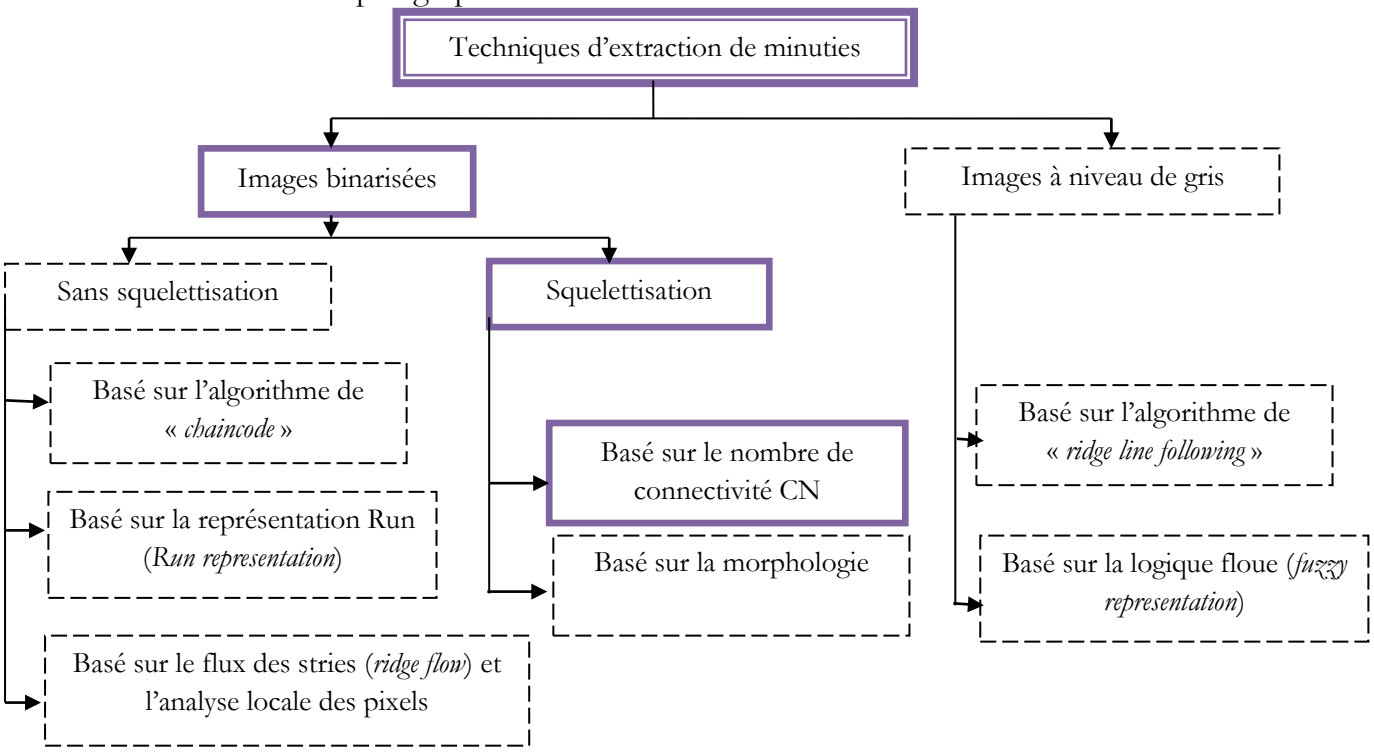


Figure 2.5 : Les techniques d'extraction de minuties.

La reconnaissance par empreinte digitale basée sur l'extraction des minuties selon le nombre de connectivité repose sur les étapes suivantes :

- Le prétraitement.
- La binarisation.
- La squelettisation
- L'extraction de minuties
- Le post traitement
- L'appariement

Nous décrivons dans ce qui suit chaque étape.

2.5.1. Le prétraitement

La qualité de la structure des stries est une caractéristique importante, car ce sont elles qui portent l'information nécessaire pour l'extraction des minuties. L'uniformité de l'image de l'empreinte facilite la tâche de détection des stries et par conséquent le repérage des minuties avec une haute précision. Malheureusement, dans la pratique, le bruit persistant corrompt la qualité de l'image et rend l'extraction imparfaite. La corruption de l'image peut être causée parla variation de la force de pression de la peau, les coupures accidentelles, l'humidité, la poussière, . . . etc.

2.5.1.1. Filtrage

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.

2.5.1.2. L'égalisation d'histogramme

En traitement d'images, l'égalisation d'histogramme est une méthode d'ajustement du contraste d'une image numérique qui utilise l'histogramme. Elle consiste à appliquer une transformation sur chaque pixel de l'image, et donc d'obtenir une nouvelle image à partir d'une opération indépendante sur chacun des pixels. Cette transformation est construite à partir de l'histogramme cumulé de l'image de départ. [Wikipédia, 2013].

L'égalisation d'histogramme permet de mieux répartir les intensités sur l'ensemble de la plage de valeurs possibles, en « étalant » l'histogramme. L'égalisation est intéressante pour les images dont la totalité, ou seulement une partie, est de faible contraste (l'ensemble des pixels sont d'intensité proches). La méthode est rapide, facile d'implémentation, et complètement automatique (i.e. pas de réglages) [Wikipédia, 2013].

2.5.1.3. Segmentation:

Le but de cette étape est de délimiter les régions d'intérêt. En effet, quelques parties de l'image sont inutiles qu'on ne doit pas les prendre en compte, il s'agit des zones vides (la périphérie de l'empreinte) ou des régions de mauvaise qualité. Les régions inutiles disposent généralement d'une variance de niveau de gris très faible, par contre les régions utiles de l'empreinte ont une variance relativement élevée. Cela est expliqué par le fait que la partie utile est constituée d'un ensemble de stries et de vallées alternés. Une telle méthode de segmentation consiste d'abord au découpage de l'image en un ensemble de blocs. Puis les blocs dont la variance est inférieure à un seuil prédéfini seront marqués comme inutiles. [Dugelay et al, 2002]

La variance d'un bloc de taille w x w est calculée comme suit:

$$v(k) = \frac{1}{w2} \sum_{i=0}^{w} \sum_{j=0}^{w} (I(i,j) - M(k))2 \qquad (2.1)$$

Où *I (i, j)* dénote le niveau de gris du pixel *(i, j)* du bloc k, *M(k)* dénote la moyenne et *v(k)* représente la variance du bloc *k*.

2.5.2. Binarisation (Seuillage)

Pour permettre la squelettisation, l'image doit d'abord être binarisée, c'est-à- dire que l'image en 256 niveaux de gris dont nous disposons à ce stade est transformée en image binaire où les pixels noirs correspondent aux stries et les pixels blancs aux vallées. Il existe de nombreuses techniques de binarisation d'images. On cite trois techniques de seuillage [IBG, 2013]:

2.5.2.1. Seuillage global

Dans ce seuillage, un même seuil est appliqué sur tous les pixels de l'image, le choix de celui-ci dépend de la qualité de l'image. Les situations principales dans lesquelles le seuil global seul n'est pas suffisant sont causées par des changements dans la luminosité, la résolution et les erreurs d'acquisition, la mauvaise qualité de l'image source et la complexité dans la structure de l'image. [Jain et al., 1998].

On compare les niveaux de gris de l'image à un seuil choisi, de telle sorte qu'on attribue le blanc pour tous les pixels de niveau de gris supérieur ou égal à ce seuil, et le noir pour tous les pixels de niveau de gris inférieur à ce même seuil, selon la règle suivante :

Si $f(i, j) \geq S$ alors le pixel est en blanc.

Si $f(i, j) < S$ alors le pixel est en noir.

Avec :

$f(i, j)$: est le niveau de gris du pixel en cours.

S : est le seuil de binarisation.

2.5.2.2. Seuillage local

Dans ce cas, il n'est pas nécessaire de fixer une valeur unique de seuil pour toute l'image, mais de modifier la valeur de chaque pixel selon son voisinage, bien que cette méthode soit robuste, elle a l'inconvénient d'être lente, car la binarisation de chaque pixel nécessite l'analyse de son voisinage. [Jain et al., 1998].

2.5.2.3 Seuillage adaptatif

Il représente la combinaison des deux techniques précédentes. Il comprend deux types de seuillage : un seuil bas et un seuil haut. Les pixels dont le niveau de gris est inférieur au seuil bas sont rendus noirs, les pixels dont le niveau de gris est supérieur au seuil haut sont rendus blancs, les pixels compris entre le seuil bas et le seuil haut prennent la valeur 0 (noir) ou 1 (blanc) suivant la majorité de leurs voisins.

2.5.3 Squelettisation

La squelettisation de l'image de l'empreinte facilite la tâche de l'extraction de minuties. Elle consiste en une suite d'opérations morphologiques d'érosion dont le but est de réduire L'épaisseur des stries en un pixel tout en retenant la connexité des stries intacte. Cf. Figure 2.6.

Figure 2.6 : La squelettisation.

2.5.4. Extraction des minuties

Une fois l'image de l'empreinte est souillée et l'épaisseur des stries est réduite, l'opération de détection des minuties devient une tâche facile et systématique. La méthode la plus utilisée pour l'extraction est la méthode dite CN (*the crossing number*) [Dugeley et al., 2002]. Cette méthode requiert l'utilisation de l'image squelettique où les pixels de stries prennent la valeur 1 qui correspond à la couleur noire. La valeur du nombre CN est calculée pour chaque pixel noir. Elle est égale à la moitié de la somme des différences entres les pairs adjacents des 08 pixels voisins. Cf. figure 2.7 et figure 2.8.

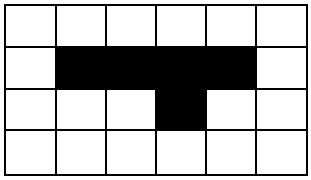
P1	P2	P3
P4	P	P5
P6	P7	P8

$$CN(p) = \frac{1}{2}\sum_{i=1}^{8} |p_i - p_{i-1}| \qquad (2.2)$$

Avec $p_0 = p_8$ et $p \in \{0,1\}$.

Figure 2.7: Le calcule de la valeur de la connectivité CN.

L'exemple suivant illustre le codage CN de l'image:



0	0	0	0	0	0
0	1	1	1	1	0
0	0	0	1	0	0
0	0	0	0	0	0

0	0	0	0	0	0
0	1	2	3	1	0
0	0	0	1	0	0
0	0	0	0	0	0

Partie de l'empreinte codage binaire codage CN

Figure 2.8 : Représentation de l'empreinte par (graphique, codage binaire, codage CN)

Selon la valeur CN, la nature du pixel est déduite selon les correspondances montrées dans le tableau suivant: Cf. Tableau 2.1.

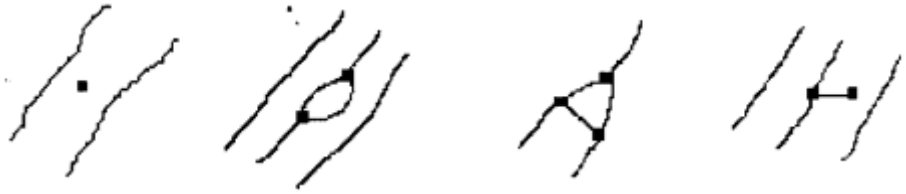
Tableau 2.1. Correspondance entre CN et les types de minuties

CN	propriété
0	Point isolé
1	Minutie de type terminaison
2	Un point de continuité, pas de minutie
3	Bifurcation triple
4	Bifurcation quadruple

Généralement les cas de CN=0 et CN= 4 sont ignorés car ils sont très rares en pratique.

2.5.5. Post-traitement

L'introduction des fausses minuties peut être due soit au bruit original de l'image de l'empreinte, soit aux artéfacts créés par les procédures du prétraitement appliquées. Par conséquent, le post-traitement est indispensable pour la validation des vraies minuties et pour l'élimination des fausses minuties.



Aiguillon (*Spur*) **Trou (*Hole*)** **Triangle (*triangle*)** **Pointe (*spike*)**

Figure 2.9 : Exemples de fausses minuties.

Les «*spurs*» sont des fausses terminaisons tandis que les «*holes* », les *triangles*, et les «*spikes* » sont des fausses bifurcations.

La majorité des approches du post-traitement proposées dans la littérature emploient une série de règles structurelles pour la détermination des fausses minuties. A titre d'exemple, Ratahan et al [Barett, 1997] ont établi un ensemble de règles heuristiques qui s'appliquant séquentiellement.

Par exemple, la règle «si la distance entre une terminaison et une bifurcation interconnectées est inférieure à un seuil minimal alors éliminer les deux minuties (le cas de spike : Cf. Figure 2.9 ». Au lieu d'effectuer un passage sur l'image pour chaque règle, Tico et Kuosmmen [Jain et al., 1999] ont établi une seule règle généralisée qui peut éliminer un grand nombre de fausses minuties en analysant le voisinage de chaque minutie en un seul passage. Cf. figure 2.10.

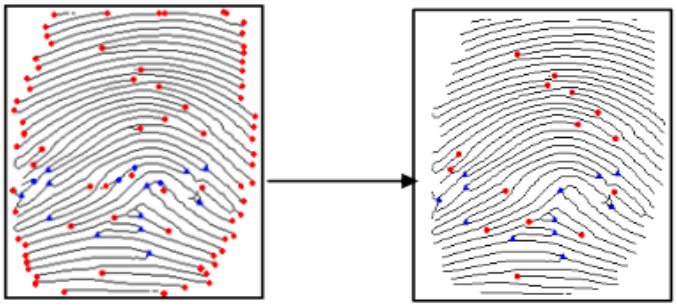


Figure 2.10 : Elimination des fausses minuties.

2.6. Appariement des empreintes digitales

2.6.1. Introduction

L'appariement (*matching*) des empreintes digitales désigne la procédure d'estimation de la similarité entre deux images d'empreintes, c'est-à-dire vérifie si elles se sont issues du même doigt. Le choix d'un tel algorithme de l'appariement dépend essentiellement de la technique utilisée pour la représentation des caractéristiques des empreintes. Un algorithme typique de .l'appariement estime d'abord les paramètres de translation, rotation, et de distorsion entre les deux images, puis il évalue leur taux de similarité en cherchant la correspondance optimale entre les signatures des deux images. Les conditions d'acquisition non idéales et les algorithmes appliqués pour le prétraitement et l'extraction des paramètres altèrent souvent la représentation effective de l'empreinte (par exemple, on peut avoir des minuties manquantes, des fausses minuties, des informations bruitées,..., etc.). Un bon algorithme d'appariement doit être robuste face à ce genre d'erreurs. Dans cette section nous allons présenter les principaux algorithmes d'appariement.

2.6.2. Méthodes d'appariement des empreintes digitales

2.6.2.1. Appariement à base de corrélation

La méthode typique de l'appariement à base de corrélation consiste à aligner les deux images d'empreintes et de soustraire l'image en entrée de l'image de référence, afin de voir les correspondances entre leurs textures respectives. Si le coefficient de corrélation est supérieur à un seuil prédéfini alors les deux empreintes sont jugées être du même doigt. Ce type d'approches est facile à implémenter, néanmoins il est très sensible aux erreurs d'estimation de l'alignement et de déformations non linéaires de l'image.

Les techniques basées sur la corrélation dans certains cas sont mieux placées que celles à base de minuties. A titre d'exemple, pour des images de mauvaise qualité, les algorithmes d'extraction de minuties détectent un nombre assez important de fausses minuties et plusieurs minuties effectives sont absentes, ce qui détériore la performance des algorithmes basés sur les minuties. Un inconvénient majeur de cette approche est sa consommation excessive en termes de temps et d'espace.

2.6.2.2. Appariement à base de minuties

Les techniques de l'appariement à base de minuties tentent d'établir la correspondance optimale entre la structure de minuties de l'empreinte en entrée et celle l'empreinte de référence. D'une façon générale, les deux structures de minuties sont premièrement alignées, puis la portion des minuties bien superposées (minuties qui se correspondent) est déterminée, deux minuties sont généralement considérées comme bien appariées si elles se sont localisées dans la même fenêtre de tolérance.

2.6.2.3. Appariement à base de la distance Euclidienne

Dans cette approche, les techniques d'extraction de paramètres collectent les informations globales et locales de l'image de l'empreinte dans une représentation compacte de taille fixe appelée "*Fingercode*", par analogie au concept de « *Iriscode »* introduit

par Daugman [Daugman, 1993]. Les algorithmes de cette approche d'appariement supposent que les représentations sont invariantes à la translation et aussi à la rotation. L'appariement se fait par le calcul de la distance euclidienne entre les deux vecteurs *Fingercode*.

2.7. Conclusion

Une empreinte digitale est une marque laissée par le relief cutané des doigts, venant de l'épiderme de la peau de celle-ci. Ce relief est constitué de crêtes et plis capillaires qui sont uniques et permanentes. Chaque individu a donc une empreinte digitale différente d'un autre, et même ses propres doigts n'ont pas exactement tous la même empreinte. Les chercheurs dans le domaine notent une chance sur 64 milliards, la probabilité que deux individus aient la même empreinte digitale.

De nos jours les empreintes sont toujours largement utilisées et reconnues comme méthode d'identification fiable, précise et bien acceptée par les utilisateurs.

Les caractéristiques d'empreintes sont divisées en plusieurs niveaux et sont utilisés pour une large classification des empreintes digitales dans différentes catégories, telles que : boucle gauche, boucle droite, spirale, arc, arc et tentes. Ces caractéristiques représentent également les informations de minuties telles que les terminaisons de crêtes et les bifurcations.

Il existe trois approches différentes d'algorithmes du traitement des empreintes digitales pour reconnaissance biométriques :

- L'approche basée sur l'extraction des minuties.
- L'approche basée sur la corrélation.
- L'approche basée sur la texture de l'image d'empreinte.

L'approche par détection de minuties est la plus utilisée par les travaux de recherche, cela est dû principalement aux résultats de reconnaissance obtenus qui sont meilleurs que ceux des approches basées sur l'image de l'empreinte. Ces dernières sont utilisées surtout lorsque l'image de l'empreinte est assez mauvaise pour ne pas détecter un nombre confident de minuties dans l'image.

Dans ce chapitre nous avons présenté l'essentiel de ce qu'il faut savoir sur la reconnaissance par empreinte digitale qui nous permettra par la suite de concevoir le module de vérification d'empreinte de nos approches proposées.

Chapitre 3

LA RECONNAISSANCE PAR L'IRIS

3.1. Introduction

L'iris de l'œil est une membrane physiologique visible de l'extérieur possédant des caractéristiques particulières du relief et une multitude de tubes très fins. Ces caractéristiques sont uniques, permanentes et très difficilement falsifiables.

L'idée d'introduire l'iris dans la reconnaissance des personnes a été introduite en 1936 par l'ophtalmologiste Frank Burch. Deux autres ophtalmologistes (Aran Safir et Leonard Flom) et un universitaire (John Daugman) ont élaborés le premier procédé pour l'identification basé sur l'iris, Breveté en 1994 par John Daugman. La méthode de Daugman, appelé *l'**Iriscode***, est à l'origine de la grande majorité des systèmes commercialisés à base de reconnaissance par l'iris [Wikepedia, 2013].

La reconnaissance par l'iris est une technologie jugée jusqu'alors sans faille. Il est prouvé que la probabilité de trouver deux iris identiques est inférieure à l'inverse du nombre d'humains ayant vécu sur terre. Ce niveau d'unicité élevé rend cette méthode biométrique très fiable.

Par ailleurs, la reconnaissance par l'iris est relativement intrusive, ceci est dû principalement aux conditions de la capture de l'image d'iris, notamment en raison de sa petite taille, de sa sensibilité ou encore de l'immobilité de l'utilisateur qu'elle impose

Ce chapitre est consacré à l'introduction de la reconnaissance d'individus par extraction de caractéristiques biométriques liées à l'iris. Tout d'abord nous commencerons par définir l'iris, ensuite le système biométrique de traitement d'iris et ses modes opératoires, par la suite nous présenterons un historique sur les travaux de recherche liés à la reconnaissance d'iris suivi par les principales méthodes de reconnaissance d'iris connues dans monde de la biométrie. Nous conclurons le chapitre par citer les bases de données d'iris les plus connues et utilisées par les travaux de recherche.

3.2. Définition de l'iris:

L'iris, qui veut dire arc-en-ciel en grec, est la zone colorée visible entre le blanc de l'œil et la pupille L'iris humain est caractérisé par les points suivant :

- L'iris commence à se former quelques mois avant la naissance jusqu'à quelques mois après.
- l'enchevêtrement des tubes qui le constituent l'iris est fixe et ne varie que très peu durant la vie de l'individu.
- L'iris contient une quantité d'information particulièrement importante, comparable à la quantité d'informations contenue dans l'ADN.
- Les filaments, creux et stries dans les cercles colorés qui entourent la pupille de chaque œil sont des motifs aléatoires de l'iris uniques à chaque individu.

3.3. Système de reconnaissance d'iris

Un système de vérification par reconnaissance d'iris peut se décomposer en deux unités principales :

- Une unité optique de capture de l'image de l'iris par dispositif de vision (acquisition de l'iris).
- Une unité de traitement des données (extraction et comparaison des informations discriminantes avec celles stockées préalablement lors de l'enrôlement

Il existe toujours au moins deux modules dans un système de reconnaissance par l'iris :

- Module d'apprentissage.
- Module de reconnaissance.

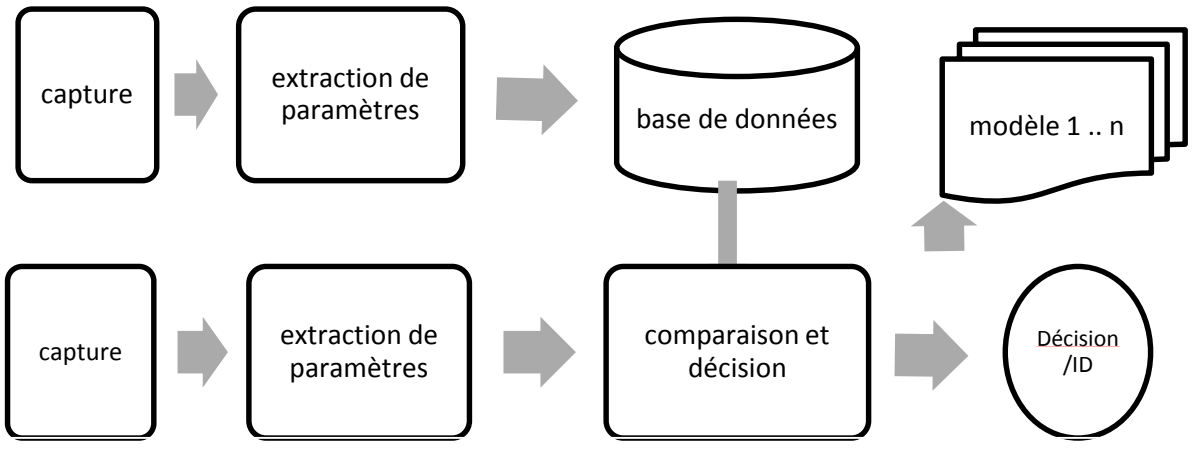


Figure 3.1 : Les modes opératoires d'un système biométrique.

La suite de la reconnaissance sera différente suivant le mode opératoire du système :

- Mode identification : problème de type 1 : N.
- Mode vérification : problème de type 1 : 1.

3.4. Historique de la reconnaissance d'iris

Plusieurs chercheurs et groupes de recherche se sont intéressé à ce domaine depuis son éclosion dans les débuts des années 1990. J. Daugman fut le pionnier et il est le véritable père, ses travaux sont les plus utilisés de nos jours.

L'ophtalmologiste Frank Burch a été le premier ç avoir proposé l'idée d'utiliser la texture de l'iris à des fins biométriques, c'était en 1936 [Bertillon, 1985]. Depuis, le domaine de la reconnaissance des personnes par l'iris a été l'objet de plusieurs recherches et travaux. Deux autres ophtalmologistes, Drs. Leonard Flom et Aran Safir ont soutenu le concept que deux iris de deux personnes différentes ne peuvent pas être identiques [Flom & Safir, 1987]. En 1987, ils avançaient l'idée de l'utilisation de l'iris comme moyen biométrique permettant ainsi l'identification des individus. Ils on breveté cette idée au courant de l'année 2007. En 1994, J. Daugman alors professeur à l'université de Harvard a breveté une méthode complète de reconnaissance par l'iris, basée sur un modèle mathématique. La méthode de Daugman, appelé *l'**Iriscode***, est à l'origine de la grande majorité des systèmes commercialisés à base de reconnaissance de l'iris.

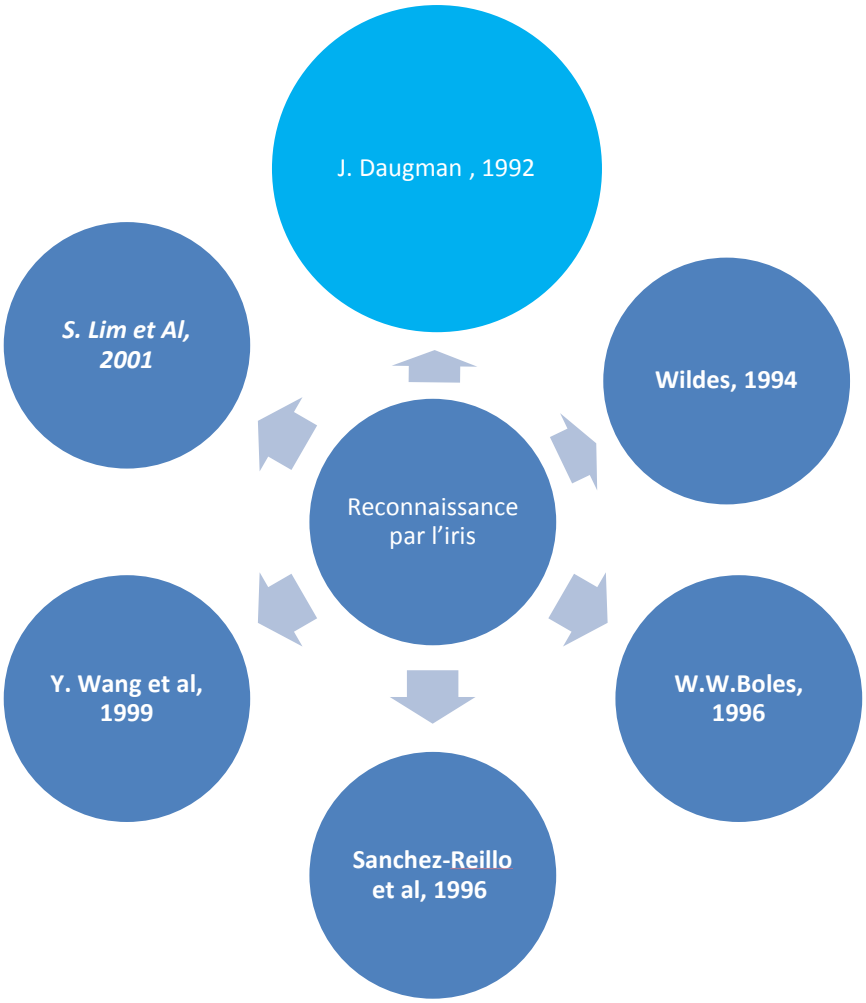


Figure 3.2 : Historique des travaux de recherche sur la reconnaissance par l'iris.

3.5. Travaux précédents

Plusieurs chercheurs et groupes de recherche se sont intéressés à ce domaine depuis son éclosion dans les débuts des années 1990. J. Daugman fut le pionnier et il est le véritable père, ses travaux sont les plus utilisés de nos jours. Voici, en détails la méthode Daugman et en bref les plus notables des autres travaux :

3.5.1. La méthode Daugman (Iris code), 1992

En 1992, J. Daugman fut le premier à publier ses recherches sur la mise au point d'un procédé d'analyse de texture de l'iris [Daugman, 1993][Daugman,1994][Daugman, 2002]. Il repose sur :

- **Normalisation de l'iris : Méthode pseudo polaire**

L'iris est un disque irrégulier. Daugman [Daugman,1993] a développé une méthode de normalisation pseudo-polaire du disque de l'iris appelée la méthode « Rubber Sheet » qui pourrait être décrit comme une tentative d'étendre le disque de l'iris comme du caoutchouc. Elle est dite pseudo-polaire car les deux cercles de l'iris et de la pupille ne sont pas concentriques (n'ont pas le même centre). La méthode est expliquée de la manière suivante :

- **Le model « rubber sheet » :**

On associe à chaque pixel de l'iris, dans le domaine cartésien, un correspondant dans le domaine pseudo-polaire selon la distance du pixel par rapport aux centres des cercles et l'angle qu'il fait avec ces centres. La transformation se fait, plus exactement, suivant l'équation suivante :

$$x(r,\theta) = (1-r)x_p(\theta) + rx_s(\theta) \qquad (3.1)$$

$$y(r,\theta) = (1-r)y_p(\theta) + ry_s(\theta) \qquad (3.2)$$

Où $x_p(\theta)$ 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 $y_p(\theta)$ représente l'ordonnée de ce même point, alors $x_s(\theta)$ et $y_s(\theta)$ représentent les coordonnées des points obtenus par le même principe mais sur le contour de l'iris.

- **Extraction des caractéristiques : Filtres de Gabor**

Pour l'extraction des caractéristiques Daugman a utilisé des filtres de Gabor 2D qu'il a adapté au traitement d'images. Les filtres de Gabor sont un moyen d'analyse espace-fréquence qui minimise l'incertitude de Heisenberg, c'est-a-dire 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 [Gabor,1946]. C'est ce qui fait la puissance des filtres de Gabor comme moyen d'analyse de texture et classification. Les filtres de Gabor analysent la texture de l'iris suivant différentes résolutions et différents angles, leur forme est donnée par l'équation suivante :

$$\int_{\rho}\int_{\phi} e^{-i\omega(\theta_0-\phi)} e^{-\frac{(r_0-\rho)^2}{\alpha^2}} e^{-\frac{(\theta_0-\phi)^2}{\beta^2}} I(\rho,\phi)\rho d\rho d\phi \qquad (3.3)$$

Où $I(\rho,\phi)$ 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 r_0 et θ_0 représentent les coordonnées des points d'analyse de l'ondelette de Gabor.

On remarque dans l'équation ci-dessus que les filtres de Gabor ont une forme complexe qu'on peut donc exploiter. D'ailleurs, Daugman a opté ce choix en ne considérant que la phase de Gabor. En effet, on code chaque phase de Gabor sur 2 bits en suivant le principe du codage quatre quadrants, comme montré dans la **Figure 3.3**. Chaque phase sera codée différemment, selon que la phase appartienne à l'un des quatre quadrants du cercle trigonométrique ; Afin de limiter les erreurs si la phase calculée est à la frontière entre deux quadrants adjacents, chaque passage entre un quadrant et un quadrant adjacent entraine un changement d'un seul bit. Cette opération se résume donc à coder les signes de la partie réelle et la partie imaginaire des coefficients de Gabor obtenus et d'assigner 0 au code si le coefficient est négatif et 1 si le coefficient de Gabor est positif.

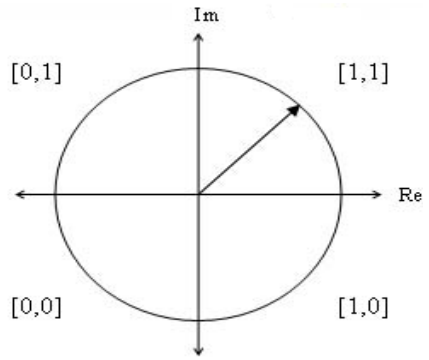


Figure 3.3 : Principe de codage de phase sur quatre quadrants et en 2 bits [Daugman, 1994].

On réitère cette opération plusieurs fois, autour de plusieurs points d'analyse, en suivant plusieurs résolutions et orientations des filtres de Gabor jusqu'à obtention d'un code de 256 octets.

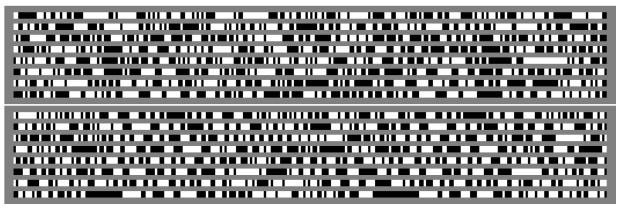


Figure 3.4 : Exemples d'*Iriscode* généré par la méthode de Daugman [Daugman, 1994].

En complément aux codes, on calcule aussi des masques de même taille fixe (2048 bits) qui déterminent pour chaque bit du code s'il faut le prendre en considération ou non. Les bits ignorés représentent les régions couvertes par les paupières, les cils, ou ayant un faible rapport qualité bruit, ou 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 ci-dessous :

$$HD_0 = \frac{\|(codeA \otimes codeB) \cap maskA \cap maskB\|}{\|maskA \cap maskB\|} \qquad (3.4)$$

Où codeA et codeB sont deux codes calculés à partir de deux images d'iris par le procédé précédemment décrit, maskA et maskB représentent leurs masques associés. Littéralement, la distance de *Hamming* calcule le nombre de bits différents et valides pour les deux iris entre le codeA et le codeB. 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.

Pour faire face aux problèmes de rotations dus aux inclinaisons de l'œil par rapport à la caméra, Daugman génère 7 codes d'iris. Chaque code correspond à un angle particulier de rotation de l'image de référence. La comparaison entre deux iris s'effectue donc en comparant un iris code avec les 7 autres iris codes qui correspondent aux différentes rotations. La distance de prise est la distance minimale entre les sept comparaisons [Daugman, 1994].

3.5.2. Travaux de Wildes, 1994

Wildes [Wildes et al., 1994]a été le premier et l'unique à proposer une méthode alternative et complètement différente de celle de Daugman. Les différences se situent dans toutes les phases de traitement incluant : la capture de l'iris, la segmentation, la normalisation et la reconnaissance.

Dans la phase de segmentation, les pourtours de l'iris sont extraits par transformée de *Hough*, appliquée à la détection de cercles sur les contours de l'image, et les paupières sont modélisées par des arcs paraboliques.

La normalisation s'effectue en alignant une image $I_a(x, y)$ avec la référence (i.e. : image stockée dans la base de données) $I_d(x, y)$ en utilisant une fonction de transformation des pixels $u(x, y), v(x, y)$ telle que les niveaux de gris dans $I_a(x - u(x, y), y - v(x, y))$ et $I_d(x, y)$ soient les plus proches possible.

D'une manière générale les fonctions u et v doivent minimiser l'intégrale suivante :

$$\int_x \int_y (I_d(x, y) - I_a(x - u, y - v))^2 dxdy \qquad (3.5)$$

Avec la contrainte de transformation suivante :

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} - sR(\phi) \begin{pmatrix} x \\ y \end{pmatrix} \qquad (3.6)$$

Où s et R représentent respectivement le facteur d'échelle et la matrice de rotation par un angle ϕ. En utilisant une méthode de minimisation itérative ; il est possible de déduire les valeurs de s et de ϕ [Masek, 2003].

La normalisation effectuée, les images sont filtrées par les Laplaciens de filtres gaussiens sur quatre résolutions. Il calcule ensuite une corrélation normalisée pour chaque résolution sur des fenêtres de taille 8x8. Pour chaque image filtrée, il considère la médiane des valeurs de corrélation. La fusion entre les quatre valeurs de corrélation d'effectue au moyen d'une analyse en composantes discriminantes.

Pour tester son système, Wildes a utilisé une base de données privée de 60 iris différents (droits et gauches) provenant de 40 personnes différentes ; Des vrais jumeaux faisaient partie des personnes enregistrées. Les résultats montrent que les deux distributions inter-classe et intra-classe sont bien séparées et donc qu'aucune fausse acceptation ni aucun faux rejet n'ont été observés.

3.5.3. Travaux de W.W.Boles, 1996

Boles [Boles & Boashash, 1998] fait usage d'une nouvelle technique basée sur une transformée en ondelettes monodimensionnelle.

Il localise d'abord le centre de la pupille par détection des contours circulaires, puis il procède de la même manière pour le diamètre extérieur de l'iris.

Ensuite, en fonction du ratio entre le diamètre de l'iris de référence et celui de l'iris à identifier, il construit un ensemble de n cercles virtuels centrés sur celui de la pupille, sur lesquels il extrait n signaux caractéristiques de relief de l'iris.

Il génère par la suite une représentation *zero-crossing* par une transformée en ondelettes (décomposition sur 8 niveaux, mais il conserve seulement les 4éme, 5éme et 6éme). « Il s'agit en fait d'un codage des points d'inflexion des n signatures de l'iris pour différents niveaux de résolution ; ce codage est obtenu en utilisant une ondelette mère spécifique du type dérivée seconde d'une fonction de lissage » [Tisse et al., 2005].

La comparaison est réalisée par quatre fonctions de dissimilitude représente le score final. Mais l'efficacité de cette technique n'a toujours pas été démontrée sur plus de 2 iris différents.

3.5.4. Travaux de Sanchez-Reillo et al, 1996

Ils ont repris dans l'ensemble les travaux de J. Daugman [Daugman,2002]. Ils transforment partiellement la texture de l'iris en un équivalent rectangulaire, puis ils en extraient le code en binarisant les résultats de filtrage avec la partie imaginaire de filtres complexes de *Gabor*. Ils utilisent la distance de *Hamming* pour comparer entre deux codes d'iris.

Cette équipe a atteint un EER (Equal Error Rate : taux d'erreur égale) de 3.6% pour une taille de code d'iris de 1860 bits. Les tests ont été effectués sur une base de données de plus de 200 images (au moins 10 images de 20 yeux).

3.5.5. Travaux de Y. Wang et al, 1999

Y. Wang et al. Ont travaillé sur une représentation rectangulaire de l'iris (proposée par J. Daugman) et ont breveté une nouvelle méthode d'extraction de caractéristiques [Zhu et al., 1999].

D'abord, un filtrage est effectué sur l'image rectangulaire d'iris soit par filtrage de Gabor suivant 4 directions et pour 6 fréquences différentes, soit par transformée en ondelettes 2D sur 5 niveaux de faible résolution uniquement. On récupère alors n images résultats (n=24 pour le 1er cas, et n=13 pour le 2ème). Puis on construit la signature d'un iris par une série de n vecteurs [moyenne écart type], extraits de ces n images. La distance euclidienne pondérée est utilisée pour effectuer la comparaison. Un taux de classification (identification en groupe fermé) de 93.8% est obtenu sur une base de 160 images [Zhu et al., 1999].

En 2002, ils apportèrent une amélioration à leur système : on filtre d'abord la texture de l'iris par un filtre passe-bande symétrique circulaire, puis un vecteur caractéristique comprenant 384 valeurs est construit, correspondant à l'écart absolu moyen (somme sur l'image des différences entre l'intensité des pixels et la moyenne de l'image) de 384 blocs de 8x8 pixels. La comparaison est faite au moyen du classificateur (*Nearest Feature Line*). Ils ont mené de nouvelles expérimentations sur 134 iris (de 7 à 25 images par œil), ils ont eu un taux de classification de 99.85% (ou FAR=0.1% et FRR=0.83 en mode vérification).

En 2004, ils proposèrent une autre technique utilisant les variations locales le long de la texture de l'iris; Les variations locales sont caractérisées par l'adaptation et la disparition d'une importante structure dans la texture de l'image (crête, sillonne, …). Ils transforment d' abord l'image en un signal 1D puis utilisent une transformée en ondelette pour générer une séquence de positions qui caractérise les points de variations aigus locales. Ces séquences de variation sont ensuite utilisées pour la comparaison.

3.5.6. Travaux de S. Lim et al, 2001

Toujours à partir d'une représentation rectangulaire de l'iris, S. Lim & al., [Lim et al.,2001] proposent en 2001 d'analyser les motifs de l'iris humaine par une transformée en ondelettes (ondelette mère de *Haar*). La texture de l'iris est décomposée sur 4 niveaux, et le vecteur de 87 caractéristiques d'un iris est construit en combinant la sous-image HH4 (4éme niveau) avec l'intensité moyenne des 3 autres sous-images HH1, HH2 et HH3.

L'étape d'identification est réalisée par un classificateur basé sur un réseau par quantification vectorielle d'apprentissage (LVQ : *Learning Vector Quantization*). Sur une base de données de 2500 images (100 iris, 25 échantillons par iris, dont 5 pour l'apprentissage du classificateur), la courbe ROC relevée indique un FRR de 1.65% pour un FAR de 2.90%.

3.5.7. Travaux récents

Dans ce paragraphe on site d'autres approches de reconnaissances d'iris :

S. Noh & Al. [Noh et al.,2002] appliquent un algorithme d'apprentissage non-supervisé utilisant des statistiques d'ordre supérieur pour l'extraction de caractéristiques, A. Muron & Al. [Muron et al., 2001] évoquent la possibilité d'identifier un iris par son spectre de puissance optique de Fourier, ou encore M. Dobes et al. [Dobes et al., 2003] proposent l'utilisation de l'information mutuelle moyenne pour aligner les motifs de deux iris et mesurer leur similarité.

D'autres études ont proposé des algorithmes améliorés [Kodituwakku et al., 2010][Kang et al., 2010]. Des travaux plus récents ont proposé l'utilisation de réseaux de neurones [Broussard & Ives, 2011], des réseaux de neurones flous avec des algorithmes d'apprentissage à l'aide des ensembles flous et les « *pattern classes* » [Chowhan et al., 2011].. Il ya peu de travaux à qui utilisent l'appariement flou « *fuzzy matching* » dans un système de reconnaissance biométrique, dans [Abhyankar & Schuckers, 2010] l'auteur a introduit un cadre pour évaluer la qualité de l'image de l'iris sur la base occlusion, le contraste, la concentration et la déformation angulaire. Dans leur travail, ils améliorent l'image avant de la segmenter afin d'obtenir de meilleurs résultats.

Selon la référence [Bowyer et al, 2008], les chercheurs dans le domaine de la reconnaissance d'iris se sont répertoriés dans quatre directions différentes :

- La reconnaissance par instances multiples d'iris.
- La reconnaissance par appariement d'une partie de la région d'iris.
- La reconnaissance par indexation
- La reconnaissance par analyse statistique des distributions d'appariement.

Dans la seconde approche de reconnaissance, les chercheurs pensent que la région proche de la pupille est la plus importante, ils préfèrent omettre la région proche des cils et de la bordure de l'œil susceptible à la distorsion.

3.5.7. Système de référence : Le système Masek

Dans la technologie d'iris, le premier système de référence est le système développé par Libor Masek de l'université de Western Australia [Masek, 2003].

Libor Masek a développé un système « *Open-Source* » de reconnaissance des personnes par l'iris [Masek, 2003]. Le système comprend un module de segmentation basé sur la transformée de *Hough* qui permet de localiser la pupille, l'iris, les paupières et les cils. Le système inclut aussi un module de normalisation basé sur la méthode de normalisation pseudo-polaire. Dans le module de la reconnaissance, il effectue un filtrage *1D de Log-Gabor* sur 4 niveaux pour coder la phase de *Gabor* selon le procédé de codage 4 quadrants. Dans son dernier module la distance de *Hamming* est employée pour la prise de décision.

Libor Masek a développé son système, à l'origine, en MATLAB. Xiaomei Lu, K Bowyer et Patrick Flynn sont venus réécrire en C ce système open-source avant que le NIST, l'entité qui organise les évaluations les plus réputées en biométrie ne traduise le système de Lu en C++ avec des modifications de vitesse et d'optimisation [NIST].

3.6. Bases de données publiques

Aujourd'hui, à la grande satisfaction des chercheurs sur la vérification des personnes par l'iris, plusieurs bases de données sont apparues, à savoir CASIA [CASIA], UPOL [UPOL], UBATH [UBATH], UBIRIS [URIBIS] et ICE [NIST].

CASIA *Chinese Academy of Science Institute of Automation*, a été le premier institut à partager la base de données d'images d'iris qu'il a collecté. La première version de cette base CASIAv1 a été réclamée par plus de 1400 groupes de recherches de 70 pays des 5 continents. CASIAv1 inclut 756 images de 108 personnes. Pour chaque personne, 7

images ont été acquises en deux sessions séparées de quelques semaines. La résolution des images CASIA-Iris V1 est de 320x280. Cette base était la plus utilisée au début des années 2000, elle a servi grandement à faire évoluer la recherche, néanmoins plusieurs points faibles l'ont rendu aujourd'hui caduque. En effet, la base est considérée comme étant très »clean » du fait que les images soient toutes nettes, et que les iris soient faiblement couverts de paupières et de cils. Les images ont aussi été prétraitées, ainsi les images ont été centrées et la pupille colorée en noir. Devant ce fait, une deuxième base de données appelée CASIA-Iris V2 est mise à la communauté scientifique par la même équipe, elle inclut quant elle 2400 images de 120 classes d'œil différentes. Cette base contient des images floues, avec des illuminations différentes et le port de lunettes est permis. La résolution des images de cette base est de 640x480 pixels, elles sont acquises avec deux capteurs différent le capteur OKI et le capteur Pattek. Cependant, on reproche à cette base le fait que tous ses sujets soient chinois.

La base UBATH contient des images de haute qualité acquise par un système de capture mis au point par l'université de Bath. Elle dispose de 2000 images d'iris de 50 personnes, téléchargeables gratuitement. Les sujets sont des européens et des asiatiques. La résolution des images est de 1280x960, elle dépasse nettement les résolutions des autres bases disponibles.

La base de données d'images d'iris UPOL inclut 384 images de 64 sujets européens. Les images ont été acquises par le capteur TOPCON TRC50IA relié à la caméra SONY DXC-950P 3CCD. Les images sont en couleur, de format PNG avec une résolution de 768x576 pixels, elles sont de très bonne qualité sans aucune occlusion des cils ou des paupières.

Les images de la base de données UBIRIS sont diversement dégradées en faisant varier les conditions d'acquisition (illumination, contraste, réflexion, focus et occlusion), elle a été conçue pour tester la robustesse des algorithmes de reconnaissance d'iris aux différents types de dégradation de qualité d'images d'iris. Elle contient 1877 images de résolution 400x300 de 241 personnes, elles sont capturées en deux sessions. Le mode d'acquisition est la lumière visible, et les images sont disponibles en couleur sous deux résolutions possibles : 800x600 et 200x150. On reproche à cette base le fait que ses images soient acquises en lumière visible, et qu'elle ne peut être utilisée pour évaluer des systèmes développés sur des images en infrarouge.

La base ICE 2005 a été mise à disposition des chercheurs par le National Institute of Standards and Technology (NIST)[NIST], La base contient 2953 images de 132 personnes capturées par la caméra dédiée LG2200. Cette base de données est une sous partie d'une base plus large de plus de 25094 images. Ses images souffrent de différents types de dégradation tels que les occlusions causées par les paupières et les cils. Le niveau de flou et le niveau de flou de bougé dépasse considérablement ceux présents dans les autres bases précédemment citées.

3.7. Conclusion

L'iris est un organe interne à l'œil possédant des caractéristiques particulières du relief (sillons de contraction, anneaux, etc), ces caractéristiques sont uniques, permanentes et très difficilement falsifiables.

La quantité d'information contenue dans l'iris est comparable à celle de l'ADN, donc l'iris est beaucoup plus riche en information biométrique que l'empreinte digitale.

L'utilisation de la biométrie par l'iris est une technique récente qui date de 1936, cette technique reste extrêmement fiable même à travers des lunettes ou des lentilles. Le seul problème de cette technique est lié à la qualité de l'image d'iris, résultat de la mauvaise capture.

En comparaison à l'identification par l'empreinte digitale, le capteur d'image de l'œil est plus volumineux et donc inadéquat pour la sécurité des objets de petite taille. Il est également plus coûteux.

Dans ce chapitre un état de l'art sur la reconnaissance d'iris a été présenté. Un résumé de travaux récents dans la reconnaissance biométrique par l'iris est présenté. Le point est mis sur le système ouvert 'open source' de Libor Masek qui sera utilisé dans le module monomodal de la reconnaissance d'iris de notre système multimodal d'iris et d'empreinte digitale.

Deuxième partie

Paradigmes de raisonnement intelligent

"La connaissance s'acquiert par l'expérience, tout le reste n'est que de l'information."

(Albert Einstein)

Chapitre 4

L'INTELLIGENCE ARTIFICIELLE

4.1. Introduction

L'un des principaux attraits de l'informatique consiste en la possibilité qu'elle offre pour traiter les connaissances dont on dispose en un système automatique de résolution ou d'assistance à la résolution.

C'est ainsi que l'informatique numérique offre des outils puissants pour résoudre des équations mathématiques modélisant un système physique, permettant ainsi de rendre effectif le modèle dont on dispose.

Mais, certaines connaissances dont on dispose sont formulées en langue naturelle : il faut être capable de traiter des connaissances exprimées linguistiquement et disposer pour cela de systèmes pouvant raisonner sur des symboles et pas seulement sur des nombres.

Le projet de l'intelligence artificielle (IA) peut être compris comme la recherche des principes permettant de concevoir et réaliser de tels systèmes.

4.2. Définition de l'intelligence artificielle

- Définition 1 [Wikipédia, 2013]

Le terme « intelligence artificielle », créé par John McCarthy, est souvent abrégé par le sigle « IA » (ou « AI » en anglais, pour Artificial Intelligence). Il est défini par l'un de ses créateurs, Marvin Lee Minsky, comme « la construction de programmes informatiques qui s'adonnent à des tâches qui sont, pour l'instant, accomplies de façon plus satisfaisante par des êtres humains car elles demandent des processus mentaux de haut niveau tels que : l'apprentissage perceptuel, l'organisation de la mémoire et le raisonnement critique ». On y trouve donc le côté « artificiel » atteint par l'usage des ordinateurs ou de processus électroniques élaborés et le côté « intelligence » associé à son but d'imiter le comportement. Cette imitation peut se faire dans le raisonnement, dans la compréhension des langues naturelles, dans la perception : visuelle (interprétation des images et des scènes), auditive (compréhension du langage parlé) ou par d'autres capteurs, dans la commande d'un robot. Même si elles respectent globalement la définition de Minsky, il existe un certain nombre de définitions différentes de l'IA qui varient sur deux points fondamentaux [Russell & Norvig, 2003] :

- Les définitions qui lient la définition de l'IA à un aspect humain de l'intelligence, et celles qui la lient à un modèle idéal d'intelligence, non forcément humaine, nommée rationalité.
- Les définitions qui insistent sur le fait que l'IA a pour but d'avoir toutes les apparences de l'intelligence (humaine ou rationnelle), et celles qui insistent sur le fait que le fonctionnement interne du système d'IA doit ressembler également à celui de l'être humain ou être rationnel.
- **Définition 2 [Nicolle, 1996]**

L'intelligence artificielle peut être vue comme une science de l'ingénieur, une spécialisation de l'informatique dont l'objet est la résolution des problèmes complexes, et en tant que science de l'ingénieur elle apporte des outils logiciels (Lisp, Prolog, Smalltalk, systèmes experts, réseaux connexionnistes...) aux sciences cognitives [Nicolle, 1996].

- **Définition 3 [Russell & Norvig, 2010]**

L'IA est un des champs les plus récents parmi les sciences de l'ingénierie. Les travaux ont sérieusement débuté juste après la Seconde Guerre Mondiale et le terme a été forgé en 1956. A l'heure actuelle l'IA est composée d'une grande diversité de sous disciplines allant des plus générales (apprentissage, perception) aux plus spécifiques (jouer aux échecs, démontrer des théorèmes mathématiques, écrire des poèmes)

- **Définition 4 [Balacheff, 1994]**

L'IA, comme a pour objectif pratique la conception et la réalisation de dispositifs informatiques dont le comportement apparaîtrait intelligent aux yeux d'un observateur humain : l'observation du système conduirait à penser légitimement que son comportement est guidé par un raisonnement. Cet objectif, formulé en termes pragmatiques, est indissociable de l'objectif théorique de modélisation opératoire des connaissances : une modélisation qui permet l'action, la communication et le contrôle.

4.3. Historique

Le projet de l'IA ne se réduit pas en effet à la conception et réalisation de systèmes à base de connaissances : l'IA se présente souvent comme une science de l'intelligence et des systèmes intelligents en général. Son projet est, comme le souligne Haugeland [Haugeland, 1989], de produire de l'intelligence « synthétique », authentique, et pas seulement de l'intelligence approchée.
Plusieurs chercheurs se sont intéressés à la portée, la pertinence et le succès de l'IA, voir par exemple Haugeland [Haugeland, 1989], Partridge et Wilks [Partridge & Wilks, 1990], Newell [Newell, 1990], Dreyfus [Dreyfus, 1984] et Winograd et Flores [Winograd et Flores, 1989].

- **L'IA dans la protohistoire**

Les premiers jalons historiques de l'intelligence artificielle datent de la Protohistoire, où mythes, légendes et rumeurs dotent des êtres artificiels, réalisés par des maîtres-artisans, Les hommes mécaniques et les êtres artificiels sont présents dans la mythologie grecque, ainsi les robots dorés d'Héphaïstos et Pygmalion et Galatée [Russell & Norvig, 2003], tandis qu'au Moyen Âge, circulent des rumeurs de secrets mystiques ou de techniques *alchimiques* pour imprégner des esprits, tels que le *Takwin* de *Geber*, les *homoncules* de *Paracelse* et le *Golem* de *MaHaRaL* [Hawkins & Blakeslee, 2004]. Au XIX[e] siècle, l'idée d'hommes artificiels et de machines pensantes prend corps dans des œuvres de fiction, telles que *Frankenstein* de *Mary Shelley* ou encore *R. U. R. (Rossum's Universal Robots)* de *Karel Čapek* [McCorduck, 2004], et des essais de spéculation, comme *Darwin among the Machines* de Samuel Butler [Butler, 1863]. L'I.A. est un élément important de la science-fiction [Wikipédia, 2013].

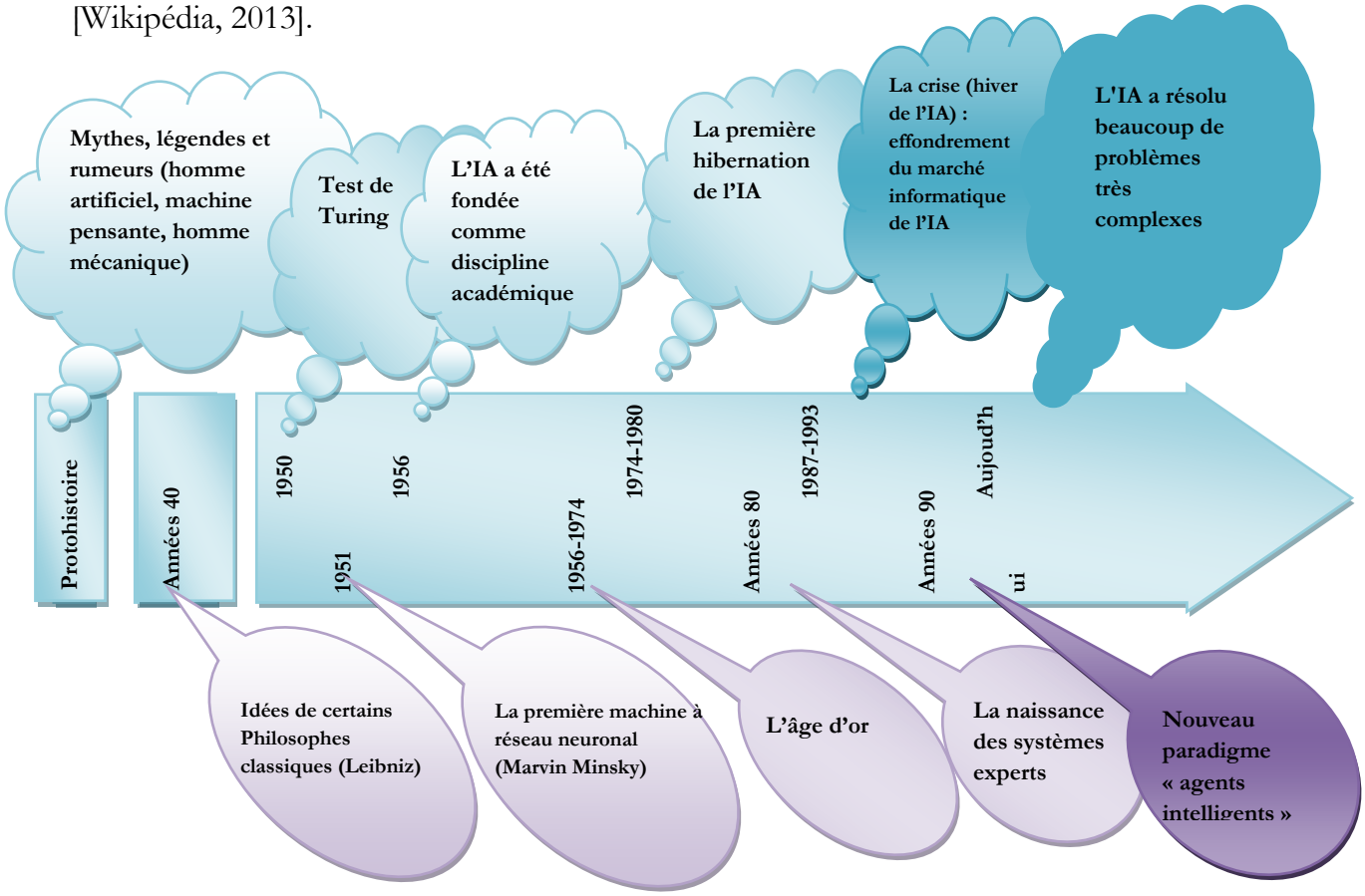


Figure 4.1 : Histoire de l'Intelligence Artificielle.

- **Fondement académique de l'IA**

Dans les années 1940 et 1950, une poignée de scientifiques d'une large gamme de domaines (mathématiques, psychologie, ingénierie, économie et science politique) ont commencé à discuter de la possibilité de créer un cerveau artificiel. Ce domaine de recherche de l'intelligence artificielle a été fondé en tant que discipline académique en 1956.

- **L'âge d'or de l'IA**

Dans l'âge d'or de l'IA (1956-1974), les programmes développés à l'époque sont considérés par la plupart des gens comme simplement « extraordinaires» [Russell & Norvig, 2003]: des ordinateurs résolvent des problèmes algébriques de mots, démontrent des théorèmes en géométrie et apprennent à parler anglais. À cette époque, peu croient que de tels comportements « intelligents » soient possibles pour des machines [Crevier, 1993]. Les chercheurs font preuve alors d'un optimisme intense dans le privé comme dans leurs articles, ils prédisent qu'une machine complètement intelligente sera construite dans les 20 ans à venir [McCorduck, 2004].

- **La première hibernation de l'intelligence artificielle (1974−1980)**

Dans les années 1970, l'intelligence subit critiques et revers budgétaires, car les chercheurs en intelligence artificielle n'appréhendent pas les difficultés des problèmes auxquels ils sont confrontés. Leur immense optimisme a engendré une attente excessive et quand les résultats promis ne se matérialisent pas, les investissements consacrés à l'intelligence artificielle s'étiolent [Crevier, 1993].

- **La naissance des systèmes experts**

Dans les années 1980, des programmes d'IA appelés « systèmes experts » sont adoptés par les entreprises et la connaissance devient le sujet central de la recherche en IA. Au même moment, le gouvernement japonais finance massivement l'IA à travers son initiative « ordinateurs de cinquième génération ». Un autre évènement est la renaissance du connexionnisme à travers les travaux de John Hopfield et David Rumelhart.

- **La crise : le second hiver de l'IA 1987−1993**

L'expression « hiver de l'IA » a circulé parmi les chercheurs qui, ayant déjà vécu les coupes de budget de 1974, réalisent avec inquiétude que l'excitation autour des systèmes experts est hors de contrôle et qu'il y aurait sûrement de la déception derrière [Crevier, 1993]. Leurs craintes sont effectivement fondées : entre la fin des années 1980 et le début des années 1990, l'intelligence artificielle a subi une série de coupes budgétaires.

- **L'IA depuis 1993**

Le champ de l'intelligence artificielle, avec plus d'un demi-siècle derrière lui, a finalement réussi à atteindre certains de ses plus anciens objectifs. On a commencé à s'en servir avec succès dans le secteur technologique, même sans avoir vraiment été mise en avant. Quelques réussites sont venues avec la montée en puissance des ordinateurs et d'autres ont été obtenues en se concentrant sur des problèmes isolés spécifiques et en les approfondissant avec les plus hauts standards d'intégrité scientifique. Néanmoins, la

réputation de l'IA, dans le monde des affaires au-moins, est loin d'être parfaite. En interne, on n'arrive pas à vraiment expliquer les raisons de l'échec de l'intelligence artificielle à répondre au rêve d'un niveau d'intelligence équivalent à l'homme qui a captivé l'imagination du monde dans les années 1960. Tous ces facteurs expliquent la fragmentation de l'IA en de nombreux sous-domaines concurrents dédiés à une problématique ou une voie précise, allant même parfois jusqu'à choisir un nom qui évite l'expression désormais souillée d'« intelligence artificielle [McCorduck, 2004] ». L'IA a du coup été à la fois plus prudente mais aussi plus fructueuse que jamais [Wikipédia, 2013].

4.4. L'intelligence artificielle expérimentale

L'intelligence artificielle expérimentale est une discipline scientifique qui a pour rôle d'augmenter les connaissances, dans différents domaines du fonctionnement mental et social (*mémoire*, *langage*, *perception*, *conception*, *diagnostic*…), en utilisant les ordinateurs comme outils pour expérimenter des modèles. Les modèles proposés par les chercheurs d'autres disciplines, comme la *linguistique* ou la *psychologie cognitive*, sont des modèles descriptifs, qui permettent une analyse rétroactive des traces d'une activité. Il n'est pas possible de les tester directement sur des machines car, contrairement à l'homme, la machine ne comprend pas avant d'analyser ; elle a besoin d'un modèle pour agir, pas seulement pour décrire. Il faut donc concevoir des modèles plus profonds, des modèles de la production et de la compréhension des systèmes de signes et de leurs expressions [Nicolle, 1996].

4.5. Quand l'information devient-elle connaissance ?

Pour qu'une information devienne une connaissance, elle doit être appropriée par la personne (avec sa connaissance et ses compétences) et réutilisée. Cette appropriation n'est pas un processus fiable ; selon le type de connaissance, l'expression et/ou la formalisation (cours, compagnonnage, article, présentation, mail…), le contexte de réutilisation, la compétence (aptitude à), et n'oublions pas la motivation, le résultat n'est pas garanti.
Si on prend l'organisation comme un système (complexe), l'information devient une connaissance quand celle-ci modifie le système et en particulier, sa manière de « penser » et de faire. Il y a donc un processus de traitement de l'information et de fabrication de connaissance qui passe essentiellement par l'humain.

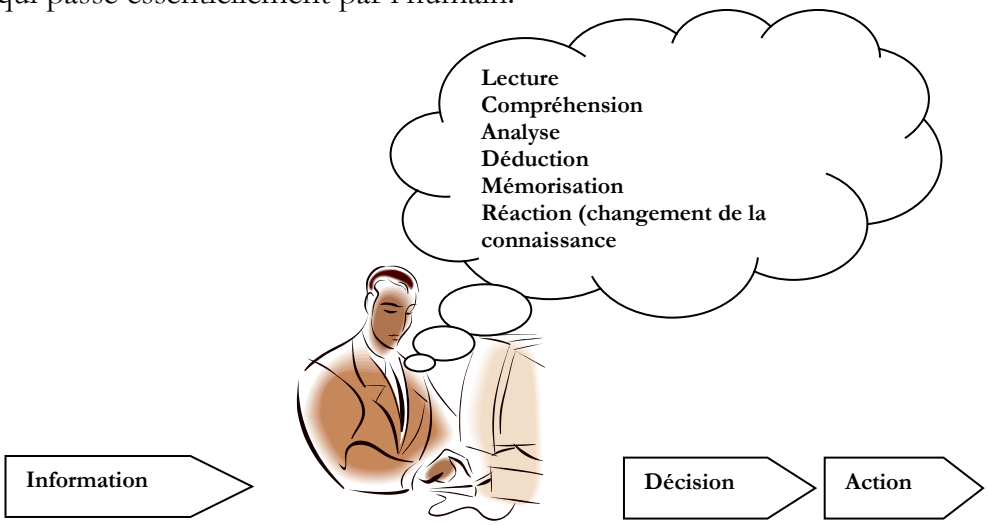


Figure 4.2 : Le raisonnement humain comme processus de traitement de l'information.

4.6. Domaines d'application de l'Intelligence Artificielle

L'Intelligence Artificielle trouve ses applications dans divers domaines (Cf. Figure 4.3) :

- Les systèmes experts.
- La représentation des connaissances.
- Le traitement du langage naturel.
- La résolution de problèmes.
- La reconnaissance biométrique.
- La robotique.
- L'apprentissage.
- L'aide au diagnostic médical.

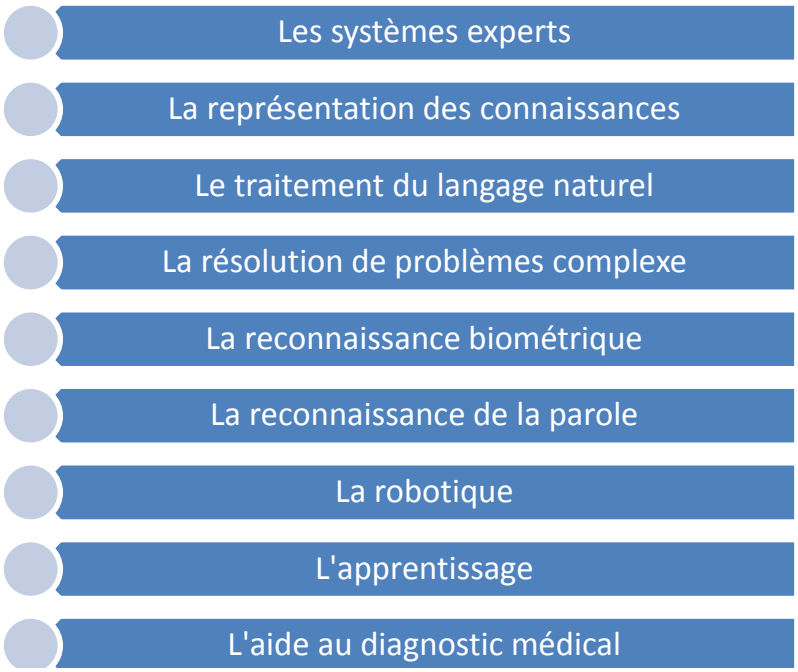


Figure 4.3 : Domaines d'application de l'Intelligence Artificielle.

4.7. L'apprentissage automatique

4.7.1. Définition

L'**apprentissage automatique** (*machine learning* en anglais), un des champs d'étude de l'intelligence artificielle, est la discipline scientifique concernée par le développement, l'analyse et l'implémentation de méthodes automatisables qui permettent à une machine (au sens large) d'évoluer grâce à un processus d'apprentissage, et ainsi de remplir des tâches qu'il est difficile ou impossible de remplir par des moyens algorithmiques plus classiques[Wikipédia, 2013] .

Des systèmes complexes peuvent être analysés, y compris pour des données associées à des valeurs symboliques (ex: sur un attribut numérique, non pas simplement une valeur numérique, *juste un nombre*, mais une valeur probabilisée, c'est-à-dire un nombre assorti d'une probabilité ou associé à un intervalle de confiance) ou un ensemble de modalités possibles sur un attribut numérique ou catégoriel. L'analyse peut même concerner des données présentées sous forme de graphes ou d'arbres, ou encore de courbes (par

exemple, la courbe d'évolution temporelle d'une mesure ; on parle alors de *données continues*, par opposition aux *données discrètes* associées à des attributs-valeurs classiques).

Le premier stade de l'analyse est celui de la *classification*, qui vise à *« étiqueter »* chaque donnée en l'associant à une classe. Différents systèmes d'apprentissage existent, utilisant divers algorithmes, selon un type d'apprentissage recommandé par l'application. (Cf. figure 4.4).

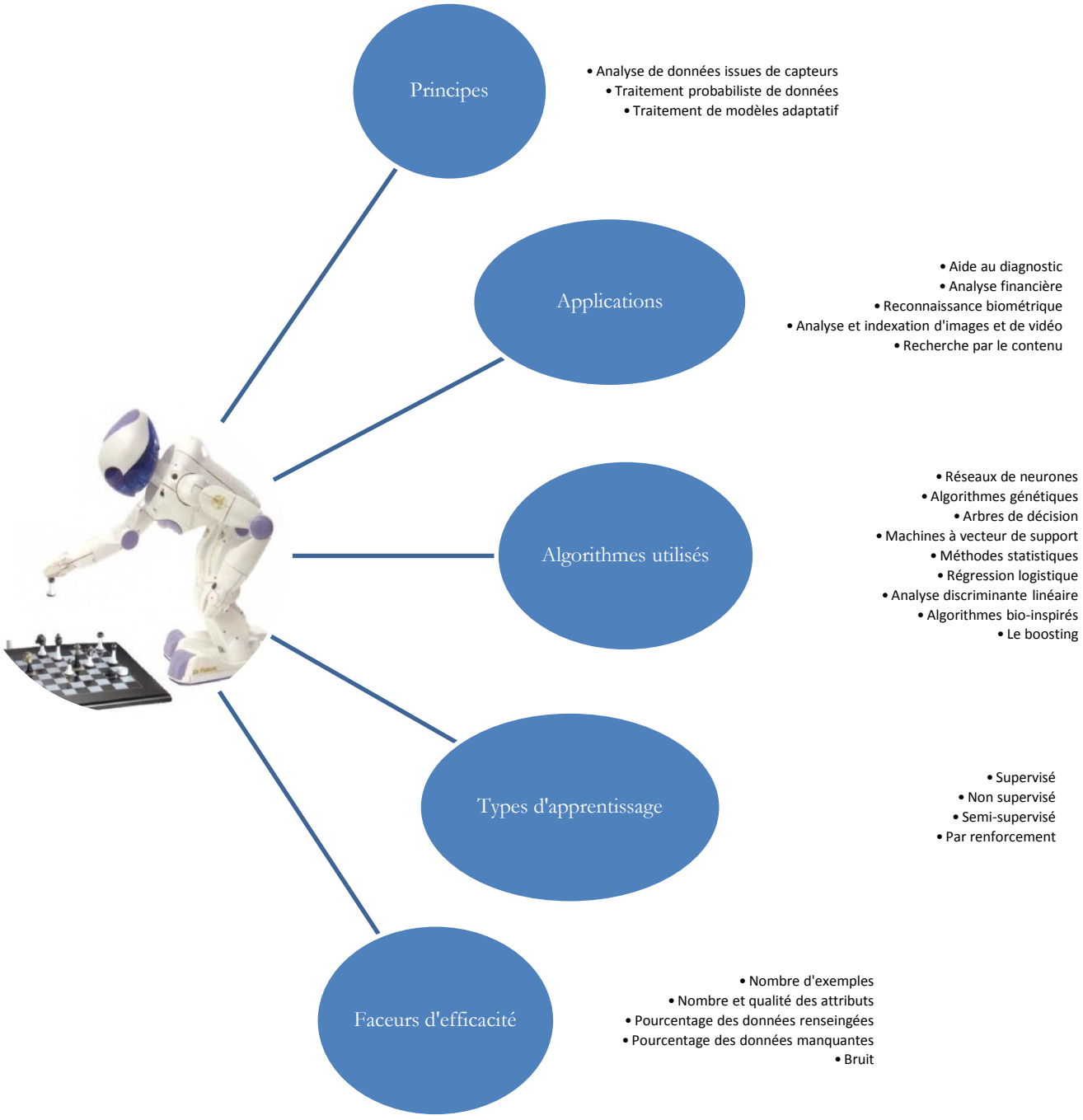


Figure 4.4 : Les différentes facettes de l'apprentissage automatique.

4.7.2. Types d'apprentissage

Les algorithmes d'apprentissage peuvent se catégoriser selon le mode d'apprentissage qu'ils emploient :

a. **L'apprentissage supervisé**

Si les *classes* sont prédéterminées et les *exemples* connus, le système apprend à classer selon un *modèle* de classement ; on parle alors d'apprentissage supervisé (ou d'analyse discriminante). Un expert (ou *oracle*) doit préalablement étiqueter des exemples. Le processus se passe en deux phases. Lors de la première phase (hors ligne, dite d'*apprentissage*), il s'agit de déterminer un modèle des données étiquetées. La seconde phase (en ligne, dite de *test*) consiste à prédire l'étiquette d'une nouvelle donnée, connaissant le modèle préalablement appris. Parfois il est préférable d'associer une donnée non pas à une classe unique, mais une probabilité d'appartenance à chacune des classes prédéterminées (on parle alors d'apprentissage supervisé probabiliste).

b. L'apprentissage non-supervisé (ou **classification automatique)**

Quand le système ou l'opérateur ne disposent que d'exemples, mais non d'étiquettes, et que le nombre de classes et leur nature n'ont pas été prédéterminés, on parle d'apprentissage non supervisé ou *clustering*. Aucun expert n'est requis. L'algorithme doit découvrir par lui-même la structure plus ou moins *cachée* des données. Le partitionnement de données, *data clustering* en anglais, est un algorithme d'apprentissage non supervisé. Le système doit ici -- dans l'espace de description (la somme des données) -- cibler les données selon leurs attributs disponibles, pour les classer en groupe *homogènes* d'exemples. La similarité est généralement calculée selon une fonction de distance entre paires d'exemples. C'est ensuite à l'opérateur d'associer ou déduire du sens pour chaque groupe et pour les motifs (*patterns* en anglais) d'*apparition* de groupes, ou de groupes de groupes, dans leur *« espace »*. Divers outils mathématiques et logiciels peuvent l'aider. On parle aussi d'analyse des données en régression (ajustement d'un modèle par une procédure de type moindres carrés ou autre optimisation d'une fonction de *coût*). Si l'approche est probabiliste (c'est-à-dire que chaque exemple, au lieu d'être classé dans une seule classe, est caractérisé par un jeu de probabilités d'appartenance à chacune des classes), on parle alors de *« soft clustering »* (par opposition au *« hard clustering »*). Cette méthode est souvent source de sérendipité.

c. L'apprentissage semi-supervisé

Effectué de manière probabiliste ou non, il vise à faire apparaître la distribution sous-jacente des *« exemples »* dans leur espace de description. Il est mis en œuvre quand des données (ou *« étiquettes »*) manquent. Le modèle doit utiliser des exemples *non-étiquetés* pouvant néanmoins renseigner. Ex : En médecine, il peut constituer une aide au diagnostic ou au choix des moyens les moins onéreux de tests de diagnostic.

d. L'apprentissage partiellement supervisé (probabiliste ou non**)**

Quand l'étiquetage des données est partiel. C'est le cas quand un modèle énonce qu'une donnée n'appartient pas à une classe *A*, mais peut-être à une classe *B* ou *C* (*A, B* et *C* étant 3 maladies par exemple évoquées dans le cadre d'un diagnostic différentiel).

e. L'apprentissage par renforcement [Mitchell, 1997]

L'algorithme apprend un comportement étant donné une observation. L'action de l'algorithme sur l'environnement produit une valeur de retour qui guide l'algorithme d'apprentissage. L'algorithme de *Q-learning* est un exemple classique.

4.7.3. Facteurs de pertinence et d'efficacité

La qualité de l'apprentissage et de l'analyse dépendent du besoin en amont et *a priori* de la compétence de l'opérateur pour préparer l'analyse. Elle dépend aussi de la complexité du modèle (spécifique ou généraliste), de son adéquation et de son adaptation au sujet à traiter. *In fine*, la qualité du travail dépendra aussi du mode (de mise en évidence visuelle) des résultats pour l'utilisateur final (un résultat pertinent pourrait être caché dans un schéma trop complexe, ou mal mis en évidence par une représentation graphique inappropriée).
Avant cela, la qualité du travail dépendra de facteurs initiaux contraignants, liées à la base de données :

1. **Nombre d'*exemples*** (moins il y en a, plus l'analyse est difficile, mais plus il y en a, plus le besoin de mémoire informatique est élevé et plus longue est l'analyse) ;
2. **Nombre et qualité des attributs** décrivant ces exemples. La distance entre deux "exemples" numériques (*prix*, *taille*, *poids*, *intensité lumineuse*, *intensité de bruit*, etc) est facile à établir, celle entre deux attributs catégoriels (*couleur*, *beauté*, *utilité*, …) est plus délicate ;
3. **Pourcentage de données renseignées** et manquantes ;
4. **« Bruit »** : le nombre et la « *localisation* » des valeurs douteuses (erreurs potentiels, valeurs aberrantes…) ou naturellement non-conformes au pattern de distribution générale des « *exemples* » sur leur espace de distribution impacteront sur la qualité de l'analyse.

4.8. La reconnaissance des formes

La reconnaissance des formes permet de reproduire les capacités de l'homme à reconnaître des *caractères*, des *objets*, des *sons*, des *Signaux temporels*. Dans ce paradigme de recherche surgissent deux grands objets d'étude:

- Le premier consiste à étudier de quelle manière l'être humain effectue cette reconnaissance (touche à des domaines comme psychologie, physiologie, biologie)
- Le second consiste à viser le développement de théories et de techniques permettant d'effectuer certaines tâches de reconnaissance (domaines: informatique, statistique, mathématiques).

4.8.1. Processus de reconnaissance

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 (Cf. Figure 4.5) :

1. Numérisation : obtenir une représentation des données à traiter qui soit manipulable en machine.
2. Prétraitement : élimination des bruits, normalisation, re-échantillonnage, amélioration des contrastes, etc.

3. Calcul des représentations : obtenir une représentation des données compatible avec les outils d'apprentissage et de décision utilisés.
4. Apprentissage : à partir d'un ensemble d'exemplaires, construire une représentation des classes.
5. Analyse : assigner une forme inconnue à une classe.
6. Post-traitement : valider les décisions de l'analyse sur la base de connaissances (du domaine).

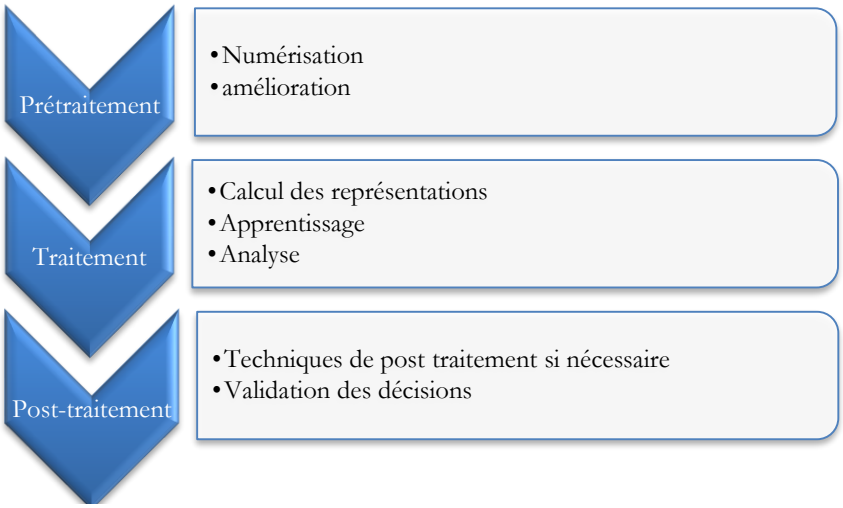


Figure 4.5 : Schéma classique du processus de reconnaissance des formes.

4.8.2. Méthodes de reconnaissance des formes

Les méthodes de la Reconnaissance des Formes sont souvent regroupées en grandes classes identifiées par : statistique, syntaxique, structurelle, hybride (voir figure 4.6).

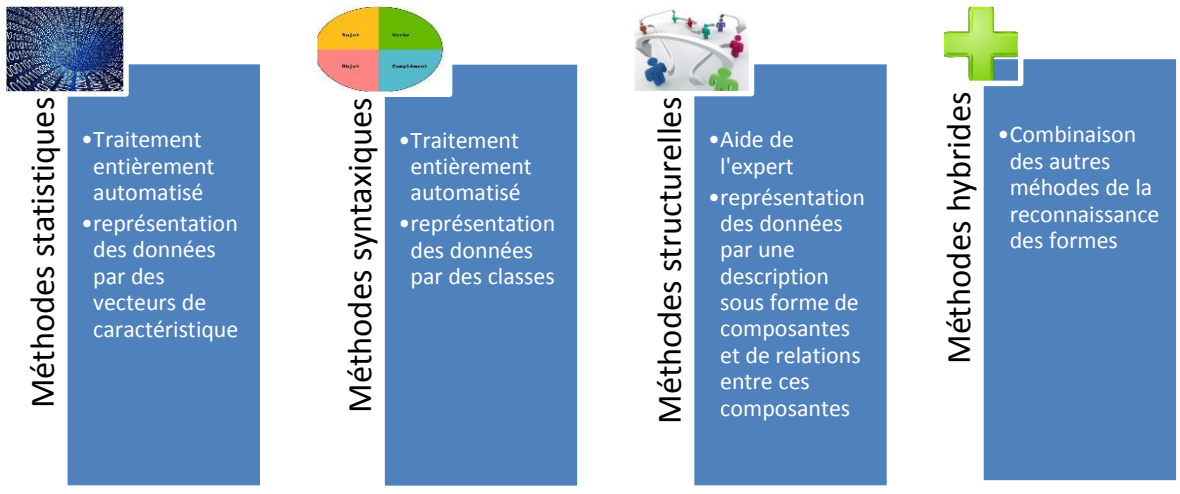


Figure 4.6 : Méthodes de la reconnaissance des formes.

A ces classes correspondent différentes manières de représenter les exemplaires et les classes et différentes méthodes pour l'apprentissage et la reconnaissance. Mais elles correspondent aussi à différentes façons d'aborder le problème de la reconnaissance de formes.

- Les méthodes statistiques et syntaxiques utilisent un traitement entièrement automatisé où le *maître* à simuler étiquette les réalisations qui seront utilisées pour l'apprentissage et

pour la validation de la reconnaissance. Ces méthodes fournissent un traitement pour induire des tests d'appartenance à partir d'un ensemble d'échantillons.

- Les méthodes structurelles utilisent une autre démarche (le maître devient l'expert). Ce dernier aide à expliciter les descriptions, à construire la représentation des classes et les critères de décision.
- Les méthodes hybrides ne signifient pas un remplacement des démarches et méthodes passées mais un enrichissement de l'ensemble des méthodes dans lequel il faudra trouver celles qui sont les mieux adaptées au problème traité.

4.8.3. La décision dans un système de reconnaissance des formes

La validation d'une méthode de reconnaissance de formes se fait par comparaison des résultats de la reconnaissance automatique aux étiquettes données par le maître. On en tire donc les taux de **reconnaissance** et les taux d'**erreur**. On peut aussi avoir des taux de **rejet** qui correspondent à la décision de ne pas classer la forme.

Le système en évaluant un critère de décision peut assigner une forme à une classe mais il peut aussi déterminer avec quelle confiance il effectue cette décision. Si le critère de décision prend des valeurs très proches pour plusieurs classes, la confiance dans la décision est faible.

La décision finale est en général le résultat de plusieurs décisions intermédiaires qui peuvent être organisées hiérarchiquement.

4.9. Conclusion

l'intelligence artificielle consiste à créer des systèmes informatiques qui allient les capacités de stockage, recherche et synthèse d'un ordinateur à ce qu'il y a de meilleur dans l'intelligence humaine, à savoir nos facultés de *compréhension*, de *cognition* et de *raisonnement*.

L'intelligence artificielle (IA) regroupe les ressources nécessaires pour manipuler de l'information tandis que la cognition rassemble les divers processus mentaux qui vont de l'analyse perceptive de l'environnement à la commande motrice et qui fait appel à l'informatique et aux neurosciences.

Dans ce chapitre nous avons présenté une introduction au domaine de l'IA, sa définition, son fondement théorique, ses domaines d'application. Le point est mis sur les notions de l'apprentissage automatique et la reconnaissance des formes.

Chapitre 5

LA LOGIQUE FLOUE

5.1. Introduction

La logique floue est destinée à traiter l'imprécis et l'incertain. Elle est fondée sur des règles théoriques logiques permettant à un système informatique de raisonner « comme » un être humain. Les avantages de l'application de la logique floue se voient par les progrès qu'elle a réalisés dans des domaines variés comme la robotique. Dans ce chapitre nous présentons un état de l'art sur la logique floue, nous tenons à donner l'essentiel de cette théorie ce qui nous aide dans la conception du module d'appariement flou de notre système biométrique multimodal. Les données pourront être également de type *imparfait* (imprécis, incertain et incomplet). C'est le cas qui nous concerne, notre problématique traite des informations imparfaites. C'est pourquoi nous discutons en détail cette notion.

5.2. Définition de la logique floue

- **Définition 1 [Wikipédia, 2013]**

La logique floue (*fuzzy logic*, en Anglais) est une extension de la logique classique aux raisonnements approchés. Par ses aspects numériques, elle s'oppose aux logiques modales.

Formalisée par Lotfi Zadeh en 1965, outil de l'intelligence artificielle, elle est utilisée dans des domaines aussi variés que l'automatisme (freins ABS, conduite de processus), la robotique (reconnaissance de formes), la gestion de la circulation routière (feux rouges), le contrôle aérien (gestion du trafic aérien), l'environnement (météorologie, climatologie, sismologie, analyse du cycle de vie), la médecine (aide au diagnostic), l'assurance (sélection et prévention des risques) et bien d'autres.

- **Définition 2 [Zadeh, 1996]**

Selon Lotfi.A Zadeh dans sa référence [Zadeh, 1996], la logique floue est synonyme de « raisonnement avec les mots ». La contribution majeure de la logique floue c'est l'introduction d'une nouvelle méthodologie à base de raisonnement avec les mots (computing with words). Selon son inventeur, Il n'existe pas de méthodologie de raisonnement similaire comme la logique des prédicats (predicate logic), la théorie des probabilités (probability theory), la théorie des réseaux de neurones (neural network theory), les réseaux bayesiens (bayesian network), et le contrôle classique (classical control).

- **Définition 3 [Zadeh, 2008]**

La logique floue n'est pas imprécise, c'est une logique précise de l'imprécision et du raisonnement approximatif. Spécifiquement, la logique floue peut être vue comme une tentative de formalisation/mécanisation de deux capacités humaines remarquables. Qui sont : le raisonnement et le cognition.

- **Définition 4 le flou « Fuzziness » [Ponce-Cruz, 2010]**

Dans notre langage quotidien, nous utilisons beaucoup de caractère vague et imprécis, qui peut également être appelé flou. Nous sommes préoccupés par la façon dont nous pouvons représenter et manipuler les inférences avec ce genre d'information. Quelques exemples: la taille d'une personne et son âge. Des termes tels que grands et jeunes sont floues car elles ne peuvent pas être définies précisément, bien que, comme les humains, nous utilisons ces informations pour prendre des décisions. Quand nous voulons .classer une personne comme grand ou jeune, il est impossible de décider si la personne est dans un ensemble ou pas. En donnant un degré de pertinence pour le sous-ensemble, aucune information n'est perdue lorsque le classement est effectué.

5.3. Historique

Le développement de la logique floue constituerait un événement historique significatif, dans la construction d'un pont privilégié et particulièrement fécond entre le champ de la logique et celui des connaissances imparfaites.

Des historiens font remonter l'histoire de la logique floue à l'antiquité grecque [Rosental, 1998]. Ce type de narration construit une généalogie des idées liant Héraclite et Platon à Zadeh, en passant par Hegel, Marx, Engels et Knuth.
Héraclite avança l'idée que certaines propositions pouvaient être à la fois vraies et non vraies. **Platon** fait alors figure de fondateur de ce qui allait devenir la logique floue, dans la mesure il indiquait qu'il existait un domaine tiers (par delà le vrai et le faux) où les opposés "prenaient certaines libertés". Pour Brule, c'est dans cet esprit que **Lotfi Zadeh** aurait élaboré la logique floue comme une logique possédant une infinité de valeurs de vérité, sur les traces successives d'**Hegel**, de **Marx**, d'**Engels**, et plus récemment du travail de **Lukasiewicz** et de **Knuth** sur les logiques à trois valeurs de vérité [Rosental, 1998].
L'auteur dans la référence [Elkosantini, 2013] présente l'historique des ensembles flous suivant :

1965 : Théorie des ensembles flous introduite par **L.A. Zadeh** (UC Berkeley)

En 1973, le Pr. Zadeh publie un article (dans l'IEEE Transactions on Systems, Man and Cybernetics) qui mentionne pour la première fois le terme de variables linguistiques (dont la valeur est un mot et non un nombre).

En 1974, première application industrielle. Régulation floue d'une chaudière à vapeur réalisée par Mamdani.

En 1980, F.L. Smidth & Co. A/S (au Danemark) met en application la théorie de la logique floue dans le contrôle de fours à ciment. C'est la première mise en œuvre pratique de cette nouvelle théorie.

Dans les années 80, plusieurs applications commencent à immerger (notamment au Japon).

1990: Généralisation de l'utilisation de cette technique dans :

- Appareils électroménagers (laves-linges, aspirateurs, autocuiseurs,...etc) ,
- Systèmes audio-visuels (appareils de photos autofocus, caméscopes à stabilisateur d'images,
- photocopieurs,...
- Systèmes automobiles embarqués (BVA, ABS, suspension, climatisation,...etc.),
- Systèmes autonomes mobiles,
- Systèmes de décision, diagnostic, reconnaissance,
- Systèmes de contrôle/commande dans la plupart des domaines industriels de production.

5.4. Définition des ensembles flous

La théorie des ensembles flous consiste le fondement théorique de la logique floue. La théorie des *ensembles flous*. de Lotfi.A Zadeh est une extension de la théorie des ensembles classiques aux ensembles définis de façon imprécise. Partant d'un concept de fonction d'appartenance à valeur dans [0, 1], Zadeh redéfinit ce qu'est un sous-ensemble d'un univers donné, bâtit un modèle complet de propriétés et de définitions formelles, et montre que cette théorie des sous-ensembles flous se réduit effectivement à la théorie des

sous-ensembles classiques dans le cas où les fonctions d'appartenance ne prennent que les valeurs binaires de{0,1}.[Wikipédia,2013].

Les ensembles flous, où de nombreux degrés d'appartenance sont autorisés, et indiquées avec un nombre compris entre 0 et 1. Le point de départ pour des ensembles flous est tout simplement la généralisation de l'évaluation prévue à partir de la paire de nombres {0,1}.pour tous les nombres de [0,1]. » [Ponce-Cruz, 2010].

5.4.1. Fonctions d'appartenance

Les fonctions d'appartenance sont des outils mathématiques pour indiquer l'appartenance souple à un ensemble, la modélisation et la quantification de la signification des symboles. Ils peuvent représente rune notion subjective d'une classe vague, tels que des chaises dans une salle, la taille de la population, et performance parmi d'autres. Généralement, il ya deux façons de désigner un ensemble flou. Si X est l'univers du discours, et x est un élément particulier de X, un ensemble flou A définie sur X peut s'écrire comme une collection de paires ordonnées.

5.4.2. Concepts fondamentaux

Dans l'approche floue :

- Un élément peut appartenir plus ou moins fortement à cette classe.
- Un sous-ensemble flou A d'un référentiel X est caractérisé par une fonction d'appartenance μ_A

$$\forall \mathbf{x} \in \mathbf{X} \ \boldsymbol{\mu}\mathbf{A} \in [\mathbf{0}, \mathbf{1}] \qquad (5.1)$$

Le degré d'appartenance donne la valeur de la vérité.

a. La fonction d'appartenance

La fonction d'appartenance décrivant un sous-ensemble flou est caractérisée par quatre propriétés : [zadeh, 1997]

- **Le type** : la forme du nombre flou qui peut être triangulaire, trapézoïdale, gaussienne ou sigmoïdale.
- **La hauteur** : H(A) = Sup $_{x\epsilon X}$ (μ(x)) de la fonction d'appartenance. Un sous-ensemble flou est dit normalisé s'il est de hauteur 1.
- **Le noyau** : N(A) = {x/μ_A(x) = 1} est l'ensemble des éléments qui appartiennent totalement à A. Pour les fonctions de type triangulaire, le noyau est un singleton qui est appelé aussi valeur modale.
- **Le support** : S(A) = {x/μ_A(x) ≠ 0} ; cet ensemble décrit l'ensemble des éléments qui sont partiellement dans A.

Les figures 5.1 et 5.2 montrent les types et les caractéristiques de l'ensemble flou.

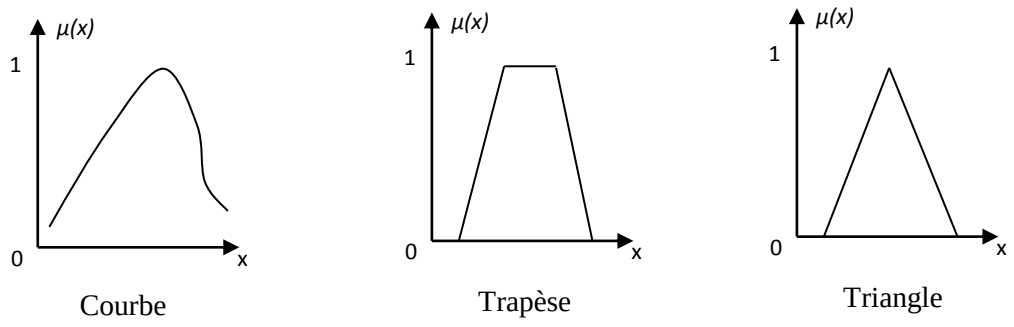


Figure 5.1 : Les types de l'ensemble flou (Courbe, Trapèze, Triangle).

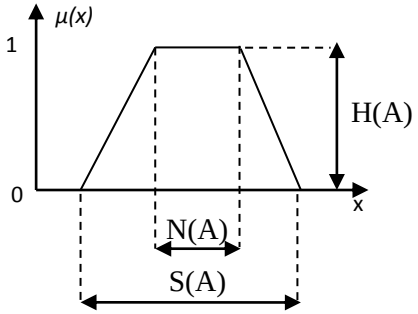


Figure 5.2. : La hauteur H de l'ensemble flou, son noyau N et son support S.

Notations :

- L'intervalle flou couramment utilisé dans R est décrit par sa fonction d'appartenance.
- Un nombre flou trapézoïdale est notée généralement par (a, b, α, β)
- Un nombre flou triangulaire est un cas particulier d'un nombre trapézoïdale. Il est notée généralement par (a, α, β). Dans le domaine de la recherche, ce type de nombres flous est très utilisé:

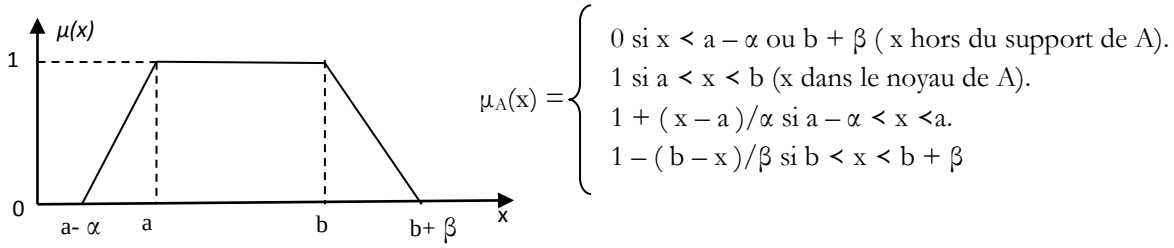
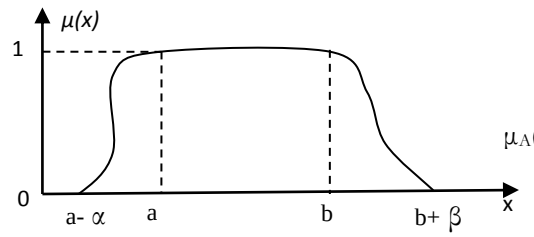


Figure 5.3 : Fonction d'appartenance d'un ensemble flou.

La fonction d'appartenance d'un nombre flou avec des cotés paraboliques est définie de la manière suivante :



$$\mu_A(x) = \begin{cases} 0 \text{ si } x < a - \alpha \text{ ou } b + \beta \text{ (x hors du support de A).} \\ 1 \text{ si } a < x < b \text{ (x dans le noyau de A).} \\ \text{Si } a - \alpha < x < a - \alpha/2 \text{ alors } 2(x - a+\alpha)^2/\alpha^2 \\ \text{Si } a - \alpha/2 < x < a \text{ alors } 1 + 2(x - a)^2/\alpha^2 \\ \text{Si } b < x < b + \beta/2 \text{ alors } 1 - 2(b - x)^2/\beta^2 \\ \text{Si } a + \beta/2 < x < b \text{ alors } 2(x - b + \beta)^2/\beta^2 \end{cases}$$

Figure 5.4 : Fonction d'appartenance d'un ensemble flou avec cotés paraboliques.

Remarque : Les nombres flous de formes gaussienne est un cas particulier.

b. Le support

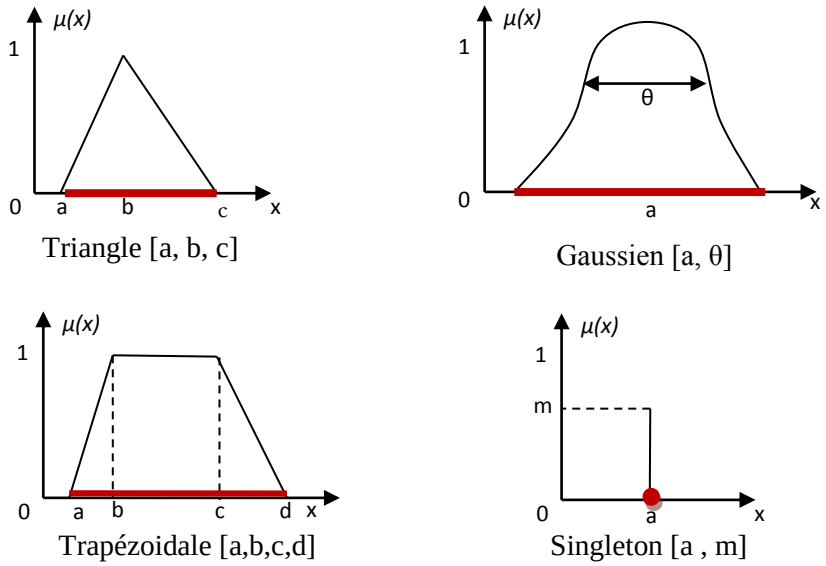


Figure 5.5 : Les différents supports d'un ensemble flou.

c. Le noyau :

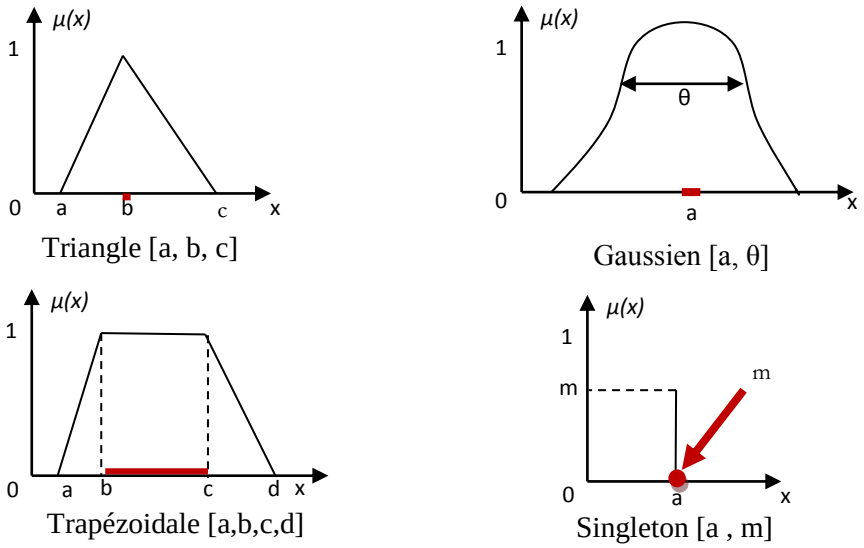


Figure 5.6: Les différents noyaux d'un ensemble flou.

5.4.3. Les opérateurs flous

Extension des opérations de la théorie des ensembles classiques: = ∪ , ∩, ç; complément.

A et B deux sefs de X, définis par les fonctions d'apprentissage $\mu_A(x)$

L'ensemble des personnes petites ou moyennes est un ensemble flou de fonction d'appartenance :

a. Egalité de sefs

$$\mathbf{A = B\ ssi\ \forall\ x\ \in X, \mu A(x) = \mu B(x)} \qquad (5.2)$$

b. Inclusion de sefs

$$\mathbf{A \subset B\ ssi\ \forall\ x\ \in X, \mu A(x) < \mu B(x)} \qquad (5.3)$$

c. Intersection de sefs

$$\mathbf{\forall\ x\ \in X,\ \mu A \cap B(x) = min(\ \mu A(x), \mu B(x))} \qquad (5.4)$$

d. Union de sefs

$$\mathbf{\forall\ x\ \in X,\ \mu A \cup B(x) = max(\ \mu A(x), \mu B(x)} \qquad (5.5)$$

$$\mathbf{\mu\ A \cup B(x) = max(\mu A(x), \mu B(x))\ \forall\ x\ \epsilon U} \qquad (5.6)$$

5.4.4. La distance entre ensembles flous

La distance entre deux ensembles flous A et B est :

$$\mathbf{d(A, B) = |\mu A(x) - \mu B(x)|(x\ \in X)} \qquad (5.7)$$

Ou autrement :

$$\mathbf{\int_a^b |\mu A(x)\ -\ \mu B(x)\ |\ dx} \qquad (5.8)$$

La notion de distance entre ensembles flous peut être utile pour définir des relations telles que «*à peu près égal*» ou «*très supérieur à*».

5.4.5. Les valeurs linguistiques

- L'ensemble de référence d'un mot du langage naturel s'appelle l'univers du discours.

- Une variable linguistique représente un état dans le système à régler.

- Sa valeur est définie dans des termes linguistiques qui peuvent être des mots ou des phrases d'un langage naturel.

Exemples:

Grand , petit, moyen.

Fort, faible, Jeune, âgé, vieux, très jeune.

5.5. Système d'inférence floue

Les connaissances utilisées pour construire un système d'inférence floue sont toujours incertaines, les sources de l'incertitude sont multiples [Wu and Mendel, 2002]: Les mots utilisés par les entrées et les sorties d'un système peuvent avoir de différentes définitions selon différentes personnes.

- Les conséquences obtenues par l'interrogation d'un groupe d'experts peuvent variées.
- Les données d'apprentissage sont bruitées.
- Les mesures activant le système d'inférence floue sont bruitées.

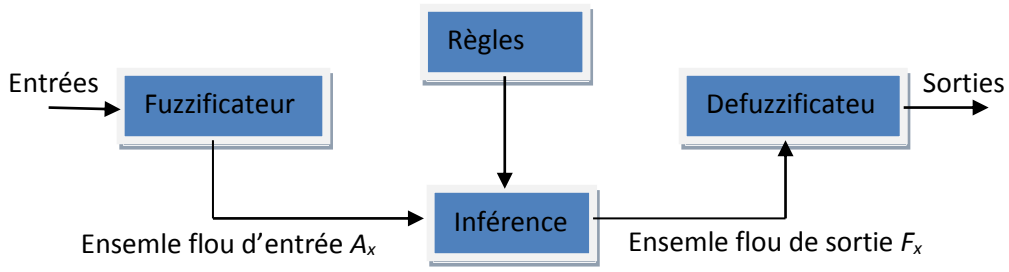


Figure 5.7: Système d'inférence flou.

Un système d'inférence flou comporte les étapes suivantes [Mendal et al, 2006] :

- La fuzzification.
- L'inférence floue.
- La defuzzification.

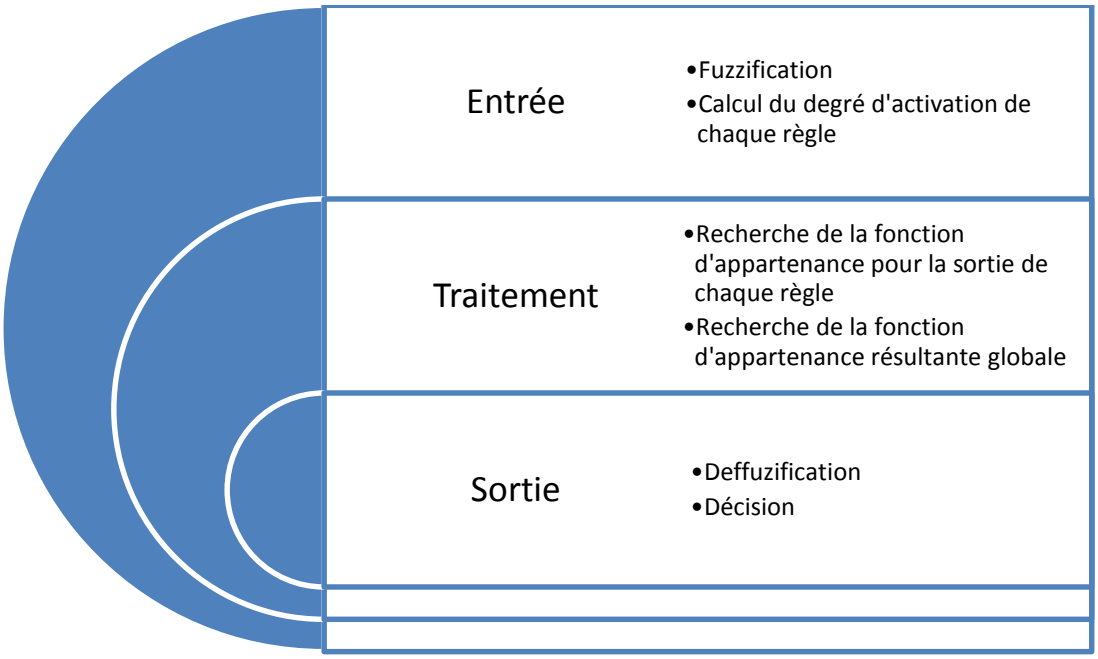


Figure 5.8: Etapes du système d'inférence flou.

5.6. La fuzzification

Lotfi.A Zadeh dans sa référence [Zadeh, 1997] a présenté une succincte définition de la fuzzification, nous présentons dans la figure 5.9 une schématisation de la transformation d'un ensemble intervalle (*crisp set*) vers un ensemble flou (*fuzzy set*).

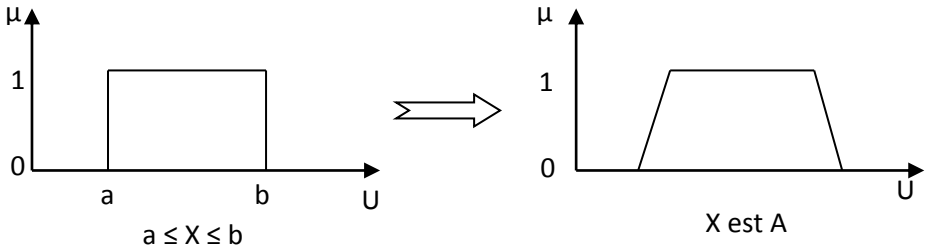


Figure 5.9: La fuzzification.

Nous présentons par la suite un exemple d'inférence floue (Cf. Figure 5.10) :

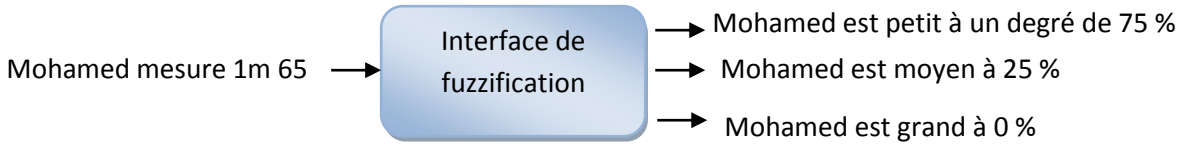


Figure 5.10: Exemple d'inférence floue

Il s'agit d'attribuer à chaque variable des degrés d'appartenance à différents états que l'on doit définir. Pour simplifier, nous allons définir trois états sorties (petit, moyen et grand). Ensuite, nous allons établir les degrés d'appartenance à ces états à l'aide de graphique (l'interface de fuzzification).

5.7. L'imprécis et l'incertain

Les données de type *imparfait* sont des données imprécises, incertaines ou incomplètes. L'imperfection des informations fait appel à plusieurs concepts. Le premier, généralement bien maîtrisé, concerne l'imprécision des informations. L'incertitude est un second concept à différencier de l'imprécision par le fait qu'il ne fait pas référence au contenu de l'information mais à sa qualité. Décrivons, de manière plus détaillée, ces deux notions :
L'imprécis : les imprécisions correspondent à une difficulté dans l'énoncé de la connaissance, soit parce que des connaissances numériques sont mal connues, soit parce que des termes du langage naturel sont utilisés pour qualifier certaines caractéristiques du système de façon vague. Le premier cas est la conséquence d'une insuffisance des instruments d'observation (2000 à 3000 manifestants), d'erreurs de mesure (poids à 1% près) ou encore de connaissances flexibles (la taille d'un adulte est environ entre 1,5 mètre et 2 mètres). Le second provient de l'expression verbale des connaissances (température douce, proche de la plage) ou de l'utilisation de catégories aux limites mal définies (enfant, adulte, vieillard).

L'incertain : les incertitudes concernent un doute sur la validité d'une connaissance. Celles-ci peuvent provenir de la fiabilité relative à l'observation faite par un système, celui-ci pouvant être sûr, susceptible de commettre des erreurs ou de donner intentionnellement des informations erronées, ou encore d'une difficulté dans l'obtention ou la vérification de la connaissance (l'affirmation d'une forte douleur par un patient). Des incertitudes sont également présentes dans le cas des prévisions (en météorologie par exemple). Pour une proposition incertaine, c'est la vérité même de la proposition qui est en cause.
Il existe d'autres sortes d'imperfections plus ou moins dépendantes de l'imprécision et de l'incertitude, telles que l'incomplétude et l'indétermination. On trouve parfois un problème dû à des connaissances hétérogènes et imparfaites, cas très fréquent en fusion d'images.

5.8. Conclusion

Dans ce chapitre nous avons présenté la théorie de la logique floue, sa définition, son fondement mathématique. Le point est mis sur la théorie des sous ensembles flous et le système d'inférence flou qui les utilise pour les raisons suivantes :

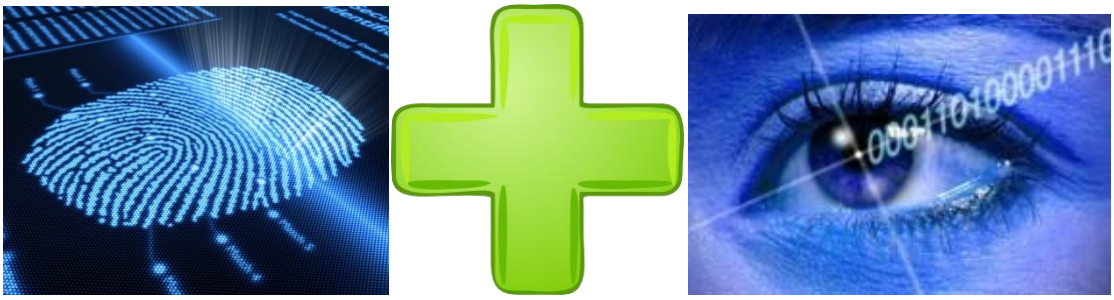
- Nous estimons modéliser les décisions provenant des deux systèmes biométriques monomodaux d'iris et d'empreinte par des ensembles flou.
- L'appariement par fusion multimodale sera effectué par un système d'inférence flou.
- Les sorties du système d'inférence flou serons des résultats « décisions » floues qui nécessitent la defuzzification.

Le chapitre suivant expliquera en détail l'introduction de la logique floue dans le module d'appariement du système biométrique multimodal proposé.

Troisième partie

Multimodalité biométrique

Approches proposées



Chapitre 6

RECONNAISSANCE D'IRIS PAR FUSION DE DECISIONS

6.1. Introduction

La recherche dans le domaine de la biométrie multimodale est relativement récente. De nombreuses études ont été menées en associant différentes modalités, en faisant varier le niveau de fusion des données biométriques et en testant plusieurs stratégies de fusion.

La reconnaissance de l'iris pour l'identification des personnes a été proposée à l'origine en 1936, et depuis cette date, des progrès ont été réalisés et des technologies ont été conçues.

La recherche dans le domaine de la reconnaissance de l'iris se heurte à de nombreux défis technologiques. Les systèmes de reconnaissance de l'iris sont généralement très couteux et volumineux. De plus, l'efficacité de ces systèmes souvent influencée par la variabilité des mouvements et de la qualité de l'image d'iris.

Dans ce travail nous tentons d'inclure des informations sur la qualité de l'image d'iris afin de renforcer l'efficacité de la reconnaissance. La fusion de sources multiples d'information est envisagée au niveau de *décision*.

L'idée principale est d'essayer de mimer le raisonnement de l'être humain quand à la décision de l'identité d'un prétendant. Les facteurs utilisés pour décider si un individu est authentique ou imposteur sont :

- Une décision d'un appariement automatique avec normalisation des scores des clients authentiques et imposteurs. Cet appariement utilise la distance de *Hamming*.
- Une décision d'un appariement automatique avec classification des scores des clients authentiques et imposteurs. Cet appariement utilise la distance *Euclidienne*.
- Une information à propos de la qualité de l'image d'iris, modélisé par une variable linguistique floue.

Ce chapitre est concerné par l'application d'une nouvelle méthode d'appariement par la fusion de décisions multiples pour la reconnaissance de l'iris. Nous donnerons tout d'abord une présentation du cadre dans lequel se situe le travail proposé. Ensuite, nous présenterons la formulation du problème suivie par les étapes de conception du système de reconnaissances d'iris par fusion floue de décisions. Nous conclurons le chapitre par une analyse et discussion des résultats expérimentaux.

6.2. Cadre du travail proposé

Les **T**echnologies de l'**I**nformation et de la **C**ommunication (**TIC**) regroupent les ressources nécessaires pour manipuler de l'information tandis que **l'intelligence artificielle** est une spécialisation de l'informatique dont l'objet est la résolution des problèmes complexes, en mimant les processus mentaux de l'homme, qui vont de l'analyse perceptive de l'environnement à la commande motrice et qui fait appel à l'informatique et aux neurosciences.

Comme le montre la figure 6.1, La biométrie et tout particulièrement **la reconnaissance d'iris par fusion floue des décisions** peut donc être vue comme étant au **croisement des TIC** incluses dans le domaine de **l'IA et de la logique floue.**

Le travail proposé fait appel aux techniques de la reconnaissance des formes, de l'apprentissage automatique, avec l'utilisation d'une nouvelle stratégie de fusion à base de la logique floue.

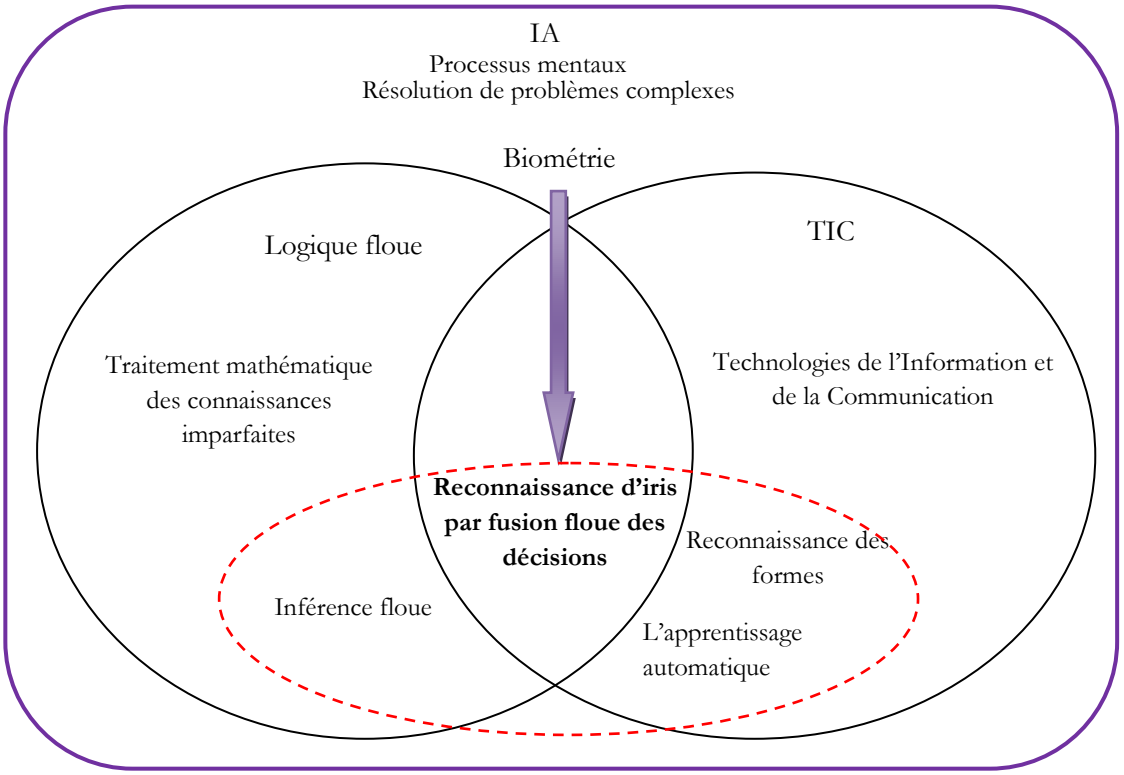


Figure 6.1 : Cadre du travail proposé.

6.3. Formulation du problème

L'iris est considéré comme un trait biométrique pertinent et précis, la reconnaissance d'individus par l'iris est très utilisée de nos jours, le problème posé par les systèmes de reconnaissance par l'iris est la qualité de l'image d'iris qui influe sur la décision de la reconnaissance. Une image d'iris de mauvaise qualité peut engendrer des erreurs comme l'impossibilité d'enrôlement (*failure to enroll*), ou l'impossibilité d'appariement (*failure to match*) et notamment les erreurs liés aux autorisations d'accès des clients (les fausses acceptations et les faux rejets).

La tendance actuelle est liée à l'amélioration des taux de ces erreurs (abaisser au maximum les taux d'erreurs) en agissant sur différents niveaux de traitement. Dans ce travail, nous avons proposé d'agir au niveau de la phase d'appariement en appliquant deux algorithmes d'appariement différents et en essayant de voir l'influence et l'apport de la fusion par l'inférence floue sur les résultats de reconnaissance du système.

Motivations:

- Surmonter les limites de la monomodalité biométrique en proposant une solution de multimodalité biométrique par fusion d'algorithmes agissant sur le même trait biométrique (l'iris).
- Utiliser la fuzzification des résultats, marquée par le degré d'appartenance aux ensembles flous modélisant les décisions du système. Elle offre un intervalle intermédiaire entre la décision d'accepter le client et la décision de le rejeter, donc le système peut déclarer une authentification comme « *fortement accepter* », ou bien « *fortement rejeter* ».

Objectifs :

- Arriver à un meilleur compromis entre le taux de fasse acceptation TFA et le taux de faux rejet TFR par rapport aux travaux de recherche sur l'identification par l'iris.
- Voir l'influence de paramètres sur les algorithmes implémentés.
- Voir l'impact de la fusion par l'inférence floue sur les résultats de reconnaissance du système.

6.4. Schéma général du système

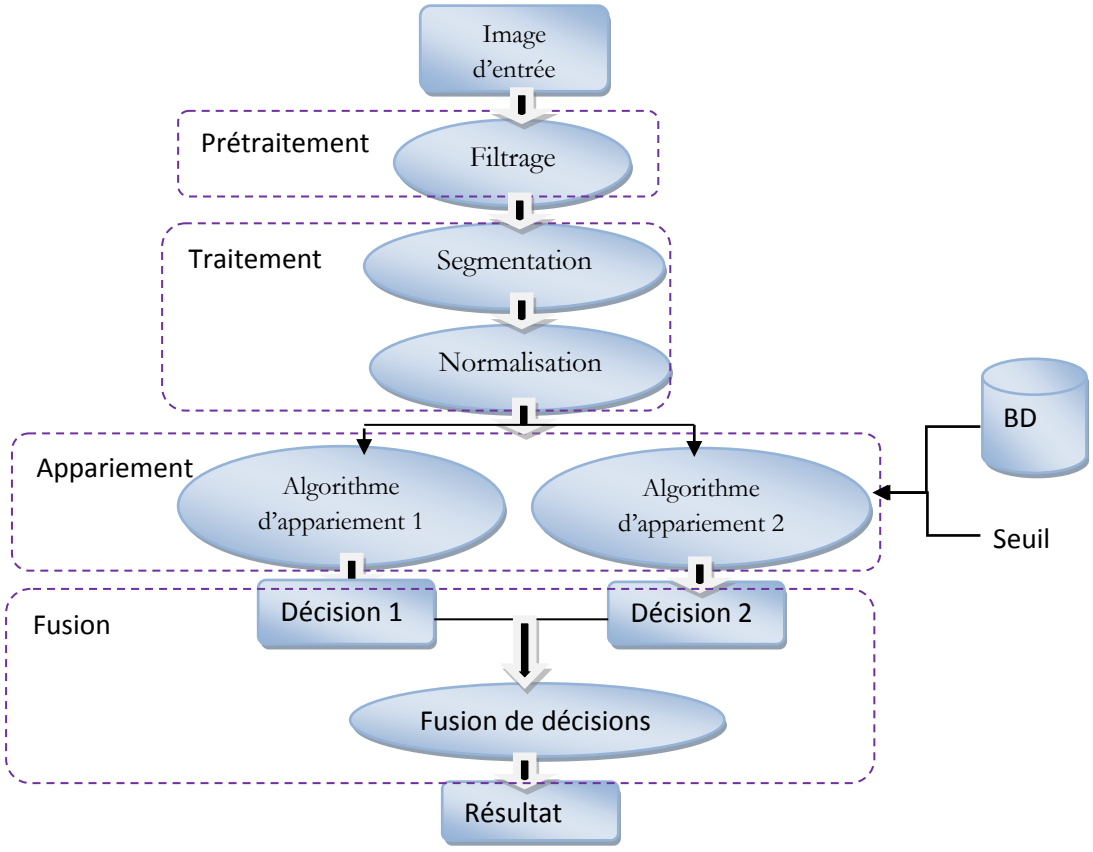


Figure 6.2 : Schéma général du système de reconnaissance par l'iris à base de fusion de décisions provenant d'appariements multiples.

La figure 6.2 représente le schéma général du système de reconnaissance par l'iris par fusion de décisions

Le système proposé comporte quatre phases consécutives, qui sont :

1. La phase de filtrage

Le filtrage a pour but de réduire le bruit de l'image d'entrée. Nous avons utilisé le filtre de Canny [Canny, 1986]. La première étape est de réduire le bruit de l'image originale avant d'en détecter les contours. Ceci permet d'éliminer les pixels isolés qui pourraient induire de fortes réponses lors du calcul du gradient, conduisant ainsi à de faux positifs.

2. La phase de traitement

Le traitement comporte deux processus, la segmentation et la normalisation. l'algorithme de normalisation utilisé est celui de Daugman [Daugman, 1994] « the rubber sheet model » détaillé au chapitre 3.

3. La phase d'appariement

- Dans cette phase nous avons implémenté deux algorithmes d'appariement, le premier est l'appariement par le calcul de la distance de *Hamming* entre les deux codes biométriques, et le deuxième est l'appariement par le calcul de la distance Euclidienne entre les deux codes biométriques.
- Les deux appariements produisent deux décisions selon des seuils définis. Dans L'appariement par la distance de *Hamming* nous avons fixé le seuil de reconnaissance à 0.35 pour la base de données CASIA-Iris V1, donc la décision d'appariement avec un seuil supérieur à cette borne est « rejeté », sinon la décision est « accepté ». quand à l'appariement par la distance *Euclidienne* nous n'avons pas pu définir un seul seuil de reconnaissance pour toute la base, les appariements varient selon un intervalle de valeurs,
- L'idée d'utiliser la *fuzzification* pour bien modéliser cette intervalle de seuils de reconnaissance nous a conduit à proposer trois ensemble flous modélisant chacun un type de reconnaissance, soit « bonne » pour une bonne reconnaissance, « moyenne » pour une reconnaissance moyenne et « mauvaise » pour une mauvaise reconnaissance.

4. La phase de fusion

Les deux appariements produisent deux décisions qui seront fusionnés par des règles floues (si alors). Les règles floues proposées sont :

Règle1 : Si décision-*Hamming* = « **accepter** » et décision-*Euclidienne* = « **bonne** » alors « **fortement Accepter** »

Règle2 : Si décision-*Hamming* = « **accepter** » et désicion-*Euclidienne* = « moyenne » alors « **Accepter** »

Règle3 : Si décision-*Hamming* = « **accepter** » et décision- *Euclidienne* = « mauvaise » alors « **Rejecter** »

Règle4 : Si décision- *Hamming* = « **rejeter** » et décision- *Euclidienne* = « bonne » alors « **Accepter** »

Règle5 : Si décision- *Hamming* = « **rejeter** » et décision- *Euclidienne* = moyenne alors « **rejeter** »

Règle6 : Si décision- *Hamming* = « **rejeter** » et décision- *Euclidienne* = « mauvaise » alors « **fortement rejeter** »

Dans ce qui suit nous donnerons plus de détails sur les valeurs de poids fixés pour chaque variable floue ainsi que les valeurs des distances d'appariements en relation avec chaque ensemble flou.

6.5. Outil d'aide au développement utilisé

Le génie logiciel peut se définir comme un ensemble composé d'une méthode, de modèles, d'outils d'aide au développement et de critères d'évaluation de la qualité permettant à un maître d'œuvre de produire un logiciel répondant aux besoins exprimés par un maître d'ouvrage. [Crampes, 2013].

Dans ce travail nous avons utilisé une des méthodes d'analyse et de conception les plus connues, la méthode d'analyse structurée et techniques de conception SADT (en anglais *Structured Analysis Structured Design*). La méthode SADT définie comme un langage pluridisciplinaire, favorise la communication entre utilisateurs et concepteurs. Les concepts de base de cette communication entre utilisateurs et concepteurs. Les concepts de base de cette méthode : concepts simples, basés sur un formalisme graphique et textuel facile. Permet de :

- Modéliser le problème. (Informatique ou non) puis expose la solution.
- Assure une communication efficace entre les différentes personnes concernées par le système.

Les limites du phénomène modélisé dépendant des objectifs du modèle. Pour ces raisons, le développement de logiciels dans un contexte professionnel suit souvent des règles strictes encadrant la conception et permettant le travail en groupe et la maintenance du code [Audibert, 2013]..Ainsi, nous détaillons dans ce qui suit la conception des systèmes de reconnaissance biométrique multimodale proposés, en utilisant la méthode d'analyse structurée SADT, tout en donnant à chaque étape et pour chaque sous module du système son DFD.

6.6. Les processus de reconnaissance implémentés

Trois processus de reconnaissance régissent dans le système proposé. Le processus d'apprentissage ou d'enrôlement permettant de construire le modèle et d'avoir une base de donnée biométrique, le processus d'identification permettant de reconnaitre l'identité d'un individu, et enfin le processus de vérification permettant d'affirmer un client authentique ou de refuser un imposteur. Dans ce qui suit nous allons détailler ces trois processus.

6.6.1. Le processus d'apprentissage

L'apprentissage automatique est un des champs d'étude de l'intelligence artificielle. L'apprentissage automatique fait référence au développement, à l'analyse et à l'implémentation de méthodes qui permettent à une machine (au sens large) d'évoluer grâce a un processus d'apprentissage, et ainsi de remplir des taches qu'il est difficile ou impossible de remplir par des moyens algorithmiques plus classiques.

Nous avons donc opté pour l'apprentissage supervise basé sur l'extraction à partir de l'image binarisée à l'aide d'une base d'exemples permettant au programme de savoir a quoi

ressemble chaque caractéristique du trait biométrique (l'iris). Nous nous sommes servis d'une base d'images binarisées (instances).

Figure 6.3 : DFD Apprentissage.

Le diagramme de la figure 6.3 et de la figure 6.4 représente le processus d'apprentissage des images d'iris. Les codes calculés sont ensuite enregistré dans une base de données pour des éventuelles identifications/vérifications.

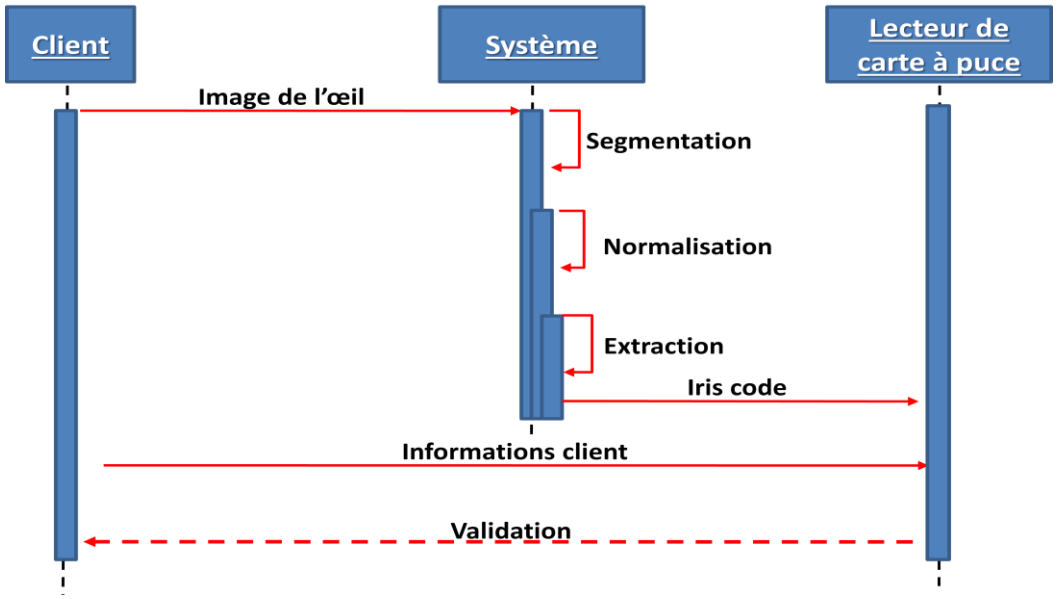


Figure 6.4 : Étapes du processus d'apprentissage

6.6.2. Le Processus d'identification

Le mode d'identification est un problème 1 à N, l'image à identifier est une image d'un individu qu'on ignore son identité (ie les informations comme le nom, le prénom, etc.). Le processus d'identification est une boucle de recherche par mesure de similarité sur la base de données. Les figures ci-dessous (figure 6.5, figure 6.6, figure 6.7 et figure 6.8) expliquent les flots de données du processus d'identification.

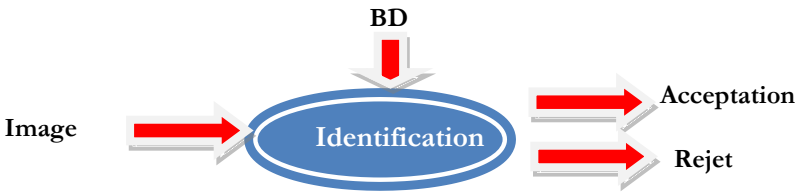


Figure 6.5 : DFD Identification (niveau 0).

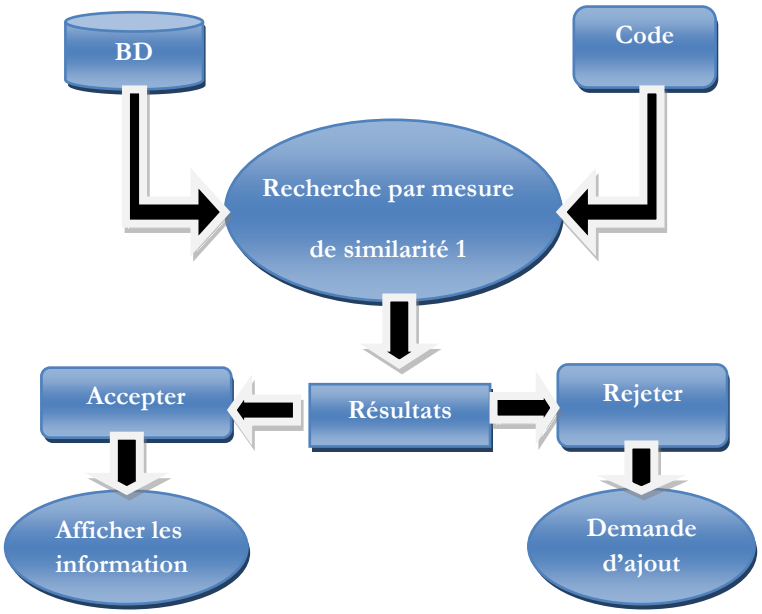


Figure 6.6 : DFD Identification (niveau 1).

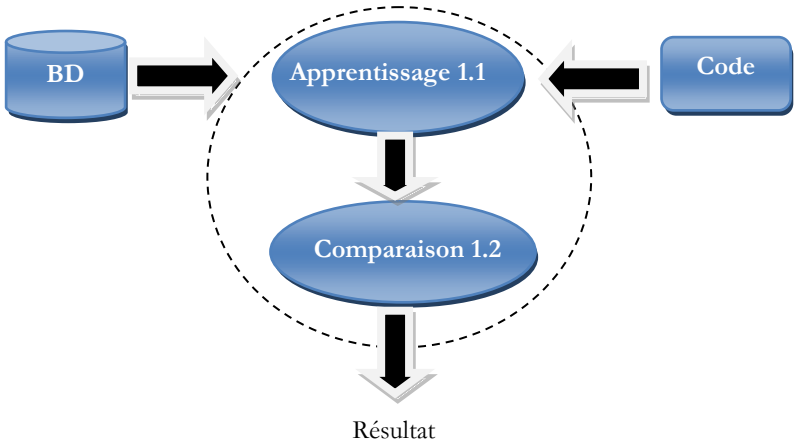


Figure 6.7 : DFD recherche de similarité (niveau 1)

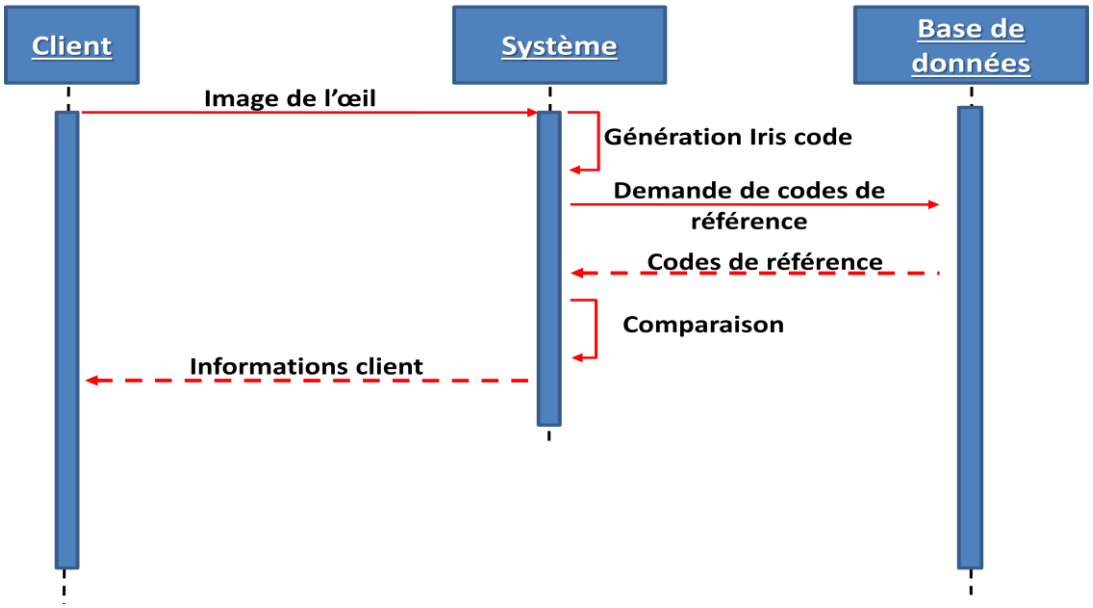


Figure 6.8 : Diagramme de séquence représentant le processus d'identification par l'iris

6.6.3. Le processus de vérification

Il comporte également deux phases : la phase d'apprentissage pendant laquelle les modèles sont construits de la même manière que pour le processus d'identification (devant être sauvegardés dans une carte de gabarit biométrique), et la phase de vérification (phase de comparaison au seuil). Cf. figure 6.9, figure 6.10 et figure 6.11.

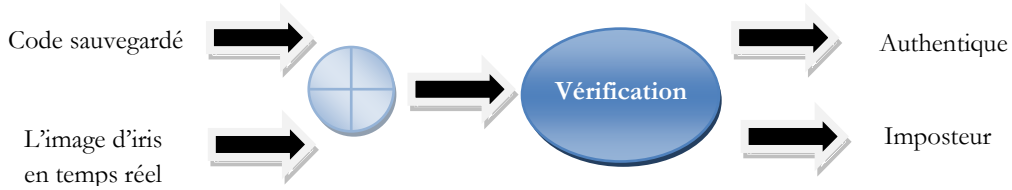


Figure 6.9 : DFD Vérification (niveau 0).

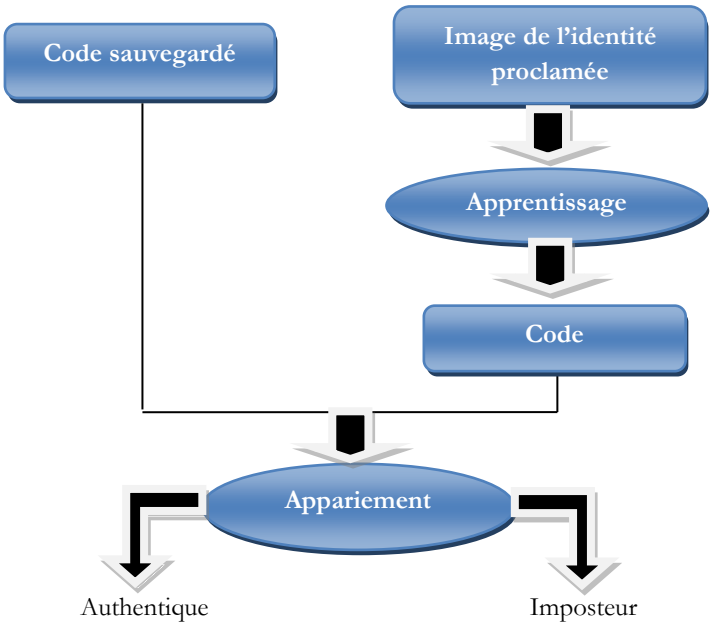


Figure 6.10 : DFD Vérification (niveau 1).

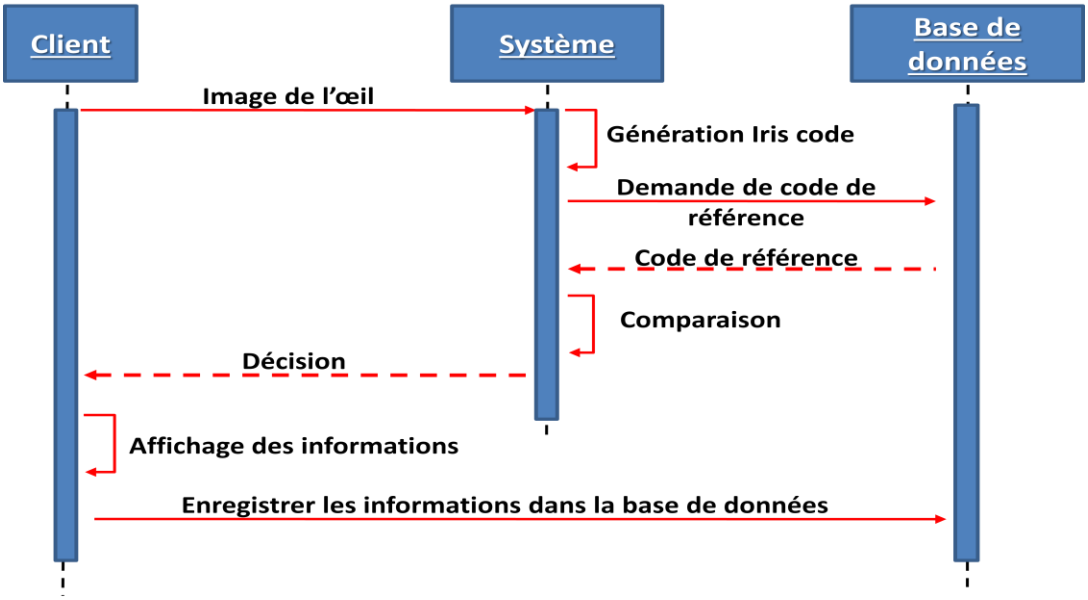


Figure 6.11 : Diagramme de séquence du processus de Vérification.

6.7. Analyse statistique de l'approche proposée

L'objectif principal de ces analyses statistiques est d'étudier les distributions des scores en sortie des modules de reconnaissance d'iris, afin de pouvoir les modéliser mathématiquement.

Dans le module de reconnaissance d'iris régissent deux algorithmes d'appariement, le premier à base de la distance *Hamming*, et le deuxième à base de la distance de *Euclidienne*. La décision se fait par un système d'inférence flou à base d'un ensemble de règle « si alors ».

Trois expériences ont été menées sur la base de données publique d'Iris CASIA-Iris V1. Cette base contient 756 images d'iris réparties sur 108 classes (la classe signifie l'individu). Chaque classe contenant 7 images d'iris prises sur deux sessions du même individu.

Expérience 1 :
Dans cette expérience l'appariement est réalisé selon la distance de *Hamming*.
Expérience 2 :
Dans cette expérience l'appariement est réalisé selon la distance *Euclidienne*.
Expérience 3 :
Dans cette expérience l'appariement est réalisé par la fusion des résultats des deux expériences précédentes en utilisant la fuzzification des scores et les règles floues citées au § 6.3.
Dans ce qui suit nous présentons des exemples de distributions intra-classes et inter classes de la reconnaissance monomodal d'iris en utilisant CASIA-Iris V1.

Tableau 6.1 : Exemple de distributions intra-classes et inter classes de l'expérience 1.

	Individu 1		
Individu 1	0.2957	0.2405	0.2581
	0.3248	0.2804	0.3227
Individu 2	0.4816	0.4783	0.4822
	0.4801	0.4772	0.4743
Individu 3	0.4783	0.4742	0.4795
	0.4850	0.4866	0.4759
Individu 4	0.4896	0.4866	0.4889
	0.4879	0.4901	0.4949
Individu 5	0.4855	0.4854	0.4877
	0.4776	0.4811	0.4781
Individu 6	0.4842	0.4924	0.4889
	0.4779	0.4752	0.4798

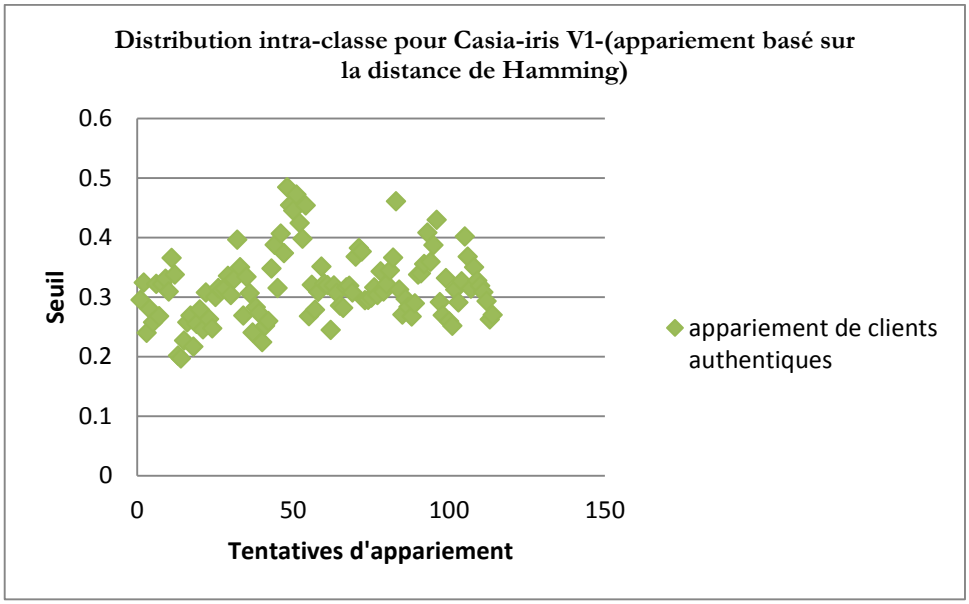


Figure 6.12 : Nuage de distribution intra-classe relatif à la reconnaissance monomodale d'iris en utilisant l'expérience 1 (CASIA-Iris V1 et la distance de *Hamming*).

On remarque que les appariements de clients authentiques enregistrent des distances d'appariement globalement inférieur à 0.45. Le seuil optimal est calculé selon la formule suivante :

$$Seuil\ optimal = \frac{\max(intraclasse) + \min(interclasse)}{2}$$

L'analyse des distributions interclasses de l'expérience 1 conclue que les appariements des imposteurs sont globalement supérieurs à la distance d'appariement 0.35 (Cf. Figure 6.13).

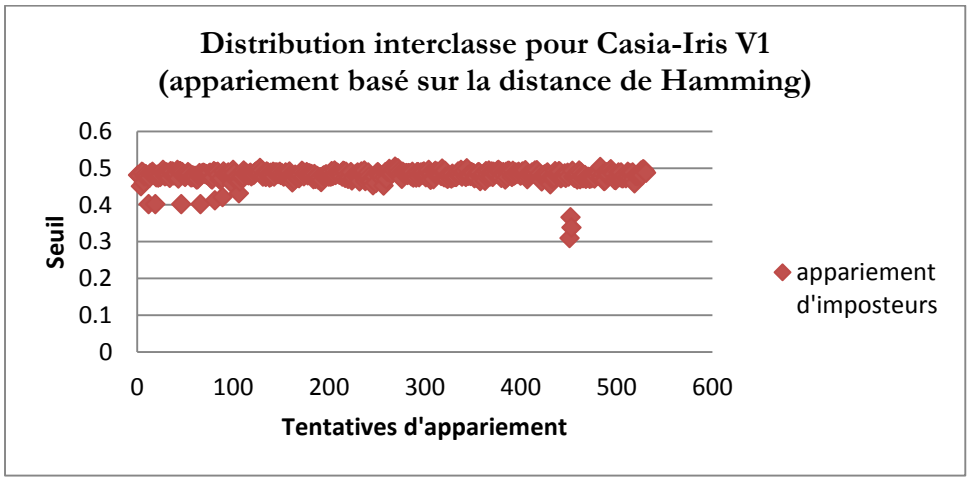


Figure 6.13 : Nuage de distribution interclasse relatif à la reconnaissance monomodale d'iris en utilisant l'expérience 1 (CASIA-Iris V1 et la distance de *Hamming).*

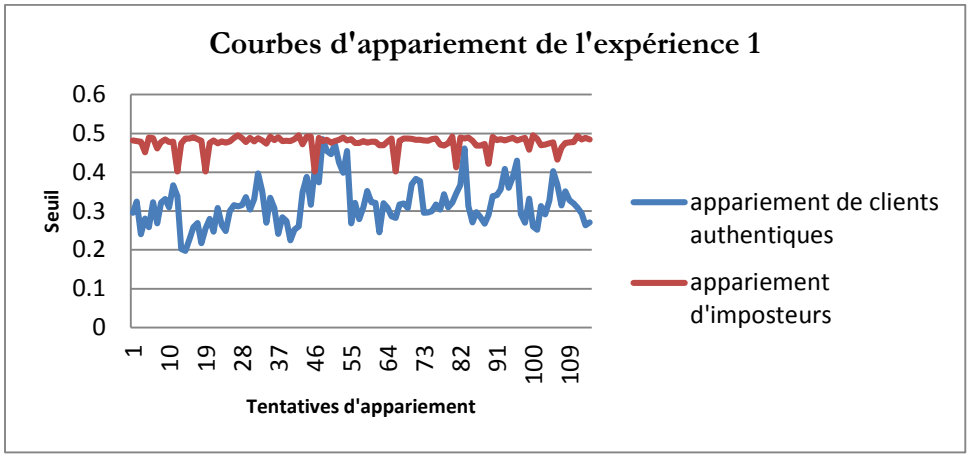


Figure 6.14 : Courbes d'appariements de clients authentiques et imposteurs relative à la reconnaissance monomodale d'iris en utilisant l'expérience 1 (CASIA-Iris V1 et la distance de *Hamming*).

La figure 6.14 présente les courbes d'appariement relatives à la reconnaissance d'iris par la distance de *Hamming* (expérience 1). On remarque que le seuil optimal menant au meilleur compromis entre les faux positifs et les faux négatifs est 0.35.

Pour valider ce seuil, nous avons calculé les taux de fausses acceptations et de faux rejets en variant le seuil de reconnaissance, les résultats sont présentés dans le tableau 6.2.

Le meilleur compromis entre les taux d'erreurs est 0% pour TFA et 5.181% pour le TFR, pour un seuil de décision égal à 0.35. Donc les scores dépassant ce seuil seront rejetés.

Tableau 6.2 : Estimation des taux TFA et TFR de la reconnaissance d'iris basée sur l'appariement par la distance de *Hamming*.

Seuil	0.20	0.25	0.30	0.35	0.40	0.45	0.50
TFA (%)	0.000	0.000	0.000	0.000	0.005	7.599	99.499
TFR (%)	99.047	82.787	37.880	5.181	0.238	0.000	0.000

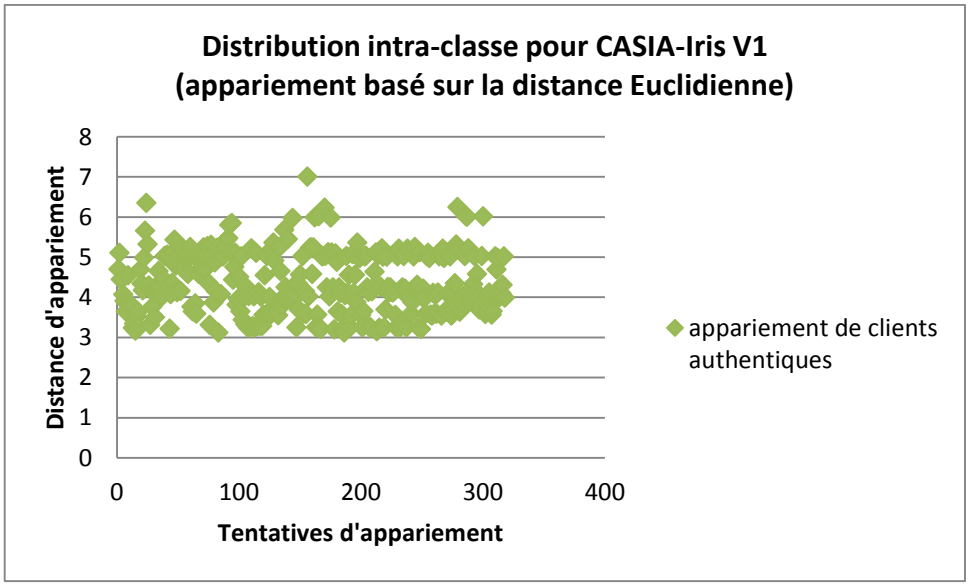


Figure 6.15 : Nuage de distribution intra-classe relatif à la reconnaissance monomodale d'iris en utilisant l'expérience 2 (CASIA-Iris V1 et la distance Euclidienne).

Selon l'expérience 2, menant des tests de reconnaissance d'iris sur CASIA-Iris V1 en utilisant un appariement basé sur la distance Euclidienne, les distributions intra-classe varient selon un intervalle de valeurs allant de 3 jusqu'à 6 (Cf. figure 6.15). Cet intervalle est plus large que celui de l'expérience 1.

Les appariements d'imposteurs varient également selon un intervalle de valeurs plus large que celui de l'expérience1. Les valeurs sont comprises entre 5 et 8.5 (Cf. figure 6.16).

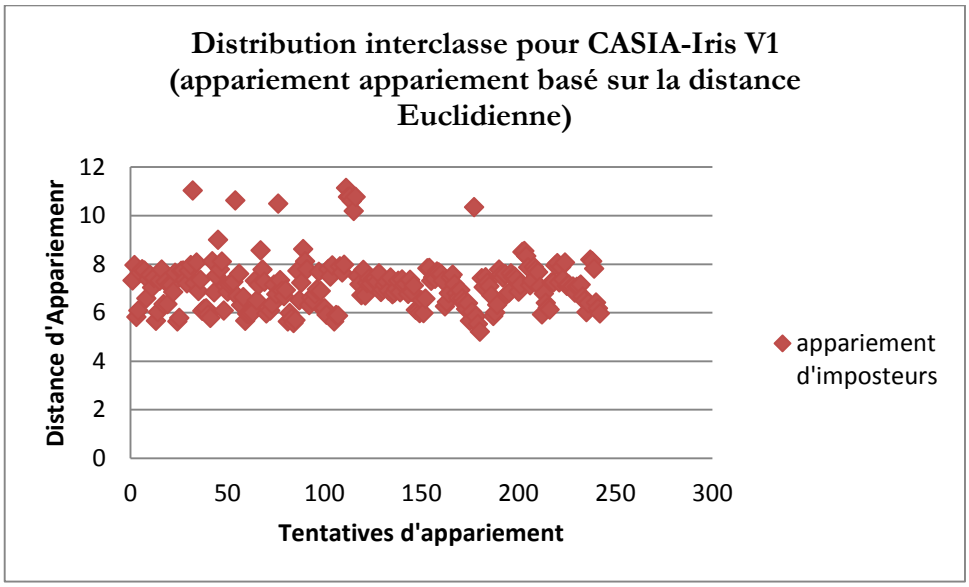


Figure 6.16 : Nuage de distribution interclasse relatif à la reconnaissance monomodale d'iris en utilisant (l'expérience 2 (CASIA-Iris V1 et la distance *Euclidienne*).

Pour valider un seuil de reconnaissance pour l'expérience 2, nous avons calculé les taux de fausses acceptations et de faux rejets en variant le seuil de reconnaissance, les résultats montrent qu'il n'est pas possible de déterminer un seul seuil optimal pour toute la base de données. La classification des images d'iris selon les seuils d'appariement correspondent à trois classes d'images d'iris avec qualité différente (Cf. tableau 6.3).

Tableau 6.3 : Classification de CASIA-Iris V1 selon le critère de la qualité d'image.

Classe 1	Classe 2	Classe 3
Images de bonne qualité	Images de qualité moyenne	Images de mauvaise qualité
391/756	292/756	73/756

- La première classe répertorie les images d'iris de bonne qualité, 391 images de CASIA-Iris V1. L'analyse statistique des distributions de clients authentiques de cette classe montre que les distances d'appariement calculées en utilisant ces images sont situées autour de l'intervalle des seuils [5, 5.5].
- La deuxième classe répertorie les images d'iris de qualité moyenne, 292 images de CASIA-Iris-V1. L'analyse statistique des distributions de clients authentiques de cette classe montre que les distances d'appariement calculées en utilisant ces images sont situées autour de l'intervalle des seuils [6, 6.5].

- La troisième classe répertorie les images d'iris de mauvaise qualité, 73 images de CASIA-Iris-V1. L'analyse statistique des distributions de clients authentiques de cette classe montre que les distances d'appariement calculées en utilisant ces images sont situées autour de l'intervalle des seuils [7.5, 7.8].

Figure 6.17 présente les fonctions d'appartenance aux trois ensembles flous de forme trapézoïdale modélisant les variables linguistiques floue (*Bonne*, *Moyenne* et *Mauvaise*).

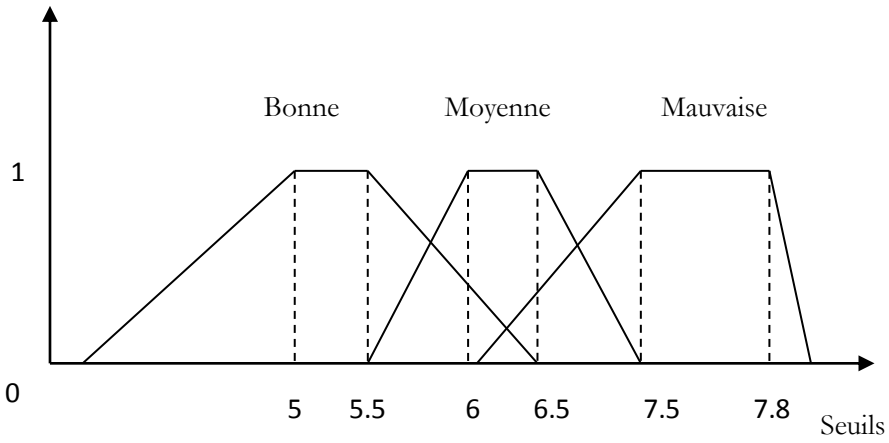


Figure 6.17 : Fonctions d'appartenance aux ensembles floues modélisant les trois classes de CASIA-Iris V1.

[5,5.5] intervalle des images appartenant à l'ensemble flou «Bonne».

[6,6.5] intervalle des images appartenant à l'ensemble flou «Moyenne».

[7.5,7.8] intervalle des images appartenant à l'ensemble flou «Mauvaise».

La classification des images d'iris selon l'analyse statistique des distances d'appariement correspond à la classification visuelle de ces images selon la quantité de bruit présent dans l'image. Le bruit se présente sous différentes formes (Cf. tableau 6.4) :

- Le flou : l'image d'iris présente un caractère flou visible à l'œil.
- La distorsion causée par le bord de l'œil.
- La distorsion causée par les cils.
- La lumière apparente.
- Des pigments noirs.
- L'ombre.

Tableau 6.4 : Exemple montrant l'identification d'images d'iris appartenant à la classe 3 (images de mauvaises qualité)

reference d'image	Type de bruit							Seuil	Identification
	Flou	Distorsion de bord de l'œil	Distorsion de cils	Lumière	Off angle	Ombre			
007-1-3	+	+	+	+	-	-		5.94	Réussie
010-1-2	+	+	+	+	-	-		3.26	Réussie
019-1-1	+	+	+	+	-	-		5.88	Réussie
041-2-2	-	+	+	+	-	-		6.12	Réussie
043-1-1	+	+	+	+	-	+		6.53	Réussie
053-2-1	+	+	+	+	+	+		7.11	Réussie
062-2-2	+	-	-	+	+	-		4.64	Réussie
065-1-1	+	+	+	-	-	+		5.51	Réussie

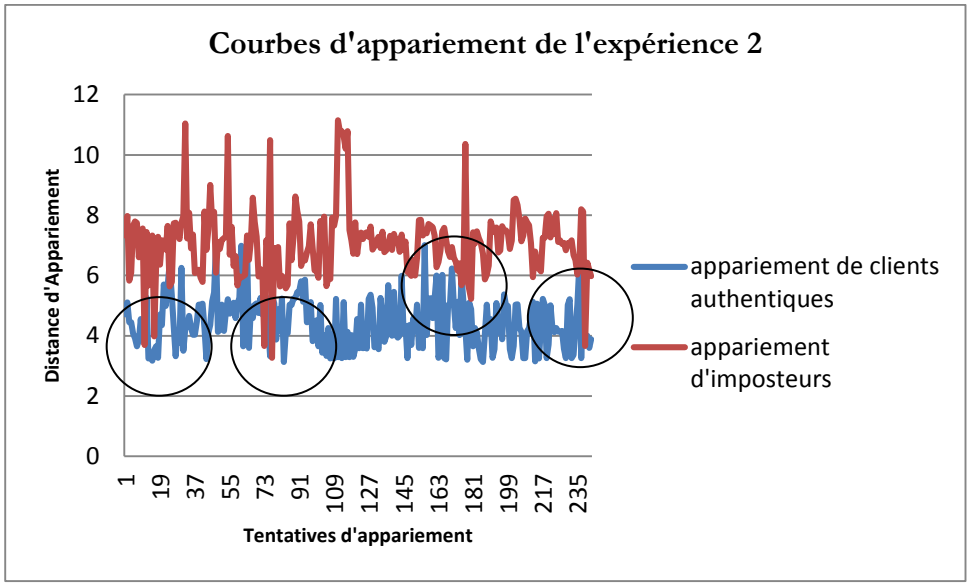


Figure 6.18 : Courbes d'appariement interclasse et intra-classe pour CASIA-Iris V1 (appariement basé sur la distance Euclidienne).

En analysant les courbes d'appariement de l'expérience 2 (basée sur la distance Euclidienne) Cf. Figure 6.18, on remarque que :

- Les seuils relatifs aux appariements authentiques sont très chevauchés avec les seuils relatifs aux appariements d'imposteurs. De ce fait,
- Les zones de recouvrement entre les deux scores sont nombreuses en les comparant avec les zones de recouvrement des deux scores de l'expérience 1, sui sont minimes.

De ce fait, un seul seuil de décision pour toute la base n'est pas la solution adéquate pour avoir un bon compromis entre le TFA et le TFR.

La solution envisagée est de partager la base de données en trois classes selon les scores des clients authentiques et imposteurs rapprochés.

Les tableaux 6.5, 6.6 et 6.7 donnent une estimation des taux TFA et TFR de la reconnaissance d'iris basée sur l'appariement par la distance euclidienne :

Tableau 6.5 : TFA et TFR de l'expérience 2 avec les images de la classe 1.

	3.5	4.5	5	5.5	6	6.4
TFA (%)	0.00	0.00	**0.00**	**1.14**	17.81	60.65
TFR (%)	86.11	30.11	**0.46**	**0.23**	0.00	0.00

Tableau 6.6 : TFA et TFR de l'expérience 2 avec les images de la classe 2.

	5.25	45.75	6	6.5	7	7.5
TFA (%)	0.00	0.00	**0.04**	**7.44**	44.561	66.31
TFR (%)	69.44	25.55	**1.44**	**0.69**	0.01	0.00

Tableau 6.7 : TFA et TFR de l'expérience 2 avec les images de la classe 3.

	6	6.50	7.50	7.80	8.20
TFA (%)	0.00	0.00	**15.14**	**88.22**	95.31
TFR (%)	60.23	43.33	**5.88**	**0.11**	0.01

6.8. Résultats

6.8.1. Résultats en termes de temps d'exécution par phase

Les tests ont été conduits sur un ordinateur pc portable doté d'un processeur ayant une vitesse de 3.6 GHz et 512 Méga-octet de mémoire vive.

Nous présentons dans le tableau 6.8 l'estimation du temps d'exécution de l'application par phase de traitement, à savoir : la phase de segmentation, la phase de normalisation, et la phase du codage.

Tableau 6.8 : Estimation du temps d'exécution par phase du traitement d'extraction de caractéristique.

	Phase	
Base de données	Segmentation (s)	Normalisation et codage (s)
CASIA V.1	**20.34**	**0.186**

Le tableau 6.9 présente l'estimation du temps d'exécution selon le type d'appariement, soit la vérification (appariement 1 à 1), ou bien l'identification (appariement 1 à n).

Tableau 6.9 : Estimation du temps d'exécution selon le type d'appariement.

	Phase			
Base de données	Vérification (s)		Identification (s)	
	Hamming	Euclidienne	Hamming	Euclidienne
CASIA-Iris V.1	0.148711	0.000559	23.75698	9.343245

On remarque que l'appariement par la distance *Euclidienne* est beaucoup plus rapide que l'appariement à base de la distance de *Hamming*.

6.8.2. Résultats en termes de Taux d'erreurs TFA, TFR et TEE

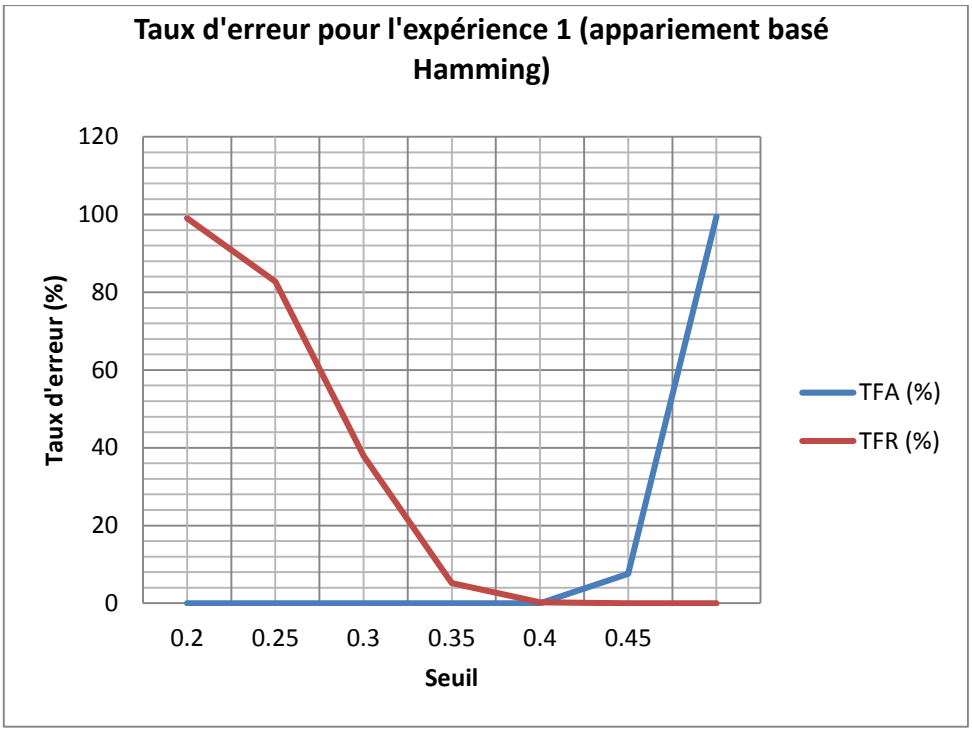


Figure 6.19 : Courbe ROC des taux d'erreurs (TFA et TFR) relative à la reconnaissance d'iris basée sur l'appariement par la distance de *Hamming*

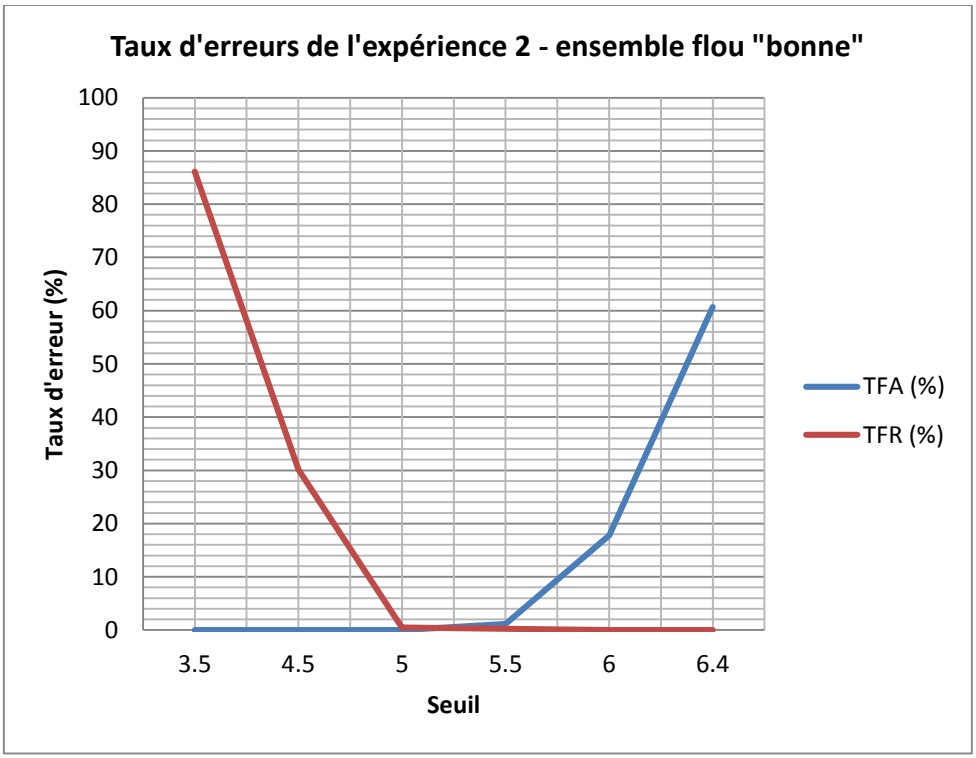


Figure 6.20 : Courbe ROC des taux d'erreurs (TFA et TFR) relative à la reconnaissance d'iris basée sur l'appariement par la distance *Euclidienne* (seulement pour les images appartenant à l'ensemble flou « bonne »)

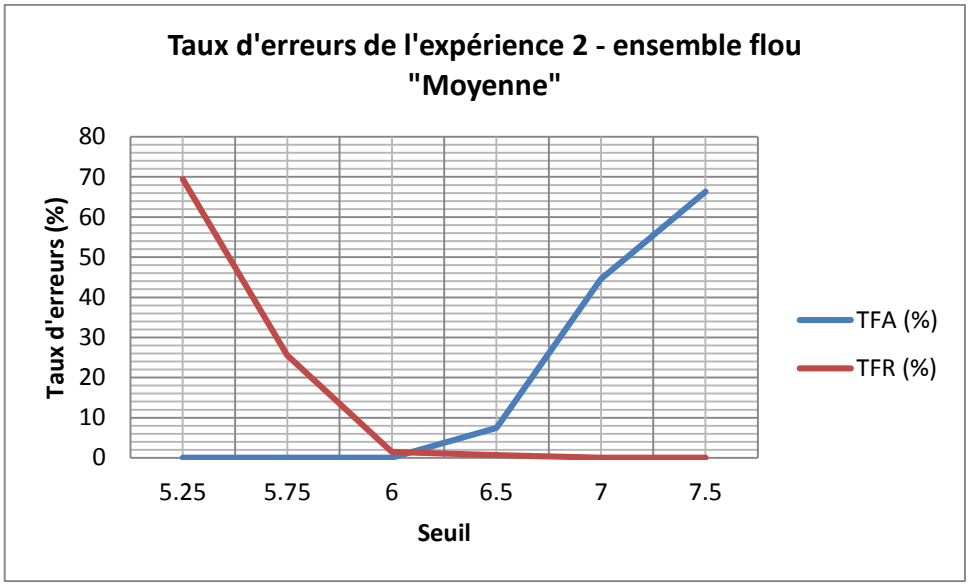


Figure 6.21 : Courbe ROC des taux d'erreurs (TFA et TFR) relatives à la reconnaissance d'iris basée sur l'appariement par la distance *Euclidienne* (seulement pour les images appartenant à l'ensemble flou « Moyenne »)

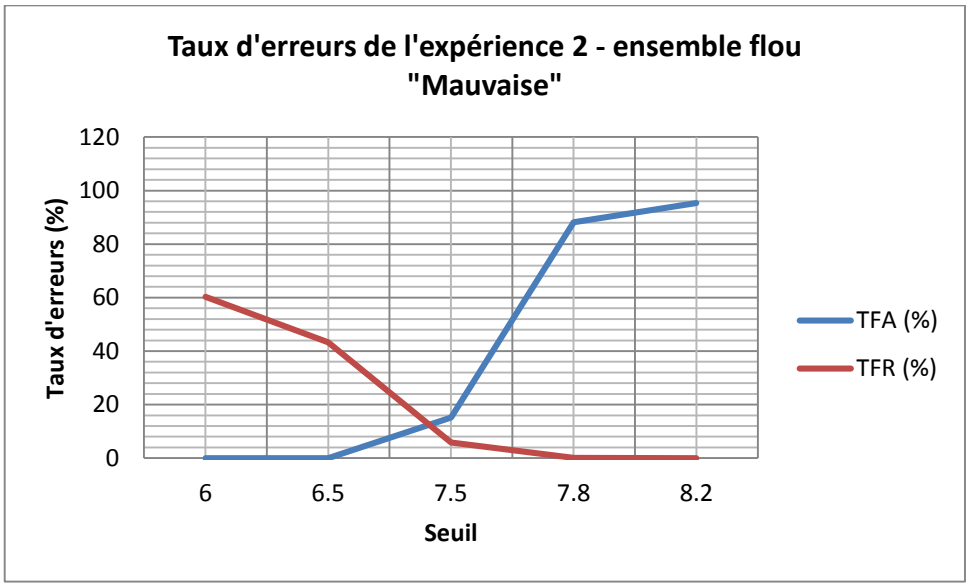


Figure 6.22 : Courbe ROC des taux d'erreurs (TFA et TFR) de l'expérience 2, relatives à la reconnaissance d'iris basée sur l'appariement par la distance *Euclidienne* (seulement pour les images appartenant à l'ensemble flou « Mauvaise »)

Il est important de noter que Les distributions des scores varient d'un utilisateur à un autre (variation interclasse) et varient aussi au sein de chaque utilisateur (variation intra-classe). On cherche toujours à

- maximiser la variation interclasse.
- minimiser la variation intra-classe.

La variation interclasse est causée par le fait qu'un système biométrique construit un modèle de référence dédié pour chaque utilisateur. Maximiser cette variation revient à construire le model ou la référence la plus optimale pour chaque utilisateur.

Le tableau 6.10 présente un résumé des taux d'erreurs calculés pour toutes les expériences menées sur la base de données CASIA-Iris V1.

Il est important de noter que la comparaison se fait selon le Taux d'Erreur Egal TEE, qui est les point d'intersection des deux courbes représentant les taux d'erreurs TFA et TFR.

Tableau 6.10 : Résumé des taux d'erreurs calculés pour chaque expérience.

		TFA (%)	TFR (%)	TEE (%)
Expérience 1 : reconnaissance d'iris avec *Hamming*		0.5	23.8	2.5
Expérience 2 : reconnaissance d'iris avec *Euclidienne*	Classe « bonne »	0	46	0.39
	Classe « Moyenne »	4	144	1.25
	Classe « Mauvaise »	1514	588	8
Expérience 3: fusion hamming *Euclidienne*	Classe « Bonne »	0	0.1	**0.28**
	Classe « Moyenne »	0.05	0.21	0.96
	Classe « Mauvaise »	0.5	12.5	2

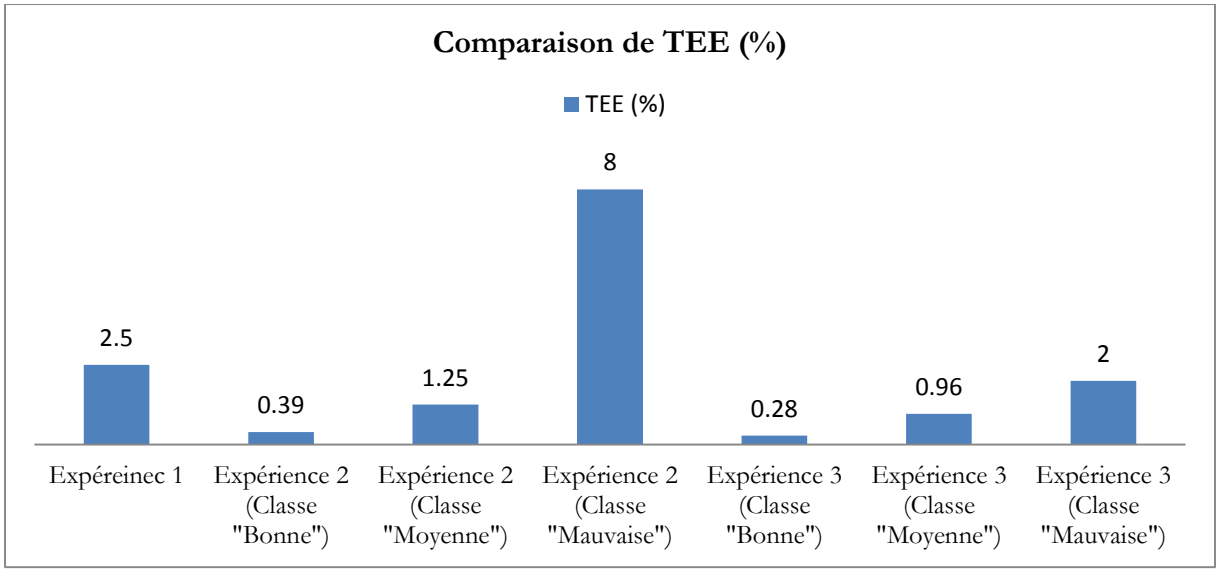


Figure 6.23 : Comparaison de TEE des expériences appliquées.

Analyse :

- L'expérience 1 sert de référence.
- Le meilleur TEE est celui de l'expérience 3, ou l'appariement a été appliqué en réalisant la fusion des décisions sur l'ensemble d'images d'iris appartenant à l'ensemble flou « bonne », suivi de celui de l'expérience 2, ou l'appariement a été appliqué sur l'ensemble d'images appartenant à l'ensemble flou « Bonne ».
- Le TEE de l'expérience 2 est acceptable, seulement lorsque les images appartiennent à la classe 3 (Mauvaise).

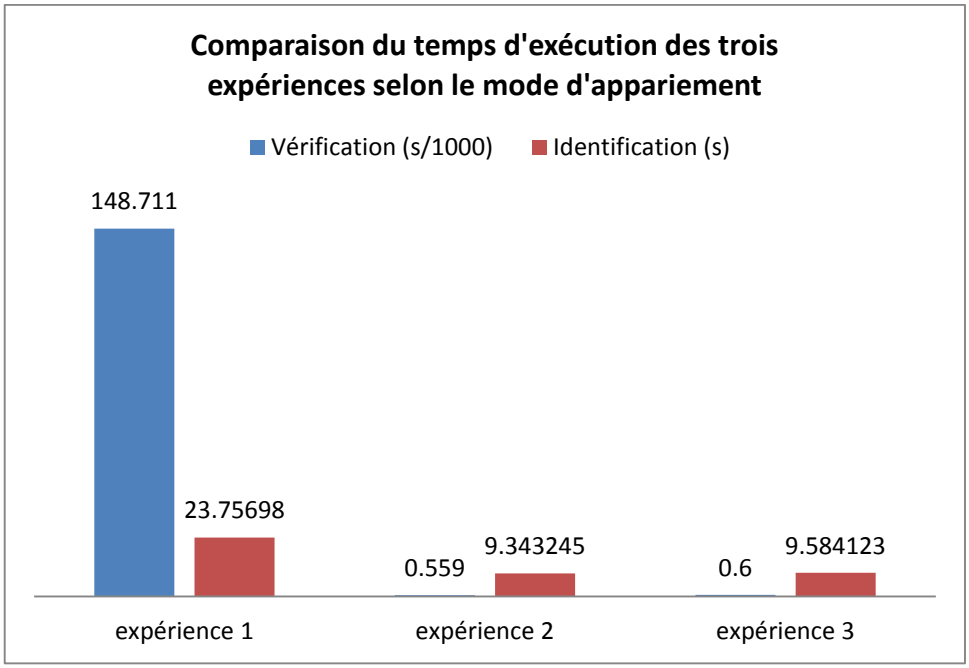


Figure 6.24 : Comparaison de temps d'exécution des expériences appliquées.

La figure 6.24 présente la comparaison des temps d'exécution calculés pour chaque expérience. Deux modes opératoires sont utilisés : le mode de vérification et le mode d'identification.

On remarque que les deux expériences 2 et 3, où la distance *Euclidienne* a été utilisée pour comparer les codes d'iris, sont les meilleurs en les comparants avec l'expérience 1, où la distance de *Hamming* a été utilisée dans l'appariement.

Discussion

Pour commencer, on a constaté que le temps d'exécution estimé pour la segmentation égale à 20.34 s, était long et important par rapport au temps d'exécution total qui est de 23.75 s (en mode identification), ce qui présente 85.64% de ce dernier.

Encore en terme de temps d'exécution on à pu voir que la distance *Euclidienne* est plus rapide que la distance de *Hamming*, avec respectivement 9.43 s et 23.75 s, donc 2.5 fois la distance euclidienne est plus rapide que la distance de *Hamming*. De ce fait, le gain de temps de réponse de la phase d'identification apporté par la distance *Euclidienne* est 60%.

Nous avons remarqué que les distances de *Hamming* et les distances *Euclidiennes* intra classe ne sont pas nulles. Ceci dû principalement aux conditions d'acquisitions d'images, elles ne sont pas toujours les même, ainsi aux bruits présents dans les images et notamment aux éventuels erreurs de segmentation.

On remarque également que les résultats obtenus des distances *Euclidiennes* étaient améliorés grâce à la logique floue, en effet, la séparation des données en plusieurs classes et l'application d'un seuil adéquat pour chaque classe améliore les taux d'erreurs.

En fin, on constate que, la classification floue, impliquant la séparation des données en plusieurs classes avec des degrés d'appartenance, permet de réduire la taille de la base de recherche et donc d'accélérer le processus.

6.9. Conclusion

En suivant un protocole de test et d'évaluation très précis, nous avons d'abord exploré une méthode de fusion inspirée de concepts de la logique floue, en particulier la fusion de décisions de reconnaissance biométrique, considérées comme des variables linguistiques floues, par un système d'inférence floue.

Cette méthode a donné des résultats prometteurs et a permis de nous orienter vers une méthode de fusion unidimensionnelle, plus rapide et plus facile à formaliser théoriquement. Cette technique de fusion, a montré à travers une étude comparative complète, qu'elle pouvait fournir d'excellents résultats en termes de taux d'erreur égal (EER), de taux Fausses Acceptation (TFA), de Taux de Faux Rejet (TFR), et de temps d'exécution.

Notons que pour pouvoir appliquer cette technique, il est important de faire des analyses statistiques préliminaires afin de vérifier l'allure des distributions des scores imposteurs pour une modalité donnée.

En perspectives, notre méthode peut parfaitement prendre en compte plusieurs modalités afin de tenter d'augmenter encore plus la sécurité d'un système biométrique multimodal.

Chapitre 7

FUSION D'EMPREINTES AU NIVEAU CARACTÉRISTIQUE

7.1. Introduction

Les systèmes biométriques qui intègrent l'information à une étape en amont du traitement sont censés être plus efficaces que les systèmes qui opèrent une fusion à un niveau plus abstrait. Puisque les caractéristiques issues d'une entrée biométrique sont supposées contenir une information plus riche qu'un score de correspondance ou la décision d'un matcher (module de reconnaissance) biométrique, la fusion au niveau caractéristiques devrait fournir de meilleurs résultats de reconnaissance que les autres niveaux d'intégration. Cependant, la fusion au niveau *caractéristique* est difficile à atteindre en pratique à cause des raisons suivantes :

1. La relation entre les espaces de caractéristiques ("*feature spaces*") de différents systèmes biométriques n'est pas forcément connue. Dans le cas ou la relation est connue par avance, on doit prendre soin d'éliminer les caractéristiques qui sont fortement corrélées. Cela requiert l'application d'algorithmes de sélection de caractéristiques avant l'étape de classification.

2. La concaténation de deux vecteurs de caractéristiques peut engendrer un vecteur de caractéristiques ayant une grande dimension, menant au fameux problème de la "malédiction de la dimensionnalité". Bien que ce soit un problème général dans la plupart des applications de reconnaissance de forme, cela est encore plus marquant dans les applications biométriques à cause du temps, de l'effort et du coût impliqués dans la collecte de grandes quantités de données biométriques,

3. La plupart des systèmes biométriques commerciaux ne fournissent pas l'accès aux vecteurs de caractéristiques qui sont utilisés dans leurs produits. Ainsi, très peu de chercheurs ont étudié la fusion au niveau *caractéristique* et la plupart d'entre eux se tournent généralement vers les schémas de fusion après le *matching*.

7.2. Objectifs et motivations

L'objectif principal de ce travail est la proposition d'un nouvel algorithme de reconnaissance par empreinte digitale assurant l'identification par instances répétées (plusieurs impressions du même doigt) et multiples (plusieurs doigts) d'empreintes digitales. La fusion est établie au niveau *caractéristique* (*Feature level*).

Motivations:

1. Surmonter les limites de la monomodalité biométrique en proposant une solution de multimodalité biométrique par utilisation d'instances répétées et multiples du même trait biométrique (l'empreinte).
2. Choisir de combiner les informations biométriques provenant d'instances répétées et/ou multiples au niveau *Caractéristique* engendre un ensemble de caractéristique (*feature set*) plus riche en information biométrique que d'utiliser la fusion au niveau *Score* ou bien au niveau de *Décision*.
3. Choisir le niveau de *caractéristique* pour faire la fusion assure la détection des points de caractéristiques biométriques redondants qui seront supprimés avant l'appariement. Cet avantage n'est pas offert par la fusion au niveau *Score* ou bien au niveau de *Décision*.
4. Choisir la fusion au niveau *Caractéristique* est idéal quand les codes à fusionner sont homogènes (dans notre cas les codes sont tous des codes d'impressions d'empreinte).

Objectifs :

1. Arriver à un meilleur compromis entre le taux de fasse acceptation TFA et le taux de faux rejet TFR par rapport aux travaux de recherche sur l'identification par l'empreinte.
2. Etudier les distributions de clients authentiques et d'imposteurs sur une large base de données d'empreinte afin de déterminer l'influence du matcher en terme de séparabilité des distributions.
3. Voir l'influence de paramètres sur les algorithmes implémentés.
4. Voir le résultat de l'algorithme proposé lors de son application sur des images d'empreinte de mauvaise qualité, pour cette raison nous avons choisi la base de donnée d'empreintes digitales FVC 2000 présentant des empreintes de mauvaise qualité dans les ensembles FVC 2000-DB2 et FVC 2000-DB3.
5. Proposer une solution au problème de l'explosion combinatoire lié à l'utilisation d'instances répétées et multiples du trait biométrique.
6. Mesurer la *Spécificité* et la *Sensibilité* de l'algorithme proposé en utilisant une instance, trois instances puis huit instances de l'empreinte digitale, et en déduire à propos de la meilleure combinaison. Le critère de la *Spécificité* (*Specificity*) mesure la pertinence du système à éviter les fausses détections, le critère de la *Sensibilité* (*Sensitivity*) mesure la pertinence du système à détecter les vraies minuties.

7.3. Formulation du problème

Les méthodes de traitement des empreintes digitales sont divisées en trois catégories :

1. Méthodes à base de texture.
2. Méthodes à base d'apparence .
3. Méthodes à bases de minuties.

Notre travail entre dans le cadre des méthodes de traitement d'empreinte à base d'extraction de minuties. Ces méthodes sont les plus utilisés par les travaux de recherche pour leur simplicité d'implémentation et efficacité d'algorithmes, leurs seul limitation est la qualité de l'image d'empreinte, qui, lorsqu'elle est mauvaise, le système sera incapable de produire un résultat, et marque l'erreur d'impossibilité d'enrôlement ou l'erreur d'impossibilité d'appariement (« *failure to enroll* » ou « *failure to match* »).

Pour éviter ces types d'erreur, nous adoptons l'idée de Jagadeesan et al [Jagadeesan, 2010], proposons de calculer la région d'intérêt et le flux d'orientation avant de passer au traitement.

La fusion d'empreinte avec d'autres modalités est très fréquente en biométrie, d'une part pour augmenter la fiabilité de la reconnaissance, et d'autre part, pour luter contre la fraude et la falsification. Les tentatives de *Kumar et al.* [Kumar et al., 2003] qui ont combiné des caractéristiques de l'empreinte palmaire et de la géométrie de la main d'une part, et *Ross et Govindarajan* [Ross & Govindarajan, 2005] qui ont combiné des caractéristiques du visage avec celles de la géométrie de la main d'autre part, n'ont rencontré qu'un succès limité.

L'idée de combiner plusieurs instances ou impressions par doigt a été adressée par plusieurs chercheurs et groupes de recherche [Jain et Prabhakar, 2002], [Giacinto et al, 2005], [Sha et al, 2007], [Ren et al, 2009], [Mane et al, 2011].

Quand les vecteurs de caractéristiques sont **homogènes** (par exemple, plusieurs images d'empreinte digitale du doigt d'un utilisateur), un unique vecteur de caractéristiques résultant peut être calculé comme une somme pondérée des vecteurs de caractéristiques individuels.

Lorsque les vecteurs de caractéristiques sont **hétérogènes** (par exemple, des vecteurs de caractéristiques de différentes modalités biométriques comme le visage et la géométrie de la main), nous pouvons les concaténer pour former un seul vecteur de caractéristiques.

Cependant, la concaténation n'est pas possible lorsque les ensembles de caractéristiques sont incompatibles. Par exemple, les minuties d'empreintes digitales et les coefficients de visage issus du PCA ("*eigen-face coefficients*").

Notre but principal est de trouver une solution simple, rapide et précise concernant la reconnaissance par empreintes digitales lorsque celles-ci sont de qualité détériorée.

Notre travail repose sur deux algorithmes de la littérature actuelle, le premier est celui de Jagadeesan et al [Jagadeesan, 2010] utilisé dans l'étape du prétraitement, et consistant à calculer la région d'intérêt et le flux d'orientation, le deuxième est celui de Jain et al [Jain et al, 1997] utilisé dans l'étape d'extraction des minuties, cet algorithme est la référence de base de la méthode d'extraction de minuties à partir de l'empreinte.

7.4. Facteurs pour déterminer la qualité de l'empreinte

La qualité de la biométrie est affectée par le dispositif de capture. Plusieurs travaux récents ont adressé le problème posé par la détérioration de la qualité de la biométrie. [Alonso-Fernandez et al., 2008], [Alonso-Fernandez et al.,, 2010], [Galbally et al., 2012] [Alonso-Fernandez et al., 2012], [Galbally et al., 2014]. Dans ce paragraphe, nous présentons un résumé des facteurs principaux déterminant la qualité de l'empreinte :

1. Qualité des crêtes et clarté des crêtes

La qualité et la clarté des crêtes sont souvent améliorées par l'algorithme de traitement d'empreintes digitales (Cf. Figure 7.1).

(a) Crêtes claires **(b) crêtes non claires**

Figure 7.1 : La qualité et la clarté des crêtes.

2. La dimension de l'image capturée

La dimension de l'image capturée peut affecter le processus de reconnaissance surtout si l'image capturée est

Dimension 1 **Dimension 2**

Figure 7.2 : Différentes dimensions de l'image d'empreinte.

3. La position de l'image capturée

Une mauvaise position signifie un bas nombre confident de minuties, la région capturée n'est pas incluse dans la région d'intérêt. Ces images présentent l'impossibilité d'enrôlement et d'appariement (Cf. Figure 7.3).

Mauvaise position **Bonne position**

Figure 7.3 : Différentes positions des empreintes.

4. La qualité et la quantité des caractéristiques d'appariement (les minuties)

Pour caractériser une empreinte digitale, il faut un ensemble suffisant et fiable de minuties. Le nombre suffisant nécessaire de minuties pour pouvoir établir des comparaisons entre différentes empreintes est de 12 ou 14 minuties, mais avec entre 15 et 20 minuties on peut réussir à cibler une empreinte digitale parmi plusieurs millions d'exemplaires (Cf. Figure 7.4).

Figure 7.4 : Empreinte avec 12 minuties.

5. L'orientation de l'image

Orientation 1 **Orientation 2**

Figure 7.5 : L'orientation des crêtes.

L'algorithme de détection de minuties doit prendre en compte l'orientation des crêtes dans l'image d'empreinte. Donc, une minutie est repérée par ses deux coordonnées et son orientation.

6. La distorsion de l'image

Les images biométriques détériorées présentent un sérieux problème. Dans la majorité des cas ces images sont supprimées de la base ou remplacées par d'autres captures de bonne qualité.

Figure 7.6 : Exemples d'images d'empreintes détériorées.

7. Solutions envisagées

- Stockage de multiples instances du même trait biométrique (vue multiples, impressions multiples etc.) représentant la variabilité de ce trait.
- Mise à jour des instances dégradées et remplacement des images détériorées par de bonnes captures.
- Utilisation de plusieurs algorithmes d'appariement.
- Utilisation des algorithmes de fusion.
- Etude d'indication quantitative relative à la décision de la reconnaissance (comme par exemple l'étude des mesures de la *Sensibilité* et de la *Spécificité*).
- Sélection d'images à base leurs qualité pour être utiliser dans l'appariement ou dans la fusion.
- Utilisation d'autres traits biométriques (*Soft biometric traits*) comme l'âge, la taille, le poids, le sexe pour assister à la reconnaissance.

7.5. Schéma général du système

Avant de traiter l'image, le flux d'orientation est calculé et la région d'intérêt est localisée. Pour segmenter les crêtes, une fenêtre 16 x 16 orientée au long de la direction de la crête est positionnée autour de chaque pixel. La projection au long de la direction des crêtes est calculée. Les centres des crêtes apparaissent comme des pics sur l'onde de projection.

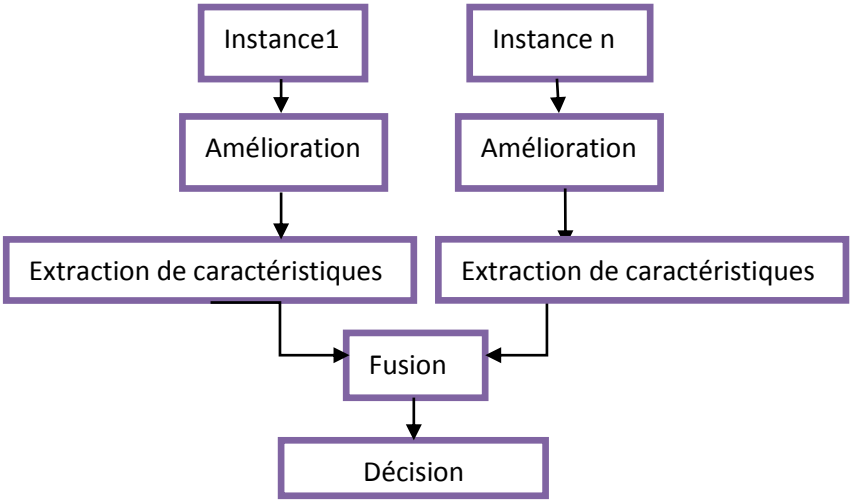


Figure 7.7 : Architecture du système de reconnaissance par empreinte à base de fusion d'impressions multiples au niveau caractéristique.

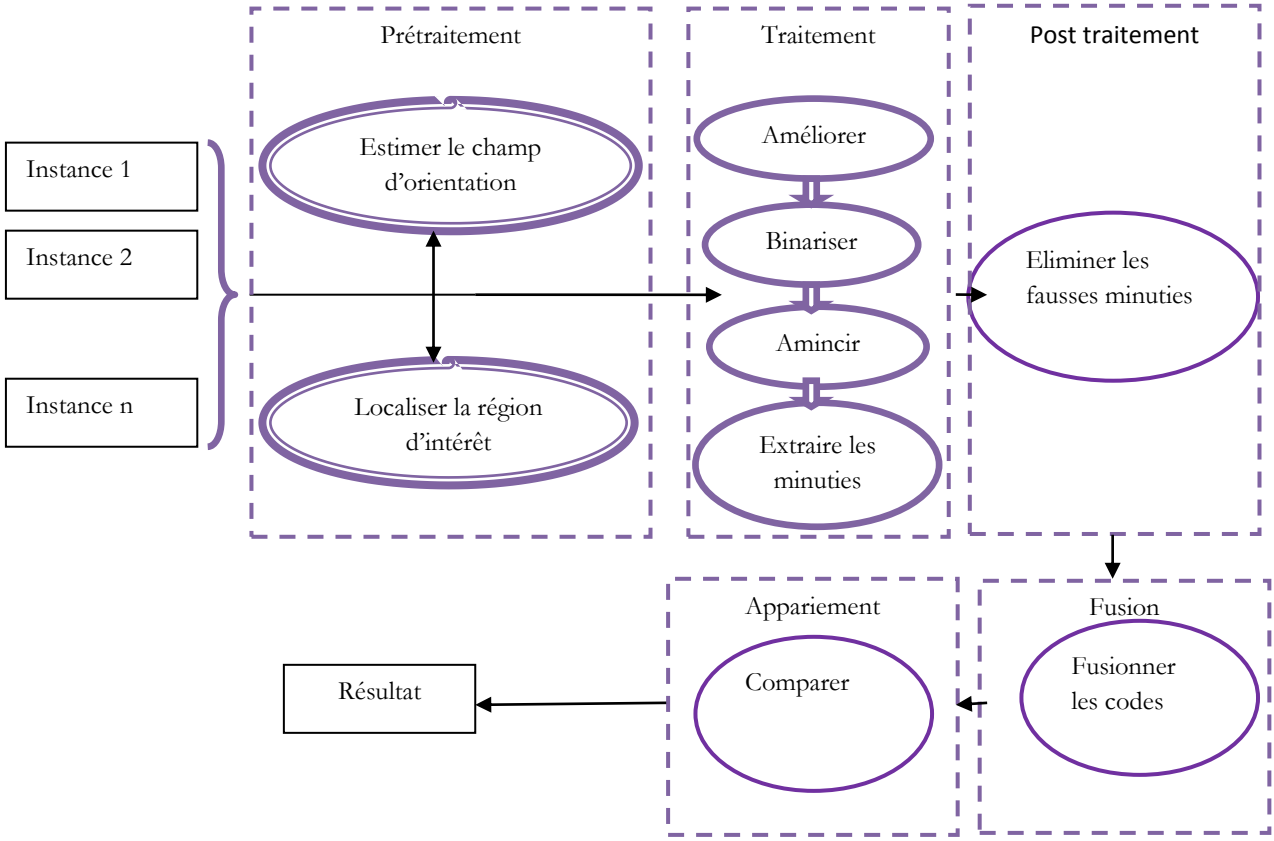


Figure 7.8 : Schéma général du système de reconnaissance d'empreinte par fusion d'impressions multiples au niveau caractéristique.

Notre contribution réside dans la proposition

1. D'un nouvel algorithme de fusion des vecteurs de caractéristiques d'empreintes digitale

Quand les vecteurs de caractéristiques sont **homogènes** (par exemple, plusieurs images d'empreinte digitale du doigt d'un utilisateur), un unique vecteur de caractéristiques résultant peut être calculé comme une somme pondérée des vecteurs de caractéristiques individuels.
Lorsque les vecteurs de caractéristiques sont **hétérogènes** (par exemple, des vecteurs de caractéristiques de différents doigts), nous pouvons les concaténer pour former un seul vecteur de caractéristiques.
Cependant, la concaténation n'est pas possible lorsque les ensembles de caractéristiques sont incompatibles.

2. D'un nouvel algorithme d'appariement basé sur La concaténation des codes générés par les instances multiples d'empreinte digitales et son utilisation dans la phase de comparaison.

Le principe est de comparer l'empreinte du client avec trois/huit instances du même doigt, on suppose que le client est accepté si et seulement si la somme des résultats de reconnaissance (matching) est supérieure ou égale à 2 (pour trois instances) et supérieure ou égale à 4 (pour huit instances) sinon le client est rejeté. Le tableau suivant présente notre logique d'appariement pour trois instances d'empreinte.

Tableau 7.1 : Logique d'appariement proposée pour trois instances d'empreinte.

Le code d'empreinte	Instance 1	Instance 2	Instance 3	résultat
	1	1	1	1
	1	1	0	1
	1	0	1	1
	0	1	1	1
	0	0	1	0
	0	1	0	0
	1	0	0	0
	0	0	0	0

7.6. Les processus de reconnaissance implémentés

Trois processus de reconnaissance régissent dans le système proposé. Le processus d'apprentissage ou d'enrôlement permettant de construire le modèle et d'avoir une base de donnée biométrique, le processus d'identification permettant de reconnaitre l'identité d'un individu, et enfin le processus de vérification permettant d'affirmer un client authentique ou de refuser un imposteur. Dans ce qui suit nous allons détailler ces trois processus.

7.6.1. Le processus d'apprentissage

L'apprentissage automatique est un des champs d'étude de l'intelligence artificielle. L'apprentissage automatique fait référence au développement, à l'analyse et à l'implémentation de méthodes qui permettent à une machine (au sens large) d'évoluer

grâce a un processus d'apprentissage, et ainsi de remplir des taches qu'il est difficile ou impossible de remplir par des moyens algorithmiques plus classiques.

Nous avons donc opté pour l'apprentissage supervise basé sur l'extraction à partir de l'image binarisée à l'aide d'une base d'exemples permettant au programme de savoir a quoi ressemble chaque caractéristique du trait biométrique (l'empreinte digitale). Nous nous sommes servis d'une base d'images binarisées (instances).

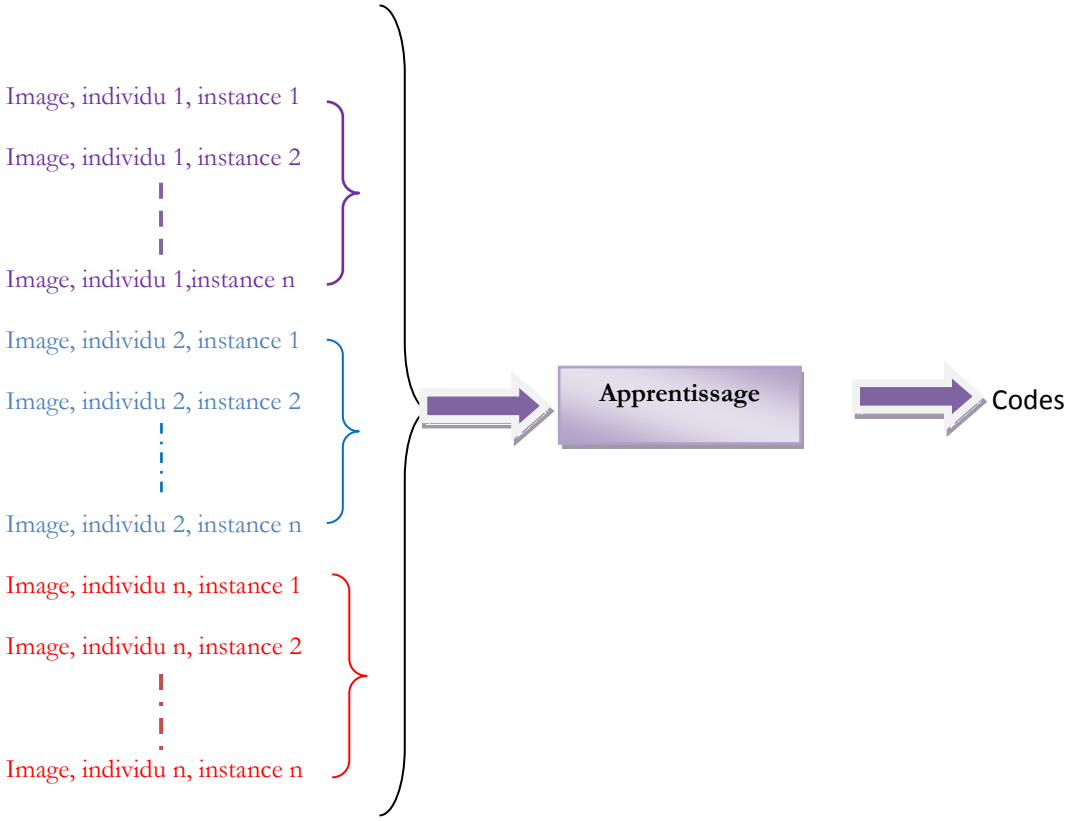


Figure 7.9 : DFD Apprentissage (niveau0).

Le diagramme de .la figure 7.9 représente le processus d'apprentissage des images contenant plusieurs instances (dans la littérature on parle de « impressions » ou « instances » qui sont des captures répétés du trait biométrique du même individu), ces instances nous permettent de calculer et ensuite tracer la courbe des utilisateurs ou clients authentiques aussi nommée les distributions intra classe en Anglais« intra *class distributions* »ou « *genuine distributions* ».

7.6.2. Le Processus d'identification

Le mode d'identification est un problème 1 à N (comme nous l'avons expliqué au chapitre 1), l'image à identifier est une image d'un individu qu'on ne connait pas son identité (c-à-d les informations comme le nom le prénom etc). Le processus d'identification est une boucle de recherche par mesure de similarité sur la base de données. Les figures ci-dessous (figure 7.10, figure 7.11 et figure 7.12) expliquent les flots de données du processus d'identification.

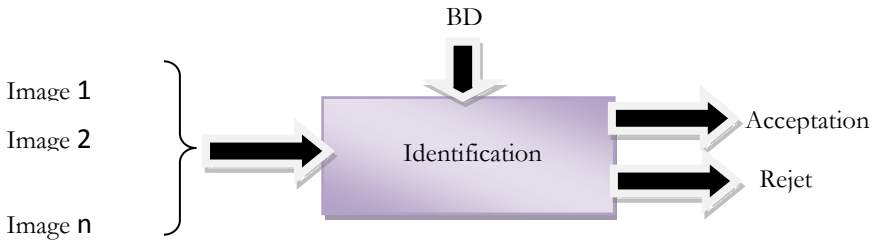


Figure 7.10 : DFD Identification (niveau 0).

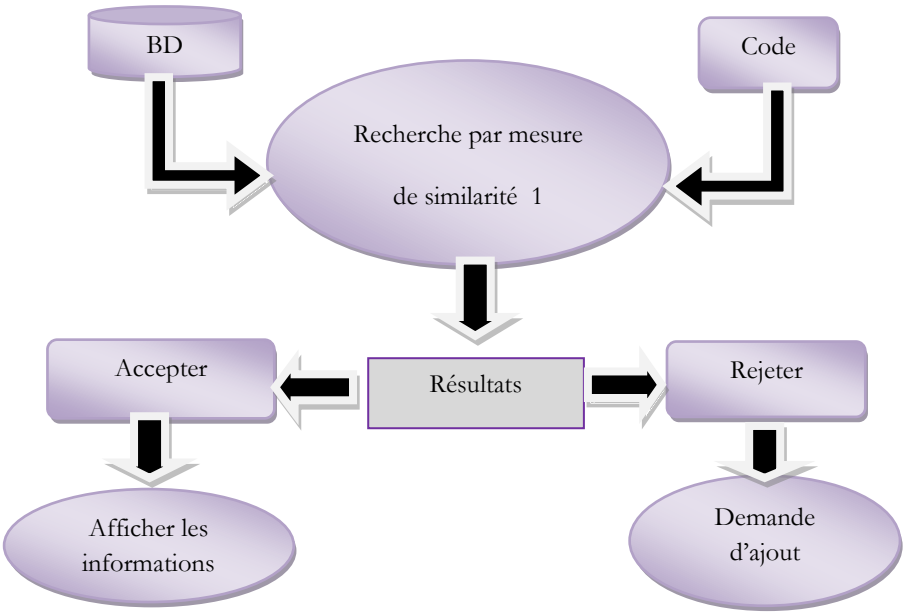


Figure 7.11 : DFD Identification (niveau 1).

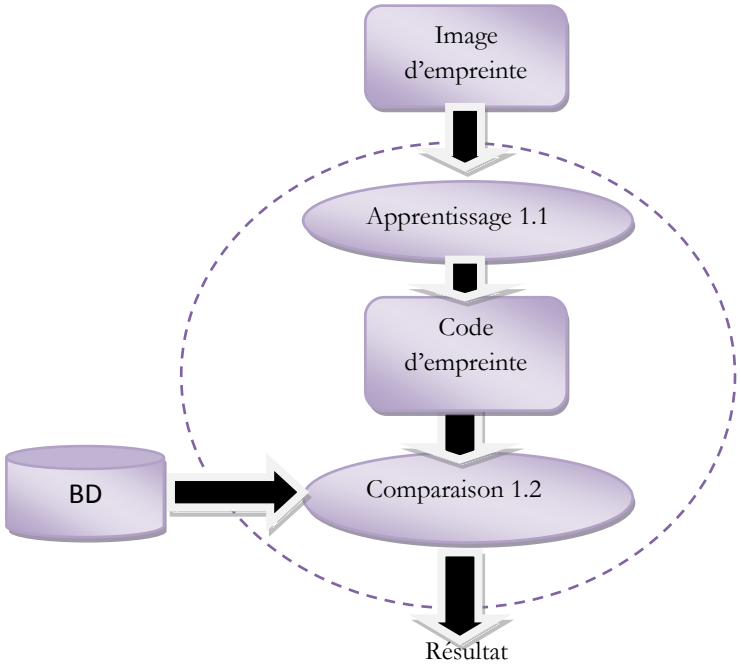


Figure 7.12 : DFD Recherche de similarité (niveau 1).

7.6.3. Le processus de vérification

Il comporte également deux phases : la phase d'apprentissage pendant laquelle les modèles sont construits de la même manière que pour le processus d'identification (les modèles sont sauvegardés dans une carte de gabarit biométrique), et la phase de vérification (phase de comparaison au seuil de décision). Cf. Figures 7.13 et 7.14.

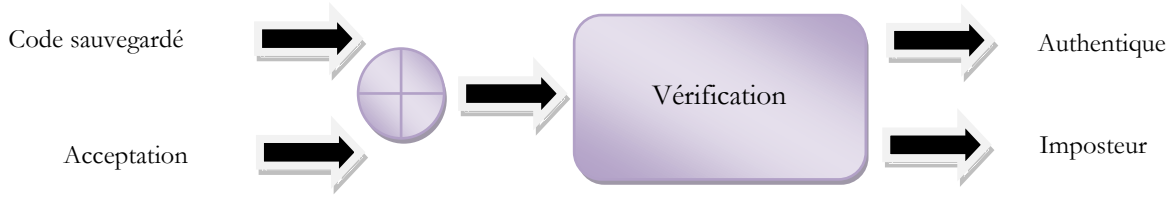


Figure 7.13 : DFD Vérification (niveau 0).

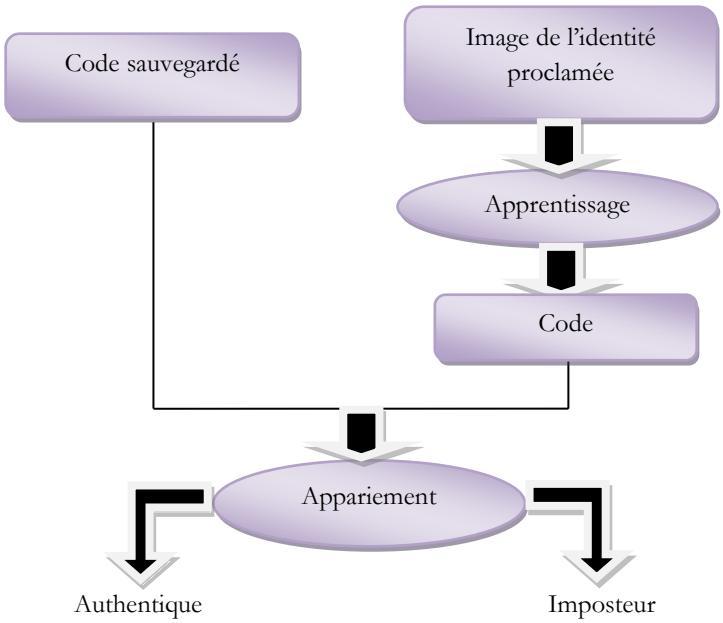


Figure 7.14 : DFD Vérification (niveau 1).

7.7. Validation et résultats expérimentaux

7.7.1. Matériel utilisé et recommandé

Tableau 7.2 : Description du matériel utilisé et du matériel recommandé pour l'application de la fusion d'empreintes.

Matériel utilisé			
Modèle	**Processeur**	**Mémoire vive**	**Système d'exploitation**
HP Compaq 6830s	**Intel ® Core™ 2 Duo CPU T5870 @ 2.00 GHz**	**2.00 Go**	**Windows VistaTM Edition Familiale Prenium**
Matériel recommandé			
/	**1.60GHz minimum**	**1.00 Go**	**Windows XP Professionnel Service Pack 2**

Le tableau 7.2 présente le matériel utilisé pour l'application et notamment la description du matériel recommandé pour le bon déroulement des processus implémentés.

7.7.2. Langage de programmation utilisé

Nous avons eu recours lors de l'élaboration de l'application à deux outils :

- Java NetBeans 6.9.1 avec le Kit de développement JDK 6 - i586.
- Microsoft Office Access 2010.

Java est un langage de programmation informatique à usage général, évolué et orienté objet été conçu par *James Gosling* en 1994 chez Sun Microsystems. L'idée était d'avoir un langage de développement simple, portable, orienté objet, interprété. Java reprend la syntaxe de C++ en le simplifiant. Java offre aussi un ensemble de classes pour développer des applications de types très variés (réseau, interface graphique, multi-tâches, etc.). Java comprend bien d'autres aspects (programmation graphique, applets, programmation réseau, multi-tâches).

7.7.3. Base de données utilisée

Nous avons utilisé la base de données FVC 2000 (Cf. Tableau 7.3). Elle est disponible en achetant le DVD contenant la base de données avec la seconde édition du livre « *Handbook of Fingerprint recognition* » de Maltoni [Maltoni et al., 2009]. Cette base contient quatre bases de données DB1, DB2, DB3 et DB4 de 880 images d'empreintes chacune.

La base de données FVC 2000 est la première base d'empreintes digitale utilisée dans les compétitions FVC [Maio et al., 2000]. Ces compétitions ont été crées afin de rassembler les programmeurs pour un seul but, réaliser le meilleur algorithme de vérification par empreinte.

Tableau 7.3 : Description de la base d'empreintes FVC 2000

	Type de capteur	Dimension de l'image	Ensemble A	Ensemble B	Résolution
DB1	Capteur Optique	300x300	100x8	10x8	500 dpi
DB2	Capteur Capacitive	256x364	100x8	10x8	500 dpi
DB3	Capteur optique	448x478	100x8	10x8	500 dpi
DB4	Capteur Synthétique	240x320	100x8	10x8	500 dpi

7.7.4. Répartition de la base de données

La base de données sera répartie comme suit :

40% de la base de données, est réservé pour l'apprentissage, c'est-à-dire l'estimation des paramètres du modèle (classificateur).

60% de la base de données est utilisé comme ensemble de test. Cet ensemble qui n'a pas était utilisé dans l'élaboration du meilleur modèle (classificateur), permet de déterminer la performance du meilleur modèle sélectionné dans la phase de validation (Cf. Figure 7.15).

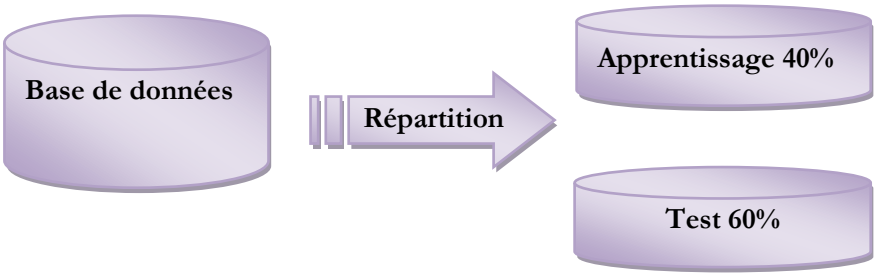


Figure 7.15 : Répartition de la base de données.

7.7.5. Les distributions intra classe et inter classes

Pour une base donnée quelconque, si c représente le nombre de classes, et n représente le nombre total d'images par classe, donc les combinaisons intra-classes sont calculées ainsi :

(n-1 x (n / 2) × c) [Abhyankar & Schuckers, 2010]

et les combinaisons interclasses sont calculées comme suit :

(c × (c -1) × n × n) [Abhyankar & Schuckers, 2010].

Par exemple, pour la base CASIA V1, les combinaisons intra-classes sont ((7-1) × (7/2) × 108)= 2268 et les combinaisons interclasses sont (108 × 107 × 7 × 7) = 566244.

Pour la base de données CASIA –V2, les combinaisons intra-classes sont ((20-1) × (20/2) × 120) = 22800 et les combinaisons interclasses sont (120 × 119× 20× 20) = 5712000.

Pour la base de données FVC 2004, les combinaisons intra-classes sont ((800-1) × (800/2) × 4) = 1278400 et les combinaisons interclasses sont (4 × 3 × 800× 800) =7680000.

7.7.6. Présentation de l'application

On présente dans cette section les différentes interfaces graphiques de l'application permettant à l'utilisateur de s'interagir avec les modules du système.

7.7.6.1. Interface Présentation (Homme)

C'est une interface destinée aux utilisateurs (Cf. Figure 7.16), elle est simple et permet d'illustrer les principaux processus de ce système (Apprentissage, Identification, Aide, A propos, Démonstration).

Figure 7.16 : Interface Principale de l'application de vérification par empreinte.

1. Il s'agit du bouton avec lequel la démonstration est lancée.
2. Il s'agit du bouton avec lequel l'identification d'un individu est lancée.
3. Il s'agit du bouton avec lequel on lance l'opération d'apprentissage.
4. Il s'agit du bouton avec lequel on obtient de l'aide sur le fonctionnement du système.
5. Il s'agit du bouton avec lequel on affiche des informations sur le système.

7.7.6.2. Interface Démonstration (01)

L'utilisateur peut parcourir l'ensemble des images d'individus et sélectionner l'une d'elles pour la démonstration (Cf. Figure 7.17).

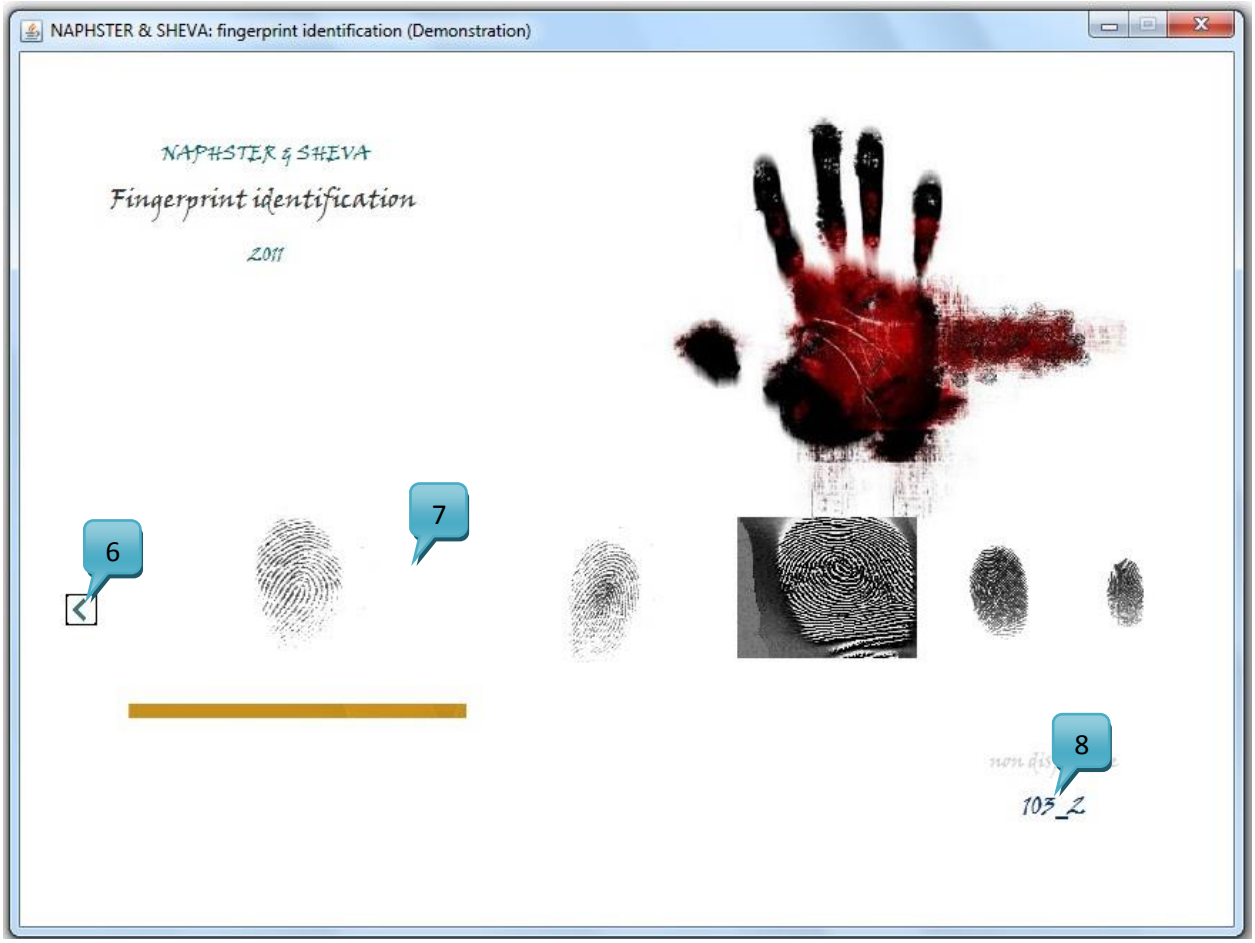


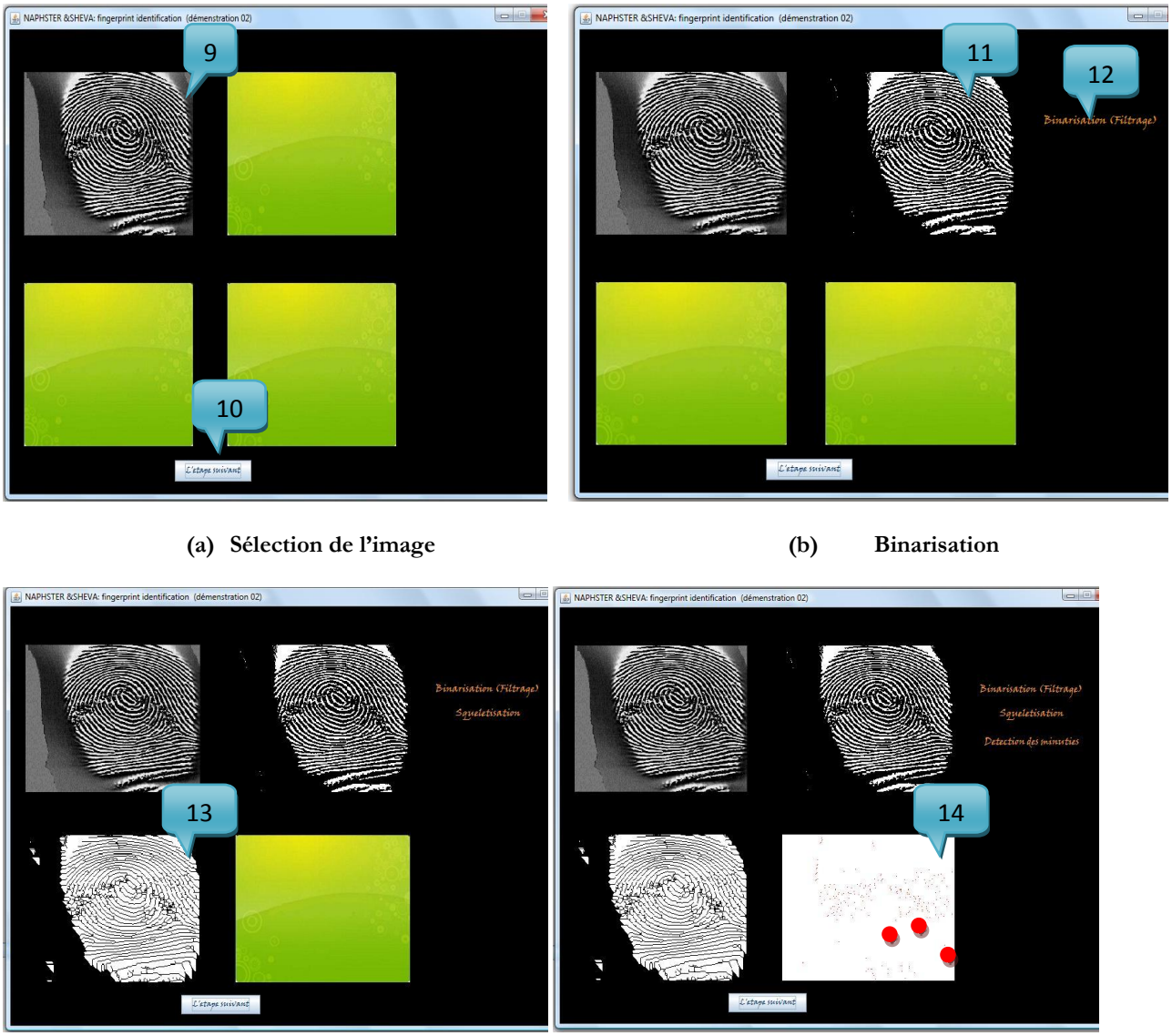
Figure 7.17 : Interface Démonstration 1, choix de l'image en entrée.

6 bouton pour parcourir l'ensemble des images d'individu.
7 Il s'agit du bouton avec lequel l'utilisateur peut sélectionner une image d'individu pour la démonstration.
8 La référence de l'image sélectionnée dans la base de données.

Cette interface graphique permet à l'utilisateur de visualiser l'ensemble des images d'empreinte dans la base de données, de selectionner l'image désirée, et de la voir en zoom avant.

7.7.6.3. Interface Démonstration (02)

L'utilisateur peut voir les différentes étapes de la démonstration de l'image sélectionnée.



(a) Sélection de l'image (b) Binarisation

(c) Squeletisation (d) Détection de minuties

Figure 7.18 : Interface Démonstration (2), montrant les étapes de la segmentation de l'empreinte.

9 Affichage de l'image original.
10 Il s'agit du bouton avec lequel l'utilisateur passe d'une étapes à une autres.

Etapes 01 (binarisation)

11 Affichage de l'image après binarisation.
12 Il s'agit d'une zone d'affichage (pour afficher le nom de chaque étape).

Etapes 02 (Squelettisation)

13 Affichage de l'image après squelettisation.

Etapes 03 (Détection des minuties)

14 Affichage de l'image après détection des minuties.

7.7.6.4. Interface Apprentissage (Ajouter personne)

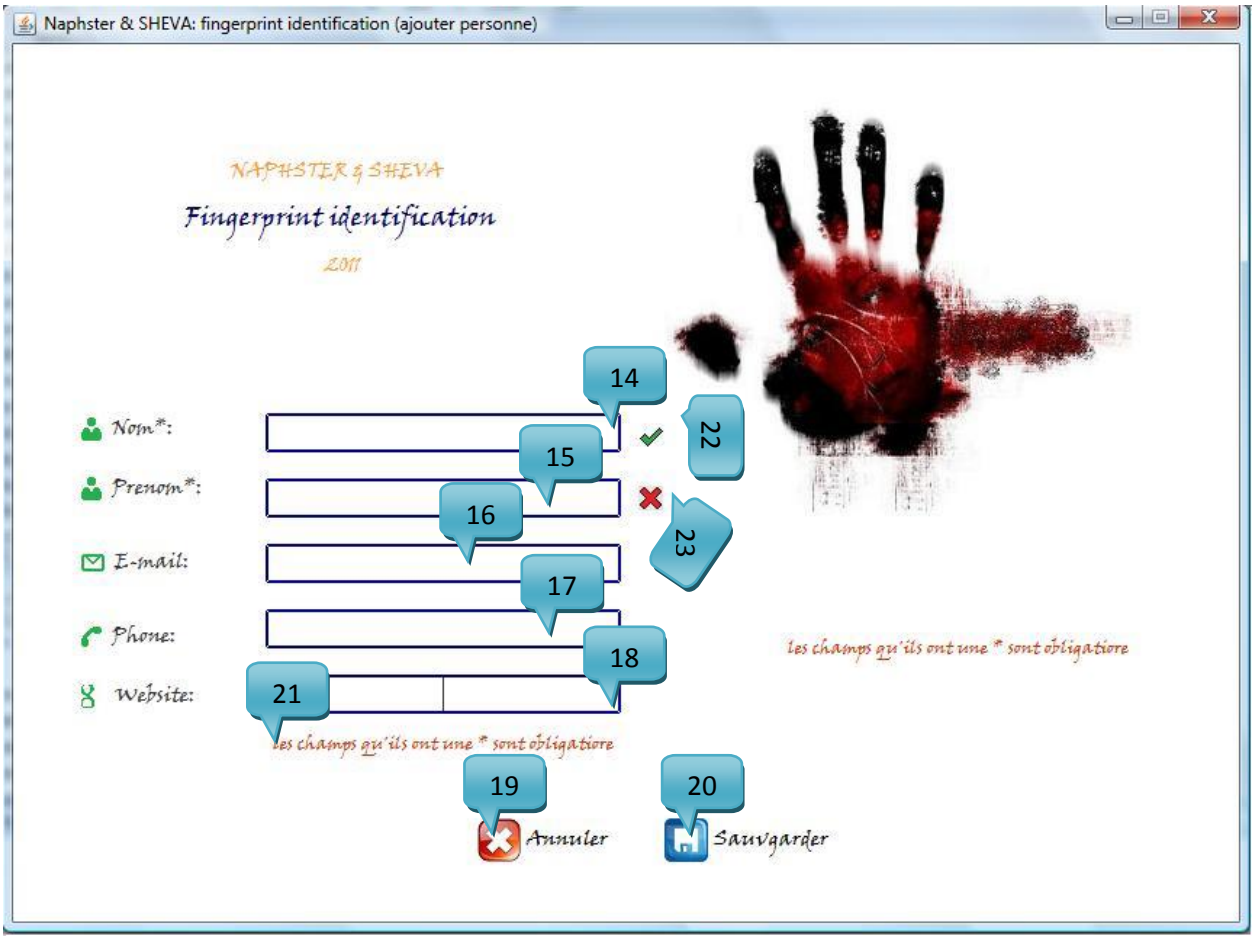


Figure 7.19 : Interface Apprentissage permettant d'ajouter une personne.

14 Champ pour saisir le (*Nom*).
15 Champ pour saisir le (*Prénom*).
16 Champ pour saisir le (*E-mail*).
17 Champ pour saisir le (*Téléphone*).
18 Champ pour saisir le (*Site Web*).
19 Il s'agit du bouton avec lequel l'utilisateur peut annuler.
20 Il s'agit du bouton avec lequel l'utilisateur peut sauvegarder.
21 Message précisant que les deux champs *Nom* et *Prénom* sont obligatoire et doivent être rempli.
22 Indique que le champ obligatoire a été rempli.
23 Indique que le champ obligatoire n'a pas été rempli.

7.7.6.5. Interface Apprentissage (sélection d'un doigt ou instances)

La figure 7.20 montre l'interface de l'application permettant à l'utilisateur de choisir les paramètres de l'apprentissage. 1 doigt ou 3 doigts, une instance d'empreinte, trois instances d'empreinte ou huit instances d'empreintes.

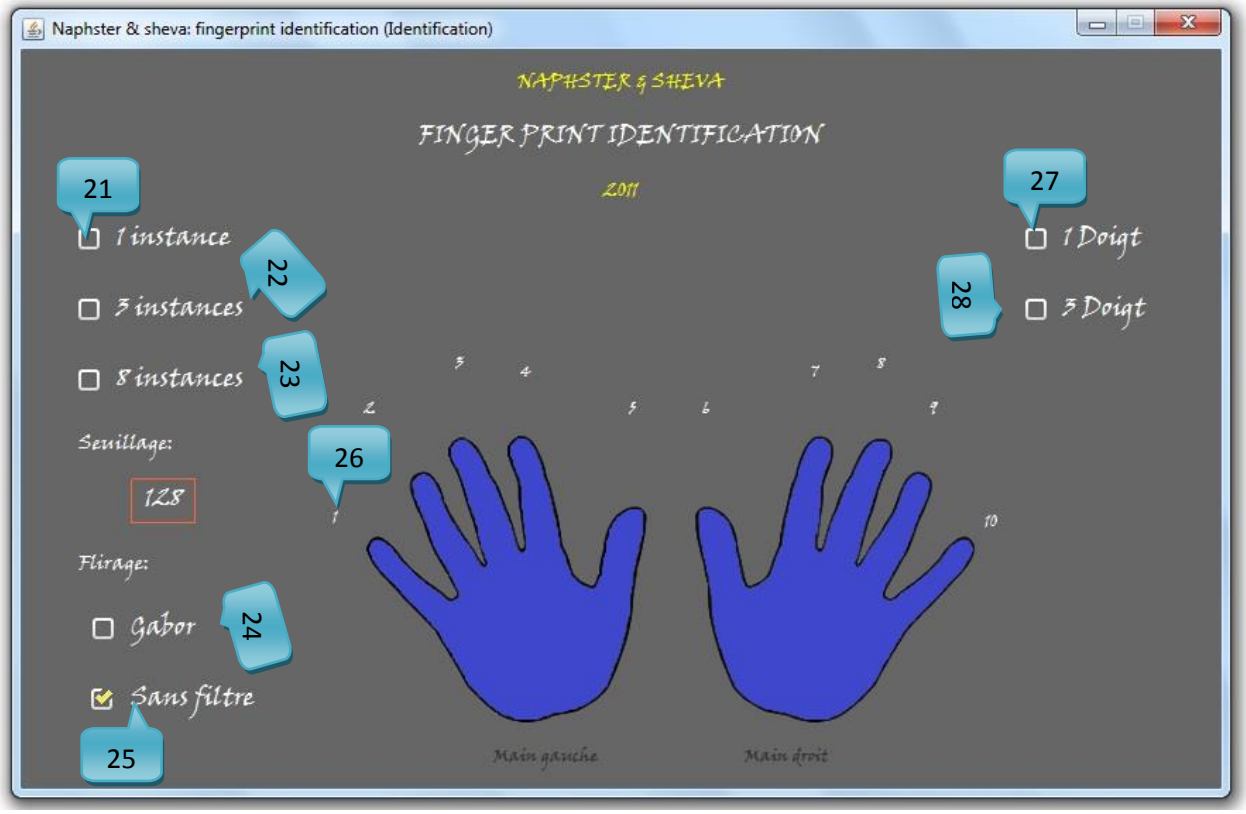


Figure 7.20 : Interface Apprentissage (choix des paramètres de l'apprentissage de l'empreinte).

21 Il s'agit du bouton avec lequel l'utilisateur choisie d'utiliser une seul instance.
22 Il s'agit du bouton avec lequel l'utilisateur choisie d'utiliser trois instances.
23 Il s'agit du bouton avec lequel l'utilisateur choisie d'utiliser huit instances.

7.7.7. Critères d'évaluation du matcher

On définit les critères d'évaluation suivants:

• *Sensibilité* (*Sensitivity*) S(%): S=D - O / N

• *Spécificité* (*Specificity*) P(%): P=D – F / N

D: le nombre de minuties détectées, O: le nombre de minuties omises et F: le nombre de fausses minuties. Avec N le nombre total des minuties dans l'image de l'empreinte digitale

La *Sensibilité* S mesure la capacité de l'extracteur de détecter de vraies minuties, alors que la *Spécificité* mesure sa capacité d'éviter les fausses détections.

Le tableau suivant (tableau 7.4) explique comment calculer les mesures de *Sensibilité* S et de *Spécificité* P, (nous avons choisi aléatoirement quatre images de FVC 2000-BD1-B).

Tableau 7.4 : Exemple montrant comment calculer les mesures de sensibilité S% et de spécificité P%.

	Im1	Im2	Im3	Im4
N	555	713	92	233
F	94	41	5	11
D	461	672	87	222
O	25	20	10	15
P%=D-F/N	83.03	94.24	94.56	95.27
S%=D-O/N	95.49	97.19	89.13	93.56

Les minuties oubliées ou omises O sont comptabilisées par l'œil humain, cela prends plusieurs jours et même des semaines pour les compter en utilisant toutes les images de la base de données (880 images d'empreinte pour FVC 2000).

Pour procéder à l'évaluation de l'approche proposée, nous utilisant trois expériences :

Expérience 1 : dans cette expérience une seule empreinte est utilisée, donc un seul vecteur de caractéristique est généré.

Expérience 2 : dans cette expérience trois empreintes du même doigt sont utilisées, donc un seul vecteur de caractéristique est généré, égal à la somme des vecteurs de caractéristiques individuels.

Expérience 3 : dans cette expérience huit empreintes du même doigt sont utilisées, donc un seul vecteur de caractéristique est généré, égal à la somme des vecteurs de caractéristiques individuels.

La concaténation des vecteurs de caractéristiques est réalisée lorsque les empreintes proviennent de doigts différents.

7.7.8. Résultats en termes de *sensibilité* et de *spécificité*

Dans cette section nous présentons les résultats expérimentaux en termes de Spécificité et Sensibilité relatifs aux trois expériences.

La figure 7.21 présente les courbes des mesures de Sensibilité S et de Spécificité P de l'expérience 1, dans laquelle une empreinte est utilisée dans le test. Cette expérience sert de référence.

La figure 7.22 présente les courbes des mesures de Sensibilité S et de Spécificité P de l'expérience 2, dans laquelle trois empreintes du même doigt sont utilisées dans le test.

La figure 7.23 présente les courbes des mesures de Sensibilité S et de Spécificité P de l'expérience 3, dans laquelle huit empreintes du même doigt sont utilisées dans le test.

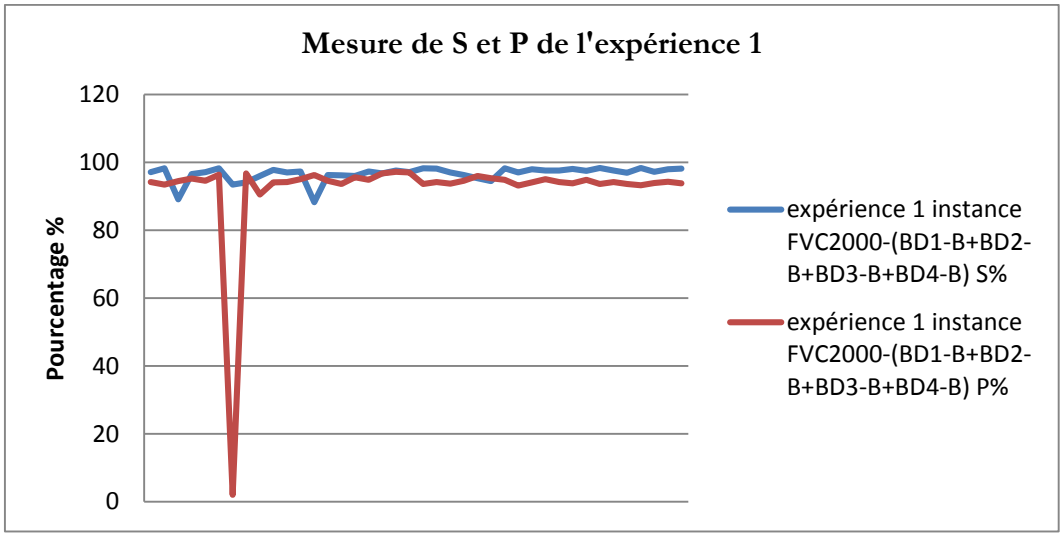


Figure 7.21 : Résultats de Spécificité et de Sensibilité de l'expérience 1 (1 instance).

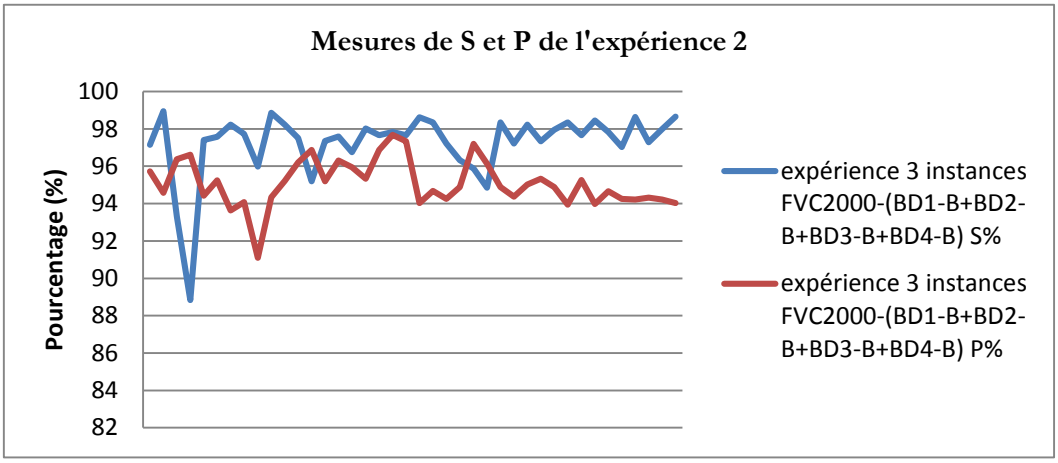


Figure 7.22 : Résultats de Spécificité et de Sensibilité de l'expérience 2 (3 instances).

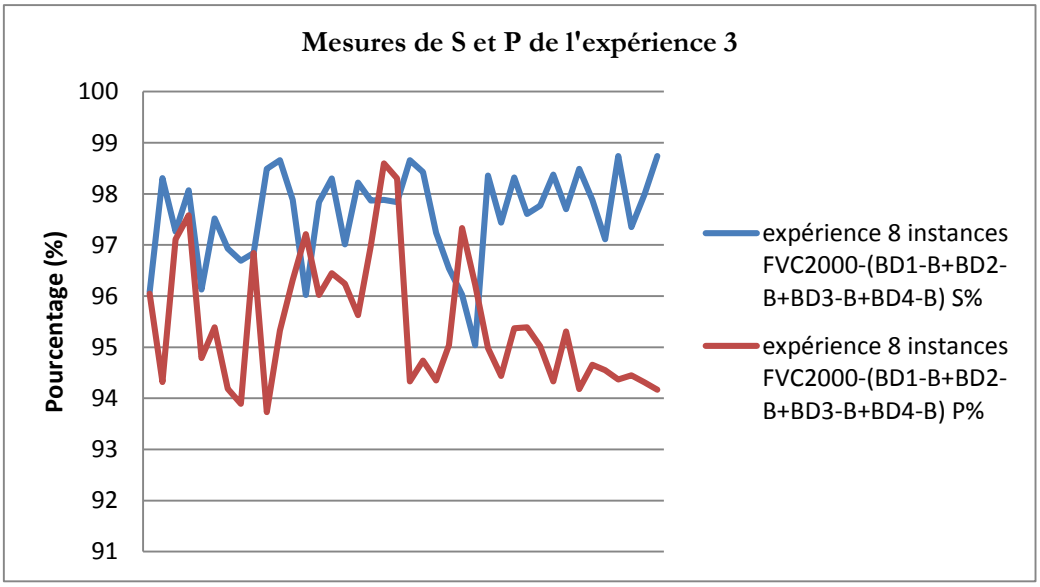


Figure 7.23 : Résultats de Spécificité et de Sensibilité de l'expérience 3 (8 instances).

On remarque que :

- les valeurs de la mesure de sensibilité sont légèrement plus grandes que celles de la spécificité dans toutes les expériences.
- Une image d'empreinte de mauvaise qualité a générée la chute de la courbe de *Spécificité* dans l'expérience 1 vers la valeur de 2%, ces types d'images fortement détériorées sont supprimés de la base.

Dans la figure 7.24, nous présentons la comparaison des trois expériences en termes de la moyenne de la *Spécificité* P et la *Sensibilité* S.

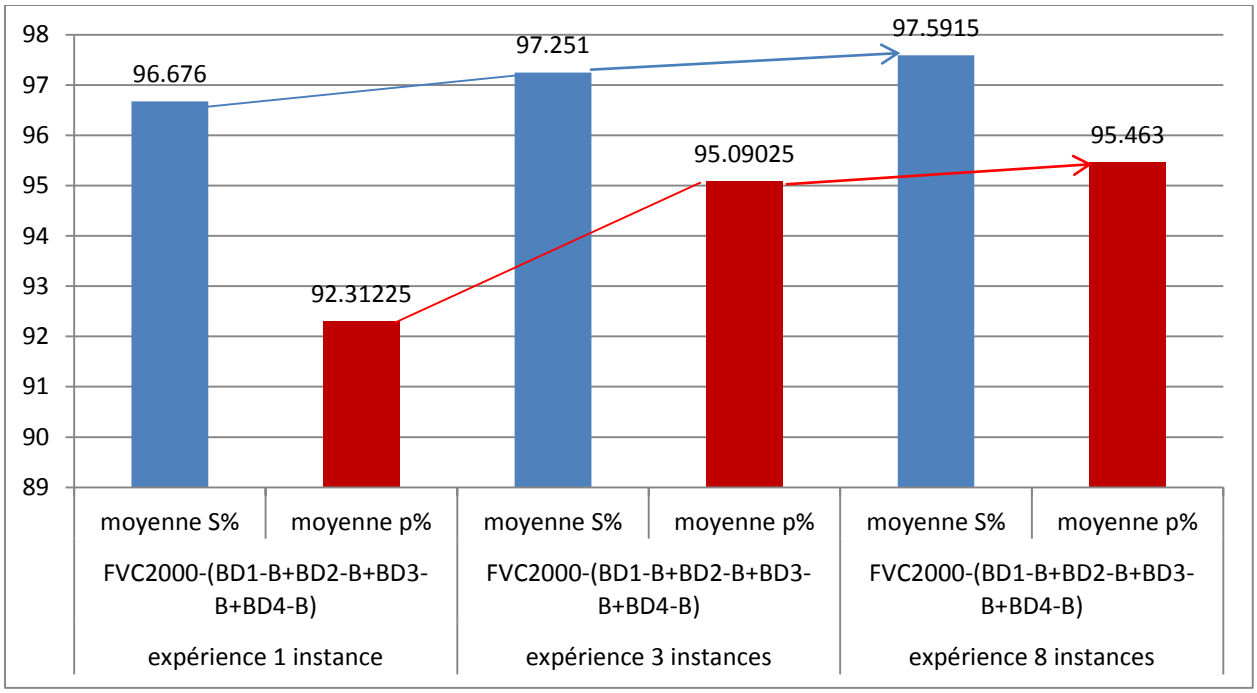


Figure 7.24 : Comparaison des Résultats de Spécificité et de Sensibilité.

D'après la comparaison, On constate que,

- le critère de la *Sensibilité* S, qui mesure la capacité de l'extracteur de détecter de vraies minuties, s'améliore à chaque fois en fusionne plus d'empreinte par doigt.
- Le critère de la *Spécificité* , qui mesure la capacité de l'extracteur à éviter les fausses détections, s'améliore à chaque fois en fusionne plus d'empreinte par doigt.
- La *sensibilité* est meilleure que la *spécificité* dans les trois expériences, donc on retient que les faux rejets sont beaucoup plus fréquents que les fausses acceptations.
- Dans les images d'empreintes de mauvaise qualité le nombre de minuties est inférieur au nombre confident permettant l'appariement. Ce nombre est fixé par 12 dans notre application, donc les images ne remplissant pas ce critère ne sont pas appariées.

Les figures 7.25, 7.26 et 7.27 présentent les courbes ROC des trois expériences.

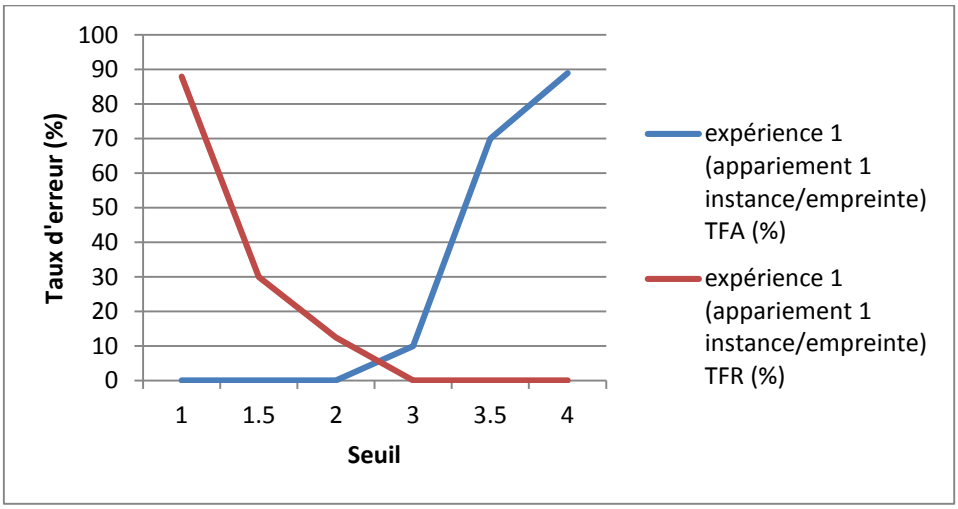


Figure 7.25 : Courbe ROC de l'expérience 1.

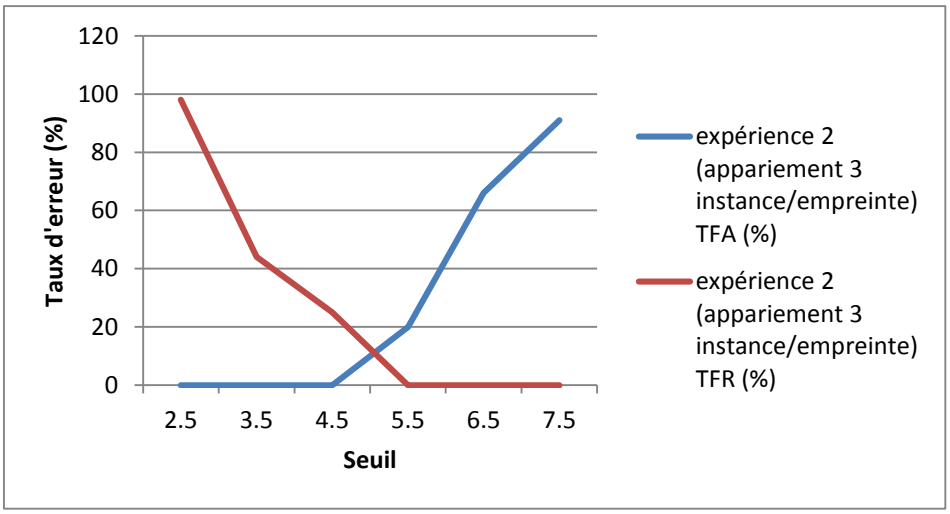


Figure 7.26 : Courbe ROC de l'expérience 2.

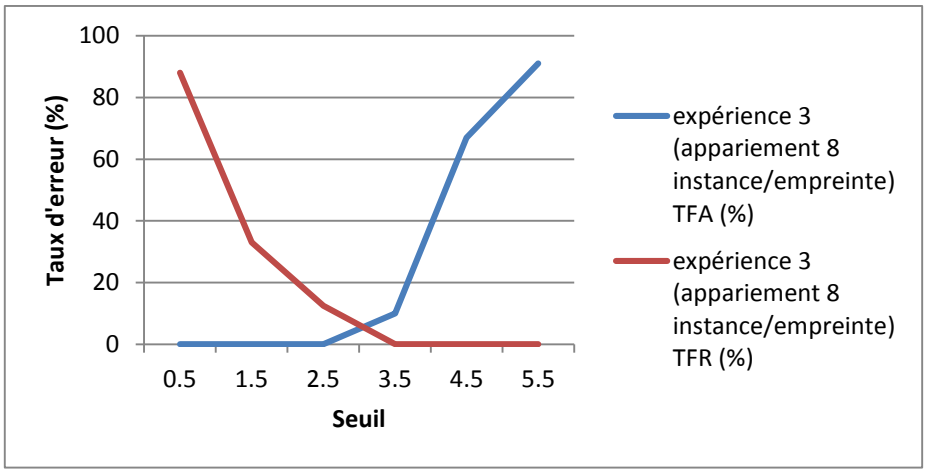


Figure 7.27 : Courbe ROC de l'expérience 3.

Tableau 7.5 : Taux d'erreurs des trois expériences.

	TFA (%)	TFR (%)	TEE (%)
Expérience 1	40	37.5	7
Expérience 2	20	25	5
Expérience 3	10	12.5	2.5

Tableau 7.6 : Précision des trois expériences.

	Précision = 1-(TFA+TFR)/2
Expérience 1	61.25%
Expérience 2	77.5%
Expérience 3	88.75%

Le tableau 7.5 présente les taux d'erreurs calculés pour chaque expérience. Le Taux d'égalité d'erreur TEE s'améliore à chaque fois on fusionne plus d'empreintes.

La précision atteinte par l'expérience 3 ou huit impressions d'empreintes ont été fusionnées est 88.75%. Ce taux est acceptable vu le nombre élevé des empreintes de mauvaise qualité présentées dans la base de données FVC 2000.

Tableau 7.7 : Temps d'exécution par phase de traitement.

Phase de traitement	Temps (s)
Amélioration et binarisation	7
Amincicement	9
Detection de minutie	11
Post Traitement	13
Appariement	14

Tableau 7.8 : Comparaison de l'approche proposée avec des Travaux voisins.

Algorithme	Meilleur TEE
FVC2000 [24]	1.32
FVC2002 [25]	0.16
FVC2004 [26]	0.81
FVC2006 [30]	0.05
[Ito et al ., 2005]	1.90
[Adytia Abhyankar et al 2008]	0.03
[Arjun V Mane et al 2011]	3.00
Approche proposée [Benaliouche & Touahria, 2012]	0.025

Les résultats obtenus sont satisfaisants. En effet, nous avons pu avoir des performances en terme de TEE de 2.5 % seulement. La comparaison de notre travail avec quelques travaux similaires a montré notre apport. En effet, les performances de notre système dépassent celles des travaux présentés dans le tableau 7.8. Ces travaux de recherche traitent le problème posé par la mauvaise qualité des images enrôlées et son influence sur les performances de la reconnaissance biométrique.

7.8. Conclusion

Plusieurs méthodes sont utilisées pour reconnaitre les empreintes digitales :

- La localisation des minuties : ces méthodes utilise la notion de minutie qui est le changement de la direction des crêtes (fin de ligne, bifurcation, ilôt, lac etc). Cette direction de recherche est très utilisées par les chercheurs du domaine pour sa simplicité et efficacité.

- Le traitement de textures : ces méthodes analysent et enregistrent les différentes propriétés de la texture de l'empreinte telles que son inclinaison, l'épaisseur des crêtes etc. cette direction de recherche est utilisées surtout lorsque la localisation des minuties échoue.

Beaucoup d'autres méthodes existent mais elles ne sont pas divulguées par les entreprises qui les exploitent dans le cadre de la propriété intellectuelle.

Pour caractériser une empreinte digitale, il faut un ensemble suffisant et fiable de minuties. Le nombre suffisant nécessaire de minuties pour pouvoir établir des comparaisons entre différentes empreintes est de 12 ou 14 minuties, mais avec entre 15 et 20 minuties on peut réussir à cibler une empreinte digitale parmi plusieurs millions d'exemplaires.

La fusion d'empreinte avec d'autres modalités est très fréquente en biométrie, d'une part pour augmenter la fiabilité de la reconnaissance, et d'autre part, pour luter contre la fraude et la falsification. L'idée de combiner plusieurs instances ou impressions par doigt a été adressée par plusieurs chercheurs. Le but de ces travaux était d'arriver à abaisser au maximum les taux de fausses acceptation et de faux rejets tout en maintenant un taux de reconnaissance élevé. Ce but n'était pas toujours atteint vu la diversité des bases de données d'empreintes digitales contenant des ensembles d'images de mauvaise qualité (mauvaise capture ou détérioration causée par le temps ou les injures).

Le but principal du présent travail est de trouver une solution simple, rapide et précise concernant la reconnaissance par empreintes digitales lorsque celles-ci sont de qualité détériorée.

Notre contribution réside dans la proposition

1. D'un nouvel algorithme de fusion des vecteurs de caractéristiques d'empreintes digitale.

Quand les vecteurs de caractéristiques sont **homogènes** (par exemple, plusieurs images d'empreinte digitale du doigt d'un utilisateur), un unique vecteur de caractéristiques résultant peut être calculé comme une somme pondérée des vecteurs de caractéristiques individuels.
Lorsque les vecteurs de caractéristiques sont **hétérogènes** (par exemple, des vecteurs de caractéristiques de différents doigts), nous pouvons les concaténer pour former un seul vecteur de caractéristiques.

2. D'un nouvel algorithme d'appariement basé sur La concaténation des codes générés par les instances multiples d'empreinte digitales et son utilisation dans la phase de comparaison.

Le principe est de comparer l'empreinte du client avec trois/huit instances du même doigt, on suppose que le client est accepté si et seulement si la somme des résultats de reconnaissance (*matching*) est supérieure ou égale à 2 (pour trois instances) et supérieure ou égale à 4 (pour huit instances) sinon le client est rejeté.

Le système de vérification d'identité est basé sur la comparaison de deux ensembles de minuties 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 aux éventuelles translations, rotations et déformations qui affectent systématiquement les empreintes digitales.

Du fait de la variation d'inclinaison, de déformation (écrasement) ou de déplacement du doigt qui existe lors de deux acquisitions différentes d'une même empreinte, l'analyse de ces dernières ne donnera jamais 100% de similitudes, mais on obtiendra néanmoins toujours un pourcentage très élevé. Dans ce cadre, nous avons mené une étude quantitative visant à évaluer la pertinence de l'algorithme de fusion proposé.

Les mesures de performance du matcher (l'algorithme de fusion des vecteurs de caractéristiques) sont la Spécificité P et la Sensibilité S. l'étude statistique a montré que :

- Le critère de la S*ensibilité* S, qui mesure la capacité de l'extracteur de détecter de vraies minuties, s'améliore à chaque fois en fusionne plus d'empreinte par doigt.
- Le critère de la *Spécificité* , qui mesure la capacité de l'extracteur à éviter les fausses détections, s'améliore à chaque fois en fusionne plus d'empreinte par doigt.

Ensuite, conclure que deux empreintes sont issues du même doigt à partir de cet indice de similitude est une question purement statistique.

L'évaluation de l'apprentissage devra être conduite avec soin, en général, on mesure la performance après avoir dérouler l'apprentissage sur un certain nombre de donnée que l'on appelle échantillon d'apprentissage.

Cependant, il faut s'assurer que la mesure de performance s'effectue sur un échantillon de test différent de l'échantillon d'apprentissage.

Un train de test a été réalisé sur la base de données d'empreintes digitales FVC 2000. Cette base est caractérisée par des ensembles d'images d'empreintes de mauvaise qualité. Les résultats expérimentaux ont donné un TEE égal à 2.5% avec une précision de 88.75% pour l'expérience réalisant une fusion de huit impressions par doigt.

Chapitre 8

RECONNAISSANCE PAR FUSION D'IRIS ET D'EMPREINTE

8.1. Introduction

A l'heure actuelle, les technologies biométriques sont basées le plus souvent sur les modalités d'empreintes digitales ou d'iris, qui sont pour l'instant réputées les plus fiables en contrepartie de leur caractère intrusif. Il est certain que des modalités comme le visage, la voix, la signature manuscrite sont des modalités plus familières mais moins performantes pour pouvoir envisager leur utilisation à grande échelle. Dans ce cadre, la fusion de plusieurs modalités paraît une voie prometteuse qui reste à valider.

La fusion des méthodes biométriques constitue une solution actuelle, adéquate et prometteuse aux problèmes posés par les systèmes biométrique monomodaux. Plusieurs travaux de recherche ont déjà montré que la combinaison de plusieurs modalités biométriques permet d'améliorer de manière significative les performances des systèmes basés sur une seule modalité.

La fusion présente les avantages de bénéficier des points forts offerts par chacune des modalités fusionnées, tout en préservant l'indépendance et la séparabilité des variations statistiques de chaque trait biométrique.

Ce chapitre est concerné par l'introduction d'une nouvelle méthode de reconnaissance bimodale d'iris et d'empreinte digitale, basée sur la fuzzification des décisions, et l'inférence floue.

Tout d'abord, nous commencerons par citer les motivations et les objectifs de l'approche, ensuite nous présenterons une synthèse des travaux de recherche voisins, par la suite, nous présenterons la conception détaillée du système de reconnaissance par fusion multimodale, suivi de sa validation et des résultats expérimentaux. Enfin, nous comparons notre travail avec des travaux similaires pour montrer sa valeur ajoutée.

8.2. Motivation et objectifs

Ce chapitre est concerné par la proposition d'un nouvel algorithme de fusion multimodale d'iris et d'empreinte digitale à base de la logique floue. L'utilisation conjointe de deux traits biométriques ou plus est une tendance actuelle pour renforcer les systèmes biométriques sur les plans de sécurité, fiabilité et pertinence.

Motivation :

- Surmonter les limites de la monomodalité biométrique en proposant une solution de multimodalité biométrique en fusionnant deux traits biométriques différents (l'iris et l'empreinte).

Objectifs :

- Arriver à un meilleur compromis entre le taux de fasse acceptation TFA et le taux de faux rejet TFR par rapport aux travaux de recherche sur l'identification par fusion d'iris et d'empreinte.
- Voir l'influence de paramètres sur les algorithmes implémentés.
- Concevoir plusieurs scénarios de fusion et les comparer afin d'en tirer conclusion à propos du meilleur scénario de fusion

Une idée largement répandue dans le domaine de la fusion de données, est de lier le gain en performance issu de la fusion, à l'indépendance des données que l'on fusionne [Verlinde et al., 1998]. Dans ce cadre, nos objectifs sont :

- garder la séparabilité des scores d'appariements du système de fusion biométrique, en proposant une classification floue des scores.
- agir sur les scores et les décisions issus des systèmes monomodaux, à la fois pour la fusion, et pour l'analyse statistique des distributions authentiques qu'on souhaite au maximum les séparés de celles des imposteurs.
- Introduire la théorie des sous ensembles flous afin de représenter l'imprécision des données, mais également d'autoriser l'expression de préférence dans les critères de sélection de l'identité biométrique. L'utilisateur peut donc exprimer des requêtes larges fournissant des résultats classés par ordre de préférence.

8.3. Travaux voisins

Besbes et al [Besbes et al., 2008] proposent une fusion multimodale d'iris et d'empreinte digitale en utilisant l'approche par détection de minuties et l'encodage du code d'iris par une représentation mathématique de la région d'iris traitée. La fusion des décisions est réalisée par l'opérateur logique AND.

Baig et al [Baig et al., 2009] proposent une fusion biométrique multimodale basée sur l'utilisation d'une mise en œuvre de matcher unique pour les deux modalités (iris et empreintes digitales). Dans leur expérience, ils ont utilisé la base de données multimodale

de l'Université West Virginia contenant 400 images (4 prises d'images x 100 utilisateurs), le seuil est fixé à la valeur du taux d'erreur égal TEE. La comparaison est faite en termes de pourcentage d'amélioration du TEE plutôt que sa valeur.

Jagadeesan et al [Jagadeesan et al., 2010] ont introduit une technique de génération de clé cryptographique par fusion d'empreinte et d'iris. L'extracteur d'empreinte est basé sur l'approche de détection des minuties quand à l'extracteur d'iris est basé sur l'approche de John Daugman [Daugman, 1993] (filtre de C*anny* et transformée de *Hough*). La fusion est réalisée au niveau d'extraction de caractéristique. Le modèle généré est ensuite utilisé pour obtenir une clé cryptographique sécurisé sur 256 bit.

Jammer Basha et al [Basha et al, 2011] ont proposés une nouvelle fusion d'empreinte et d'iris au niveau *rang* (*rank level*); ils ont réalisés des tests expérimentaux en utilisant trois méthodes différentes de fusion multimodales: la méthode *du plus haut rang* (*Highest rank method*), la méthode de *compte de Borda* (*Borda count méthode*), et la méthode de la *régression logistique* (*Logistic regression method*). Leur travail a réalisé un meilleur temps d'exécution de la phase d'appariement égal à 0.45 seconde en utilisant la méthode du plus haut rang (*Highest rank method* avec des taux d'erreur optimaux égal à 0% pour le TFA et 0.25% pour le TFR.

Gawande et al [Gawande et al, 2012] ont présentés un nouveau scénario de fusion d'iris et d'empreinte en utilisant la concaténation des codes extraits d'iris et d'empreinte. Le filtre de *Gabor* est utilisé pour extraire les caractéristiques de l'iris et de l'empreinte. L'appariement est réalisé par la distance de *Hamming*. Les tests ont été conduits sur une base de données de 50 utilisateurs et ont donné un taux de faux rejet TFR = 4.3% pour 0% de taux de fausse acceptation TFA.

Radha & Cavitha [Radha & Cavitha, 2012] ont présentés un nouveau scénario de fusion d'iris et d'empreinte en utilisant le niveau de fusion de *rang*. Leur Approche est basée sur l'attribution de poids aux codes d'iris et d'empreinte selon leur importance dans la reconnaissance. Les techniques de « *Eigenimage* » et « *fisherface* » sont utilisés. . L'appariement est réalisé par deux algorithmes de fusion, (*Logistic Regression Method LRM*) et (*Borda Count Method BCM*). Les tests ont été conduits sur une base de données de 100 utilisateurs et ont donné un taux de faux rejet TFR = 88% pour 0.04% de taux de fausse acceptation TFA. Ces scores sont les meilleurs enregistrés selon la méthode de fusion (Logistic Regression Method LRM).

Récemment, Abdolahi et al [abdolahi et al, 2013] ont présenté un système de reconnaissance bimodal d'iris et d'empreinte avec l'utilisation de la logique floue et le code pondéré dans la phase d'appariement. Les auteurs ont choisi de pondérer Le code de l'empreinte par 20% et le code de l'iris par 80% pour donner plus d'importance à la décision de l'iris par rapport à la décision de reconnaissance donnée par l'empreinte. Leur travail a donné un taux de fausse acceptation TFA = 2% avec un taux de faux rejet égal TFR =20%, et une précision de reconnaissance égale à 98.3%.

P.U.Lahane et S.R.Ganorkar , [Lahane & Ganorkar, 2012] proposent une fusion de l'iris et de l'empreinte au niveau *extraction de caractéristiques*. Un code homogène est généré à partir d'un calcul de la région d'intérêt de la région d'iris et de la région d'empreinte. Après la normalisation des deux codes le filtre de *Gabor* est appliqué et le code des deux traits biométrique sera généré. L'appariement est réalisé par la distance E*uclidienne*. Les

meilleurs scores réalisé sont autour du seuil = 1 avec un taux d'erreur égal TEE =1.66, une précision = 99.5% et un taux de fausse acceptation TFA = 0.3% et un taux de faux rejet TFR = 0.5%.

Tableau 8.1. : Synthèse des travaux de recherche de la fusion Iris-Empreinte.

référence	[abdolahi et al, 2013]	[Gawande et al, 2012]	[Radha & Cavitha, 2012]	[Lahane & Ganorkar, 2012]	[Basha et al, 2011]	[Jagadeesan et al, 2010]	[Baig et al, 2009]	[Besbes et al, 2008]	[Lumini & Nanni, 2007]
Base de donnée	Non indiquée	Une base de données multimodale de 50 personnes	Une base de données de 100 personnes et (empreinte)	FVC2002 et URIBIS		Empreinte disponible publiquement + CASIA-iris V1	la base de données multimodale de l'Université West Virginia	Non indiquée	4 bases de données contenant 100 personnes avec 7 images
Niveau de fusion	décision	Extraction de caractéristique (feature level)	Niveau rang (rank level)	Extraction de caractéristique (feature level)	Niveau rang (rank level)	Extraction de caractéristique (feature level)	Extraction de caractéristique (feature level)	décision	score
méthode d'extraction de caractéristiques	Approche de Daugman pour l'extraction des codes d'iris et d'empreinte	Approche basée sur la fréquence	Les techniques de « Eigenimage » et « fisherface » sont utilisés pour les deux modalités.	Approche basée sur l'extraction des singularités de la région d'intérêt de l'empreinte et de l'iris		Approche par Extraction de minuties (empreinte)+approche basée transformée de hough (iris)	Approche par Extraction de minuties (empreinte)+approche basée transformée de hough (iris)	Approche par Extraction de minuties (empreinte)+approche basée transformée de hough (iris)	Approche de Daugman (iris) et quatre algorithmes d'extraction de code d'empreinte appartenant aux
Méthode d'appariement	Logique floue et code pondéré	Distance de Hamming	deux méthodes différentes de fusion multimodales (Borda count	Distance Euclidienne	Trois méthodes différentes de fusion multimodales (Highest rank	Pas d'appariement mais le travail vise à créer une clé cryptographiq	Règle somme	Opérateur AND	Quatre algorithmes de fusion (mean rule), (Linear Support
résultats	TFA=TFR=20	TFA= 0 % and TFR = 4.3 %.	TFA= 0.04 % and TFR = 88 %. Meilleur TFR et TFA pour la méthode de la	1.66 précision = 99.5% TFA = 0.3% TFR = 0.5%	TFA = 0% TFR = 0.25%	Sécurité améliorée système ayant la clé cryptographique associée à	TEE amélioré dua 50%	Non indiqués	Meilleur TEE =0.065 pour la méthode de fusion « Linear Support

8.4. Schéma général du système

En utilisant les concepts et les notations du langage pluridisciplinaire SADT et à l'aide de la technique de représentation des flots d'information « le diagramme de flots de données » DFD nous allons représenter la conception des différents modules du système qui sont :

1. Le module de la reconnaissance d'iris.
2. Le module de la reconnaissance d'empreinte.
3. Le module de la reconnaissance multimodale d'iris et d'empreinte.

La figure 8.1 schématise les différentes étapes incluses dans notre système de reconnaissance multimodale.

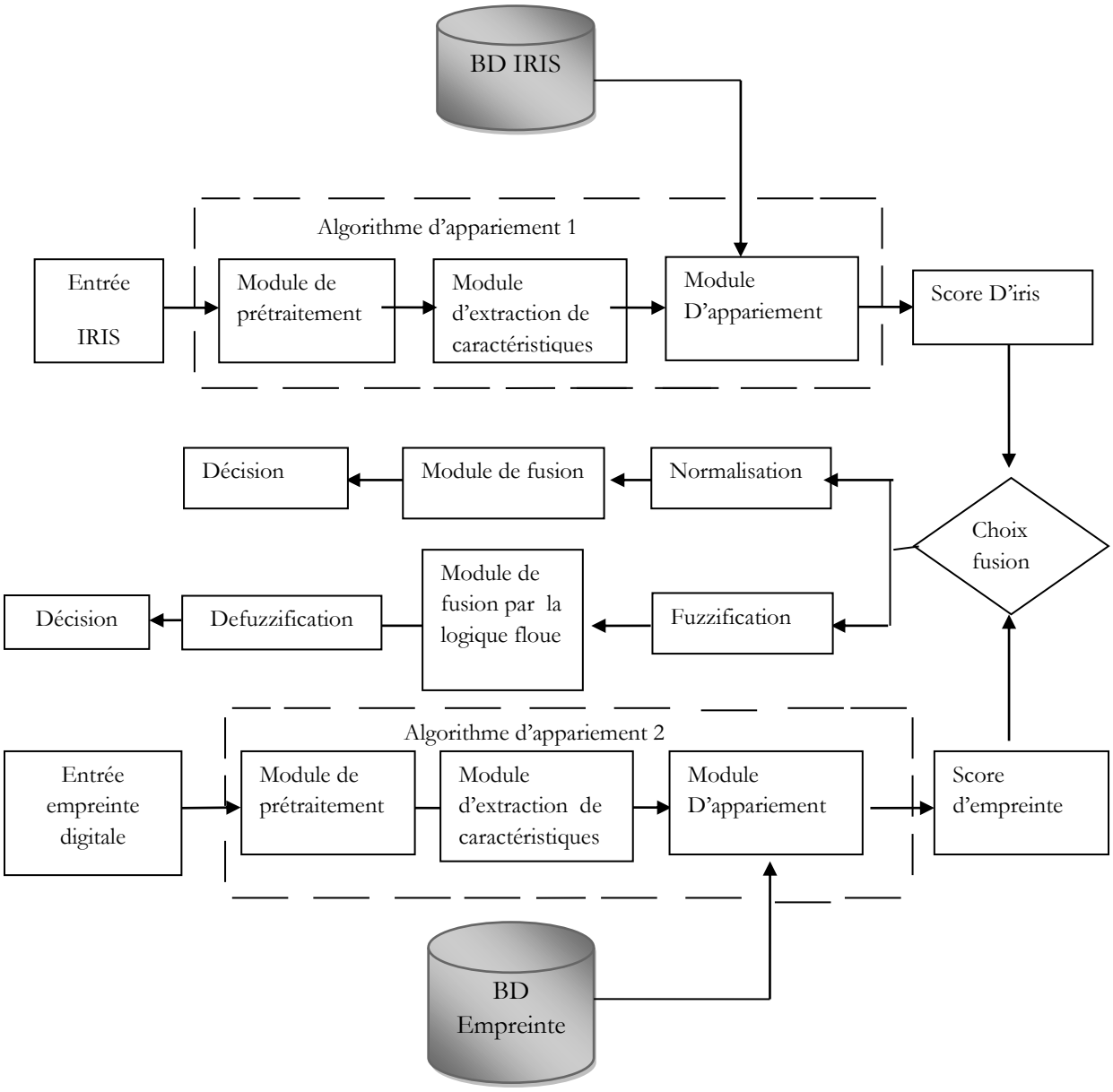


Figure 8.1 : Conception globale du système de reconnaissance multimodale d'iris et d'empreinte digitale.

Cette conception globale permet de voir :

1. à quel niveau les informations biométriques de l'iris et de l'empreinte sont fusionnés (le niveau score pour la fusion classique et le niveau décision pour la fusion avec la logique floue),
2. l'approche de fusion utilisée est l'approche par combinaison de scores lorsque la fusion est classique.
3. L'autre approche de fusion utilisée est la fusion des décisions lorsque la fusion est floue.
4. La normalisation des scores est nécessaire avant la fusion (ce qui est expliqué par l'utilisation de l'approche par combinaison de scores ou de décisions).
5. trois modalités ou algorithmes d'appariement sont utilisés : l'appariement par la somme classique, l'appariement par le somme linéaire pondérée et l'appariement par la logique floue.

L'architecture du système de reconnaissance multimodale proposé dans ce travail se base sur la fusion de score classique et la fusion de décisions par la logique floue comme la présente la figure ci dessous. Nous avons opté pour l'utilisation de deux niveaux différents de fusion (la fusion au niveau score et la fusion au niveau décision) afin de comparer les résultats des deux éventualités et en tirer la conclusion à propos de la meilleure démarche. Cf. Figure 8.2.

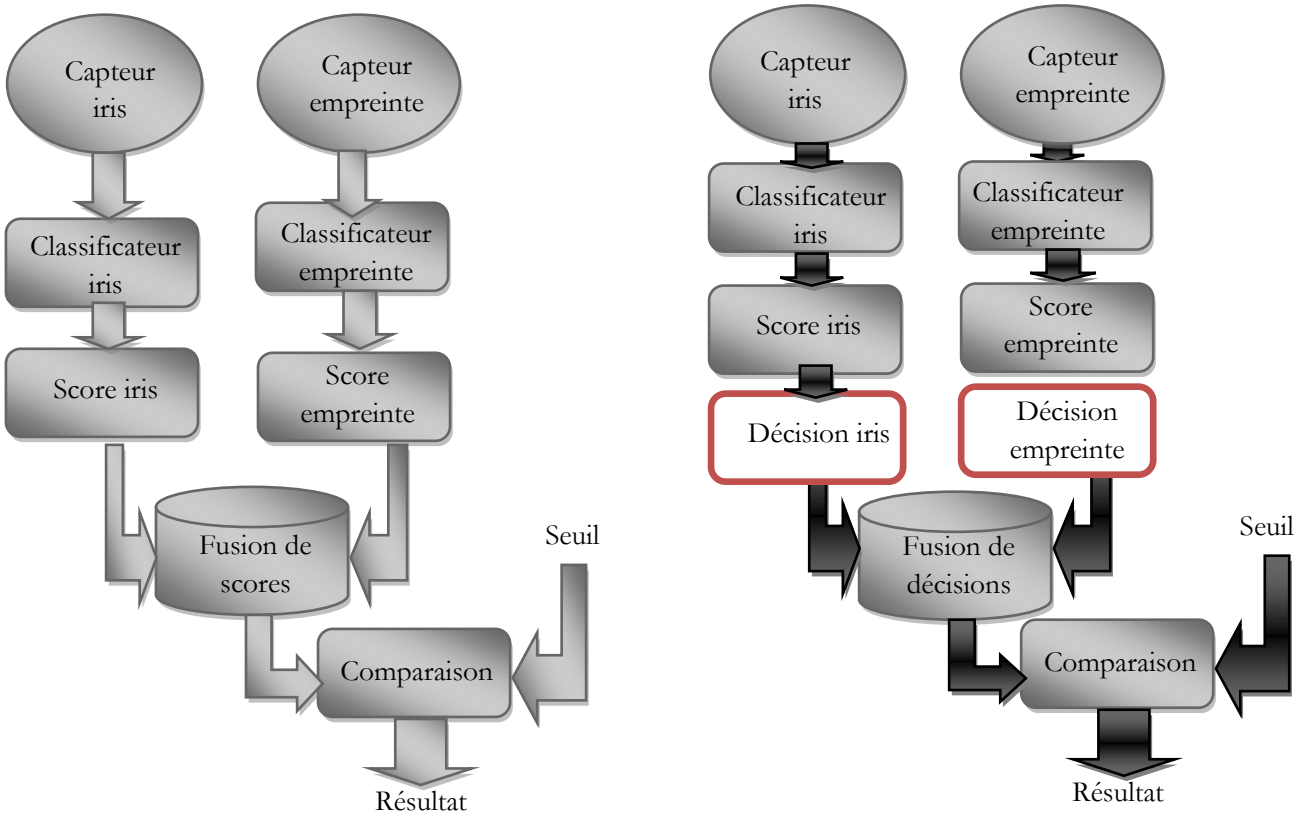


Figure 8.2 : Schéma représentant l'architecture du système multimodal proposé (la fusion de scores classique et la fusion des décisions par la logique floue sont deux approches de fusion différentes adoptées par notre système).

8.5. Les modules du système multimodal proposé

Notre système permet d'illustrer le processus d'apprentissage, identification et de vérification d'un individu. Nous Décrivons dans ce qui suit, les différents événements qui s'y passent lors de ces processus.

8.5.1 Le module de reconnaissance d'iris

Dans cette section nous présentons les détails de conception du module de reconnaissance d'iris. Nous utilisons une bibliothèque accessible au public de la reconnaissance d'iris (Masek & Kovesi, 2003) [Masek et Koveski, 2003] écrit en MATLAB. L'étape de localisation consiste en une segmentation automatique système basé sur la transformée de *Hough*; la région extraite d'iris est ensuite normalisée dans une fenêtre rectangulaire fixe, en remappant chaque point dans la région de l'iris pour un aire de coordonnées polaires en fonction du modèle de « *Rubber sheet* » développé par Daugman [Daugman, 1993]; en ce qui concerne l'extraction de caractéristiques et l'appariement, les données polaires résultantes de l'application du filtres *1D Log-Gabor* sont extraites et quantifiées à quatre niveaux , la distance de *Hamming* est employée dans la phase d'appariement.

Nous avons développé un système de reconnaissance d'iris avec deux modes opératoires :

1. **Le mode de vérification :** dans ce mode les variables d'entrée sont deux images d'iris, le système effectue une comparaison entre les deux identités et affiche le résultat.
2. **Le mode d'identification :** ce mode n'a pas été développé par Libor Masek, nous l'avons développé pour la recherche du code de l'image à identifier dans la base de données et afficher le résultat.

Dans ce qui suit nous détaillons notre conception du module de reconnaissance d'iris basée sur le noyau d'implémentation de Libor Masek [Masek, 2003].

8.5.1.1. Schéma général du système

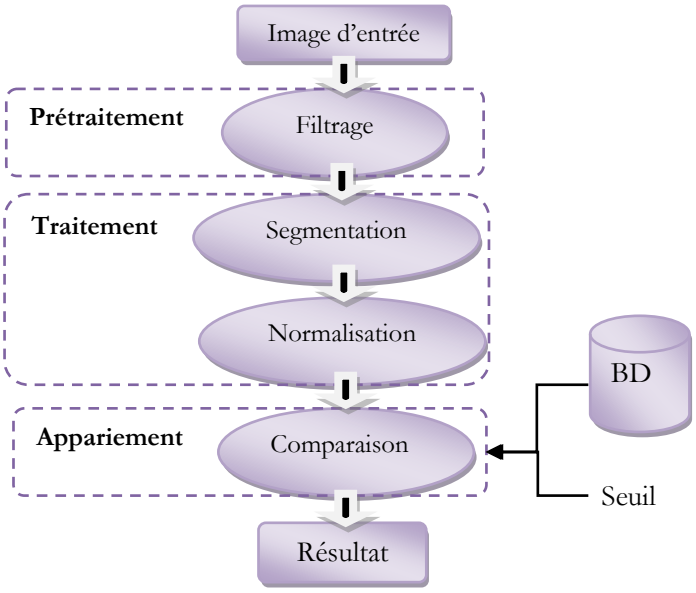


Figure 8.3 : Schéma général du système de reconnaissance d'iris.

8.5.1.2. La segmentation

La segmentation de l'iris est la première étape dans un processus de reconnaissance basé sur ce dernier. Elle consiste à isoler la texture de l'iris du reste de l'image de l'œil.

Objectifs:

- Localiser la frontière pupille/iris.
- Localiser la frontière iris/sclérotique.

Image initiale **Image segmentée**

Figure 8.4 : L'étape de segmentation.

Nous avons utilisé une technique basée sur *la transformée de Hough* pour la détection des lignes (paupières et bruit) et des cercles (frontières de l'iris).

Algorithme de segmentation : Notre système segmente les iris de la manière suivante :

1. *L'étiquetage des points de contours se fait par l'utilisation de l'algorithme de détection de Canny.*
2. *La détection de la frontière extérieure de l'iris se fait avant celle de la frontière intérieure:*
3. *Les gradients verticaux seuls sont utilisés pour détecter la frontière Iris-blanc de l'œil.*
4. *les gradients verticaux et horizontaux sont équitablement pondérés pour détecter les points de frontières de la pupille.*
5. *Chaque point de contour vote pour les cercles dont il appartient et le cercle qui obtient le plus de vote est le cercle recherché.*
6. *La détection des paupières est effectué en cherchant des droites détectés en utilisant la transformée de Hough.*

L'algorithme de détection de contour de *Canny* : Il est utilisé en traitement d'image pour mettre en évidence les contours des images analysées. Ses étapes sont les suivantes :

1. *Réduction de bruit : Permet d'éliminer les pixels isolés qui pourraient conduire à de faux contours.*
2. *Calcule du gradient.*
3. *Suppression des non-maxima : seuls les points correspondants à des maxima locaux sont considérés comme correspondants à des contours et seront conservés.*
4. *Seuillage des contours : ça nécessite deux seuils, un haut et un bas et pour chaque point, si l'intensité de son gradient est Inférieur au seuil bas, le point est rejeté. Supérieur au seuil haut, le point est accepté comme formant un contour. Entre le seuil bas et le seuil haut, le point est accepté s'il est connecté à un point déjà accepté.*

La transformée de Hough :

La transformée de *Hough* est une technique qui peut être utilisée afin d'isoler des objets de formes géométriques simples dans l'image. En général, on se limite aux lignes, cercles ou ellipses présents dans l'image. L'un des grands avantages de la transformée de *Hough* est qu'elle est tolérante aux occlusions dans les objets recherchés et demeure relativement inaffectée par les bruits [Masek, 2003].

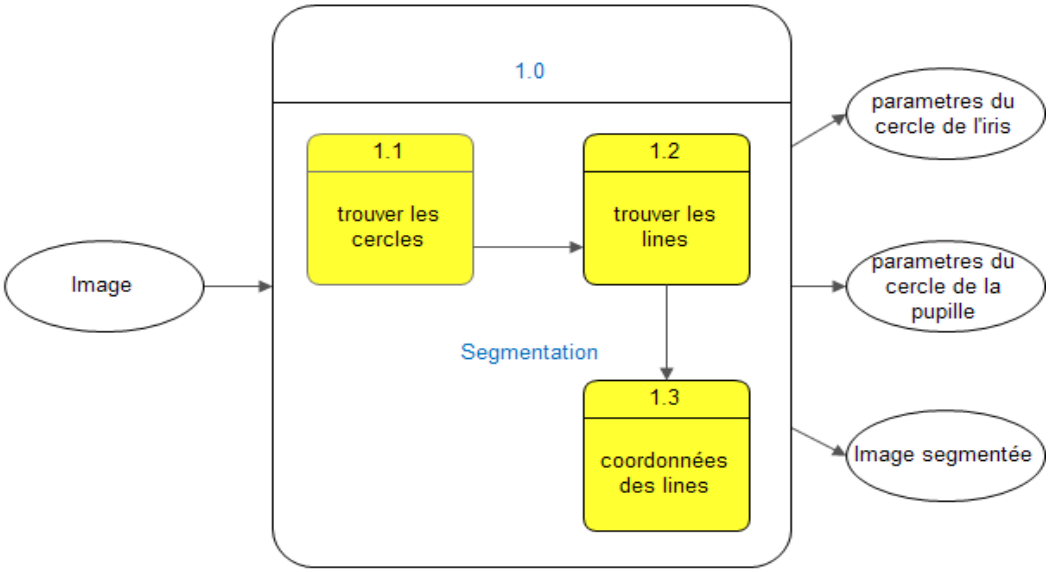


Figure 8.5 : DFD des principales étapes de segmentation.

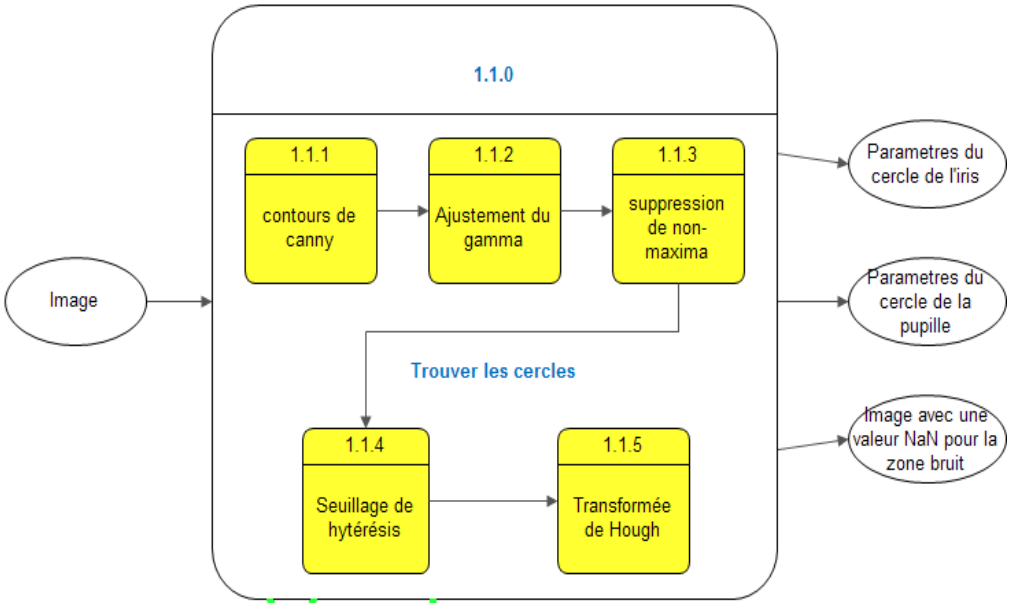


Figure 8.6 : DFD pour la procédure utilisée pour trouver les cercles.

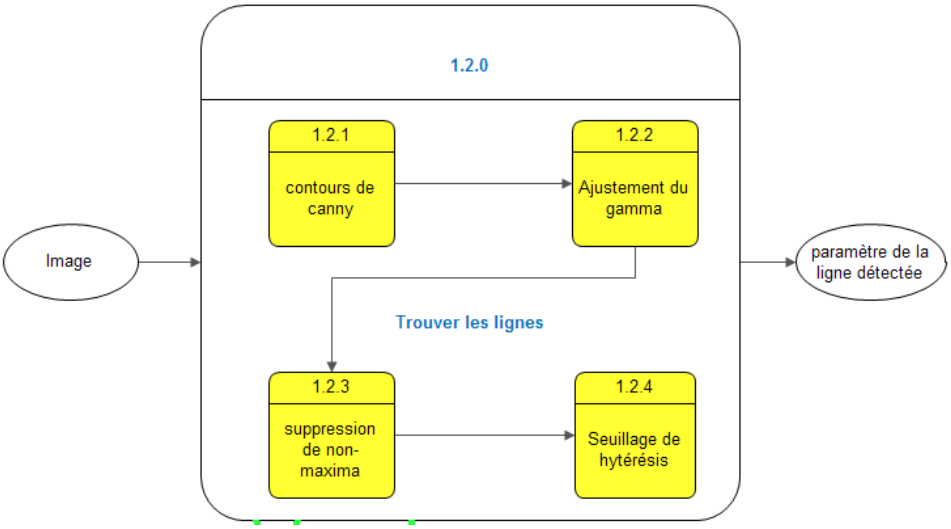


Figure 8.7 : DFD de la procédure suivie pour trouver les droites.

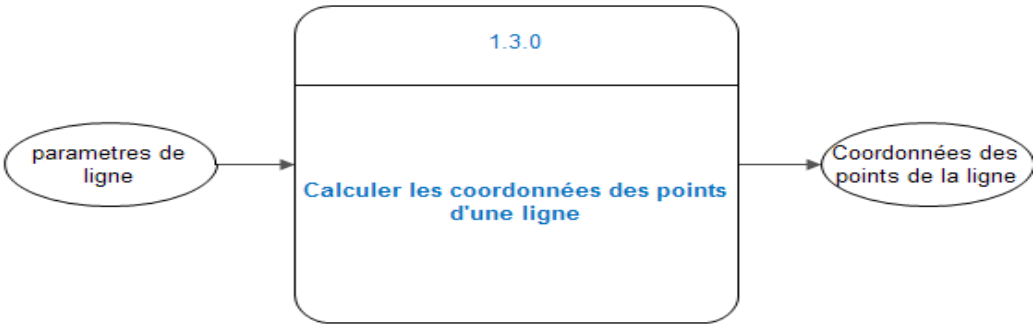


Figure 8.8 : DFD de la procédure de calcul de coordonnées des points d'une ligne.

Maintenant nous présentons l'algorithme de la transformée de *Hough* pour la détection de cercle :

L'algorithme de la transformée de Hough pour la détection des cercle :

Pour chaque point de contour du cercle
Pour chaque rayon r

1. Dessiner un cercle en prenant ce point comme le centre.

2. Incrémenter la valeur de tous les points, sur lesquels ce cercle passe dans La matrice de l'accumulateur.

3. Chercher une ou plusieurs valeurs maximales dans la matrice de l'accumulateur.

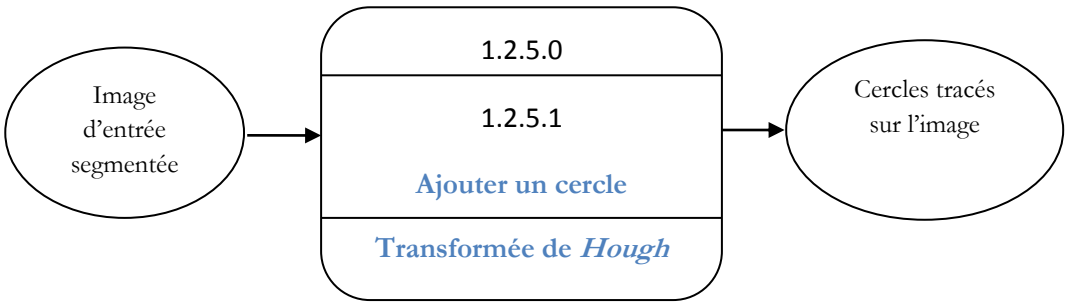


Figure 8.9 : DFD de la transformée de *Hough*.

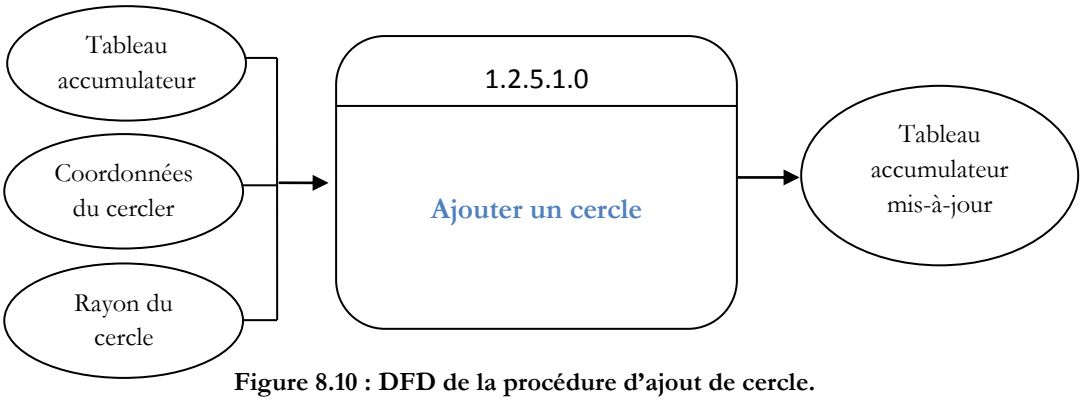


Figure 8.10 : DFD de la procédure d'ajout de cercle.

Les Figures 8.11**,** 8.12 et 8.13 présentent les DFD des opérations de prétraitement avant l'application de *Canny*.

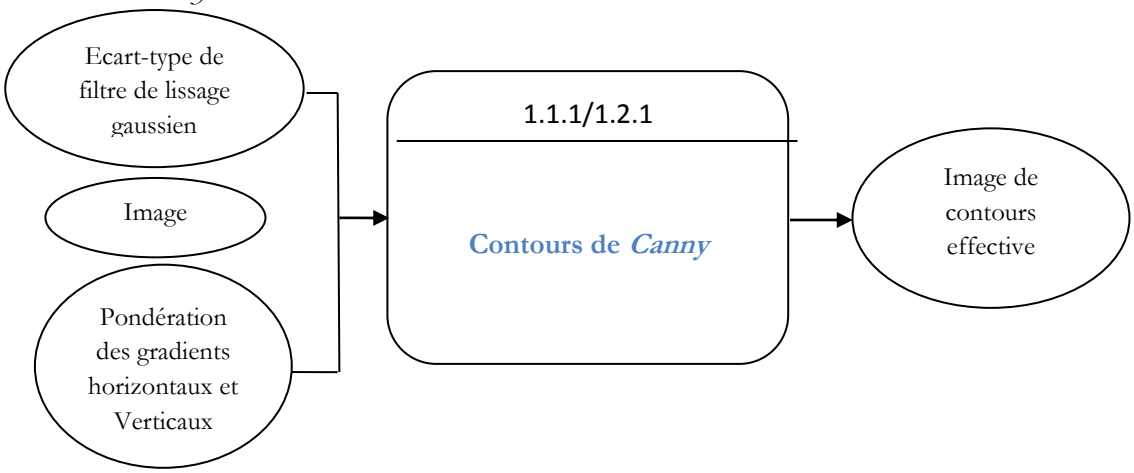


Figure 8.11 : DFD de la l'algorithme de contour de *Canny*.

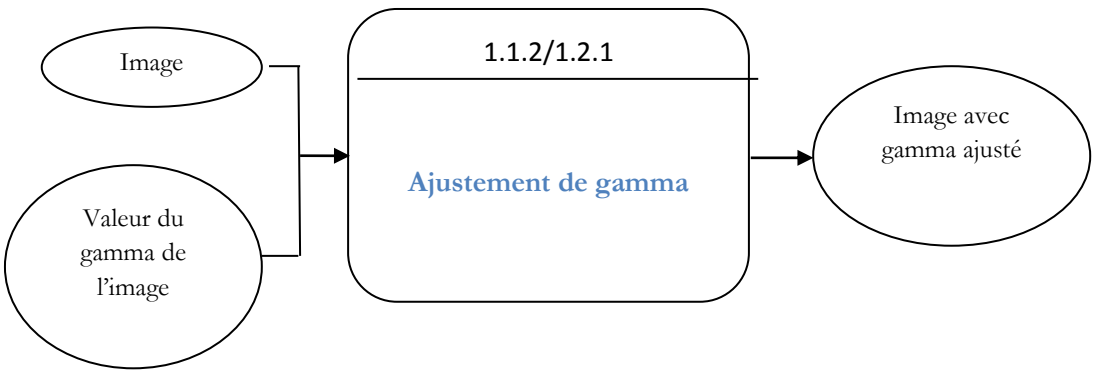


Figure 8.12 : DFD de la procédure d'ajustement du *gamma*.

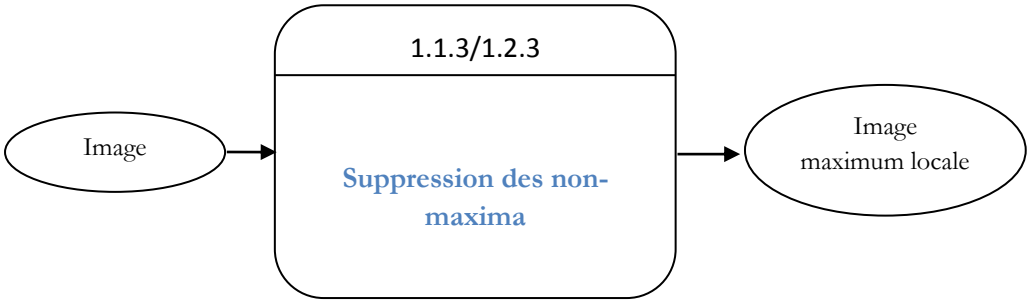


Figure 8.13 : DFD de la procédure des suppression des *non-maxima*.

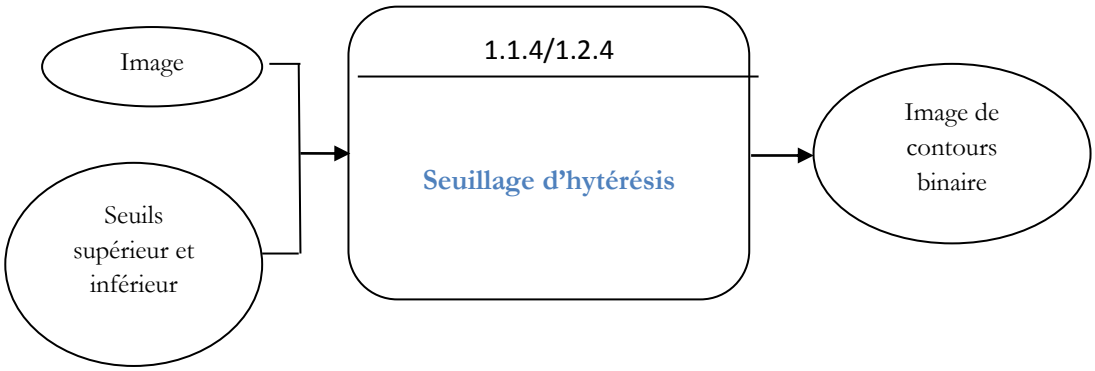


Figure 8.14 : DFD de la procédure d'obtention d'une image de contours binaire.

8.5.1.3. Normalisation et codage

Algorithme de Normalisation (méthode pseudo-polaire):

Le dépliage de l'iris s'effectue comme suit :

1. Découpage de l'iris en zones circulaires, le nombre de cercles dépend de la taille en pixels de l'image d'iris et de celle des zones circulaires, à titre d'exemple : 32 zones circulaires sur les images de taille 280 x 320 pixels

2. Choix d'un nombre de points fixes équidistants dans chaque cercle (à titre d'exemple : 240 points), sur lesquels une interpolation linéaire est appliquée

3. Cette transformation est faite conformément au modèle de normalisation de John Daugman. Elle permet le passage d'une représentation par coordonnées cartésiennes vers une représentation polaire (r, θ) *où* r *est dans l'intervalle [0,1] et* θ *est dans l'intervalle [0,2π]*

Le passage de la représentation cartésienne à la représentation polaire rectangulaire est modélisé par la formule :

$$I(x(r,\theta),y(r\theta)) \rightarrow (r,\theta) \quad (8.1)$$

Avec $(r,\theta) = (1-r)x_p(\theta) + rx_l(\theta), y(r,\theta) = (1-r)y_p(\theta) + ry_l(\theta)$

Où $I(x,y)$ est la région de l'image d'iris, (x,y) sont les coordonnées cartésiennes initiales, (r,θ) sont leurs coordonnées polaires correspondantes dans l'image normalisée, x_p ,y_p ,x_l ,y_l , sont les coordonnées des contours de la pupille et de l'iris respectivement le long de la direction .

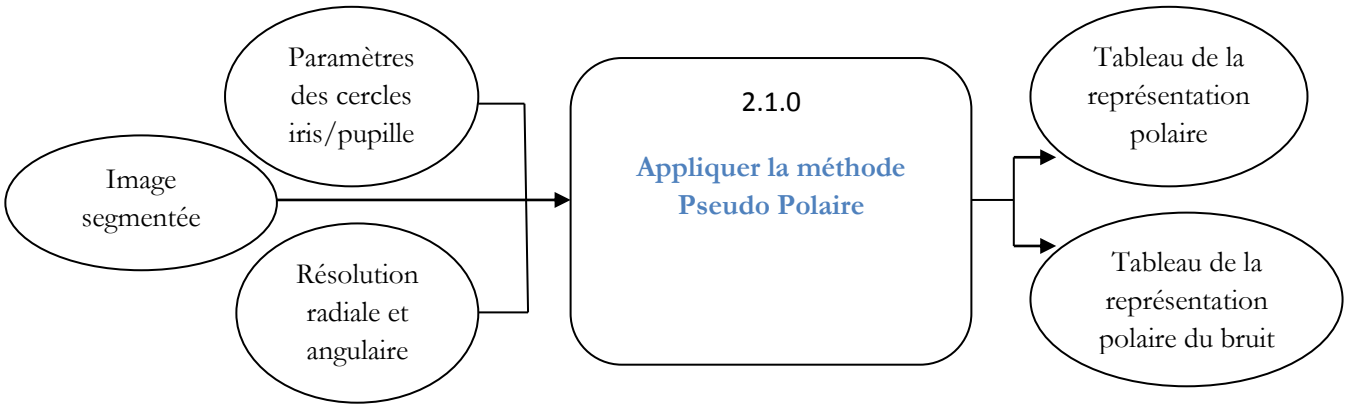


Figure 8.15 : DFD de la normalisation par la méthode *pseudo polaire*.

8.5.1.4. Encodage /Extraction des caractéristiques (*Ondelettes* de *Log-Gabor*)

Le codage consiste à appliquer les ondelettes de Log-Gabor. Le processus de codage produit un modèle binaire contenant un nombre de bits d'information, et un masque du bruit correspondant qui correspond aux zones corrompues au sein du motif de l'iris, et marque les bits dans le modèle comme étant corrompus. Tant que l'information de phase sera dénuée de sens au niveau des régions où l'amplitude est égale à zéro, ces régions sont également marquées dans le masque de bruit. Le nombre total de bits dans le modèle sera « la résolution angulaire multipliée par la résolution radiale, fois 2, multiplié par le nombre de filtres utilisés ».

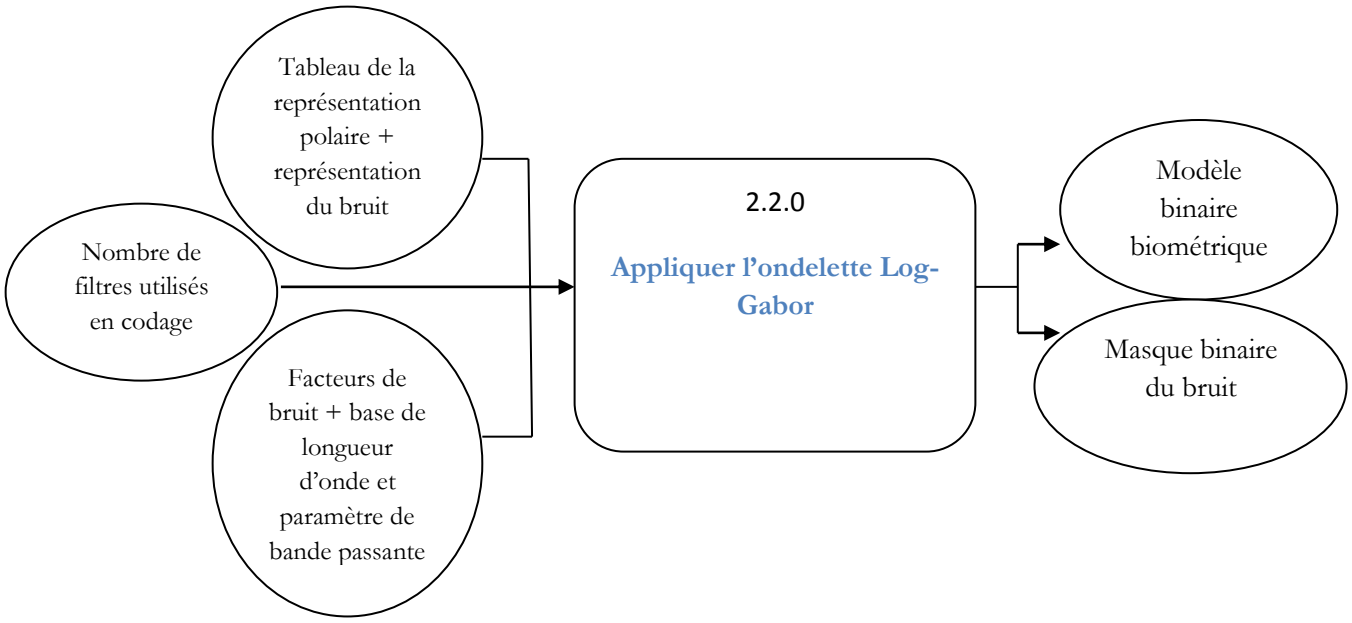


Figure 8.16 : DFD de l'encodage par l'*ondelette* de *Log Gabor*.

8.5.2. Le module de reconnaissance d'empreinte

La reconnaissance d'individus par empreintes digitales a été adressé par plusieurs recherches depuis la naissance de l'informatisation dans le monde, et jusqu'à aujourd'hui les travaux ne cessent de présenter le meilleur pour une bonne et robuste identification.

8.5.2.1. Schéma général du système

La figure 8.17 présente la chaine des étapes de la reconnaissance par empreinte digitale basée sur la détection des minuties.

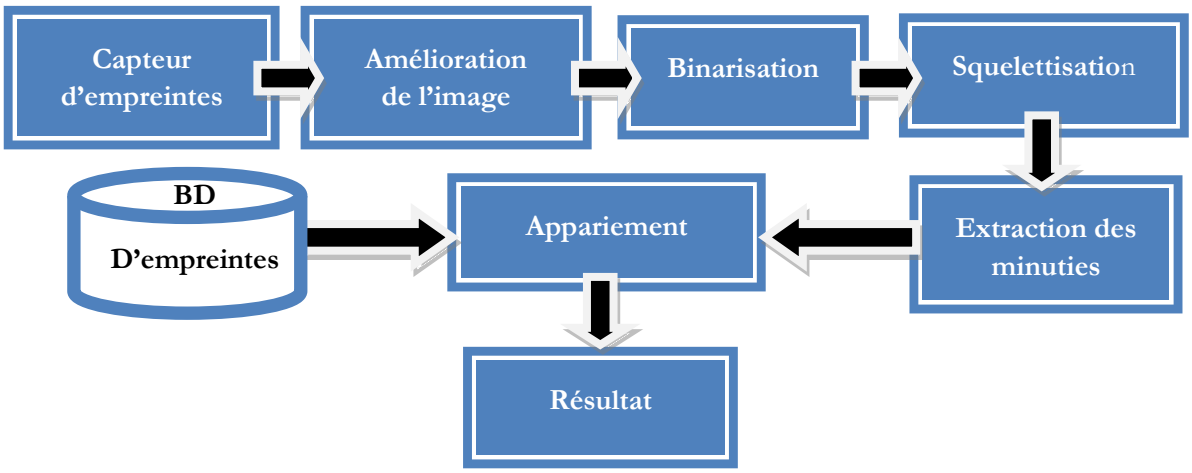


Figure 8.17 : Schéma présentant la chaîne du scan de l'image de l'empreinte jusqu'à l'authentification.

Nous avons choisi d'extraire les information biométriques des empreintes en utilisant l'approche par détection des minuties pour sa simplicité et facilité d'implémentation (l'autre approche est l'approche de texture), cette approche est la plus utilisée par les travaux de recherches, son seul inconvénient se voit lors de l'utilisation des images fortement bruitées, là ou les minuties sont complètement non repérés, cet inconvénient est pallié par l'amélioration de l'image en prétraitement, cette phase entrainera l'identification de fausses minuties ce qui exige l'étape du post traitement pour les éliminé.

Pour ce faire, nous utilisons l'algorithme de Jagadeesan et al [Jagadeesan et al., 2010] pour la localisation de la région d'intérêt et le champ d'orientation, l'algorithme de Jain et al. [Jain et al., 1997] pour l'extraction de minuties et le post traitement.

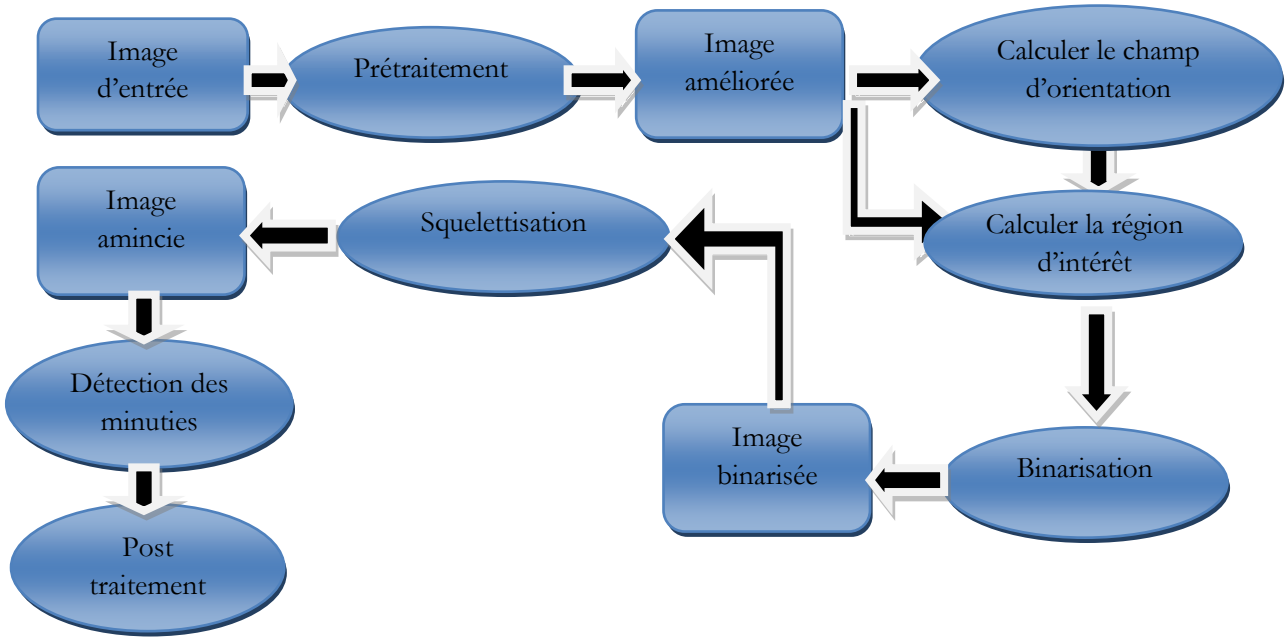


Figure 8.18 : DFD des principales étapes du système de reconnaissance d'empreintes.

8.5.2.2. Les étapes du traitement

1. Phase du ***prétraitement*** : Dans cette phase nous utilisons l'égalisation par histogramme.
2. Phase du calcul du champ d'orientation et de la région d'intérêt : Le champ de l'orientation de l'empreinte détermine l'orientation locale des stries contenues dans l'empreinte. L'estimation des orientations locales est une phase importante dans le processus de prétraitement.
3. Phase de ***binarisation*** : Son algorithme transforme l'image en entrée en une image binaire.
4. Phase de ***squelettisation*** « *thinning* » : Son algorithme amincie les dimension des crêtes.
5. Phase ***d'extraction de minuties*** : L'extraction des minuties est réalisée selon l'approche par détection de minuties de Jain [Jain et al., 1997].
6. Phase du ***post traitement*** : Son rôle est l'élimination des fausses minuties engendrées éventuellement par l'algorithme d'extraction des minuties.

8.5.3. Le module d'appariement

8.5.3.1. L'appariement dans les modules de reconnaissance monomodale

Concernant les modules de reconnaissance monomodaux (l'iris et l'empreinte), l'appariement se fera en utilisant :

- **La distance de *Hamming* pour la reconnaissance de l'iris**

L'algorithme de distance de *Hamming* employé intègre également le masquage du bruit, de sorte que seuls les bits significatifs sont utilisés dans le calcul de la distance de *Hamming* entre les deux modèles d'iris. Maintenant lorsqu'on prend la distance de *Hamming*, seuls les bits dans le motif de l'iris qui correspondent aux bits '0' dans les masques de bruit des deux motifs d'iris à la fois seront utilisés dans le calcul. La distance de *Hamming* sera calculée en utilisant seulement les bits générés par la vraie région de l'iris, et la formule de la distance de *Hamming* est la suivante :

$$HD = \frac{\sum_{j=1}^{N} X_j (XOR) Y_j (AND) Xn'_j (AND) Yn'_j}{N - \sum_{k=1}^{N} Xn_k (OR) Yn_k} \qquad (8.1)$$

Où X_j et Y_j sont les deux modèles à comparer bit a bit, et Xn_j et Yn_j sont les masques de bruit correspondant pour X_j et Y_j, et N est le nombre de bits représentés par chaque modèle. Bien que, en théorie, deux modèles d'iris générés à partir du même iris auront une distance de *Hamming* de 0.0, en pratique cela ne se produira pas parce que La normalisation n'est pas parfaite, et aussi il y aura quelques bruits qui passent inaperçus, donc une certaine variation sera présente lors de la comparaison des deux modèles intra-classe d'un iris.

- **La distance *Euclidienne* pour la reconnaissance d'empreinte**

La distance *Euclidienne* permet d'évaluer la proximité de deux vecteurs de même dimension suivant la formule suivante :

$$DE = \sqrt{\sum_{i=1} (Xi - Yi)^2} \qquad (8.2)$$

Où X_i et Y_i sont les deux modèles à comparer.

8.5.3.2. L'appariement dans le module de fusion d'iris et d'empreinte

Notre approche fait appel à trois méthodes différentes d'appariements par fusion de scores qui sont :

1. L'appariement par la méthode de la *Somme Linéaire* « *Sum Rule* »

Après la normalisation des scores d'empreinte et d'iris, le score de fusion sera calculé comme suit :

$$S' = \sum_{i=1,n} S \qquad (8.3)$$

n est le nombre de scores, ici n = 2.

2. L'appariement par la méthode de la somme linéaire pondérée « Wheigted Sum Rule »

Après la normalisation des scores d'empreinte et d'iris, le score de fusion sera calculé comme suit :

$$S' = \alpha S_1 + (1 - \alpha) S_2 \qquad (8.4)$$

La pondération par des poids de scores provenant de traits biométriques différents indique l'importance de chaque score par rapport à la précision du trait biométrique et par conséquent la décision sera meilleure.

3. L'appariement par la logique floue

Notre système d'inférence floue ajuste le poids de pondération pour chaque trait biométrique (l'iris et l'empreinte) selon l'importance de chaque trait (ici le score de l'iris est plus confiant que celui de l'empreinte) et les règles floue produisent des décisions selon la distance d'appariement calculée pour chaque trait biométrique.

Donc :

- On définit deux variables floues d'entrée : '*finger*' pour l'empreinte et '*iris*' pour l'iris.
- On définit une variable floue de sortie : '*fusion*'
- Chaque variable sera modélisée par un ensemble flou.
- Le type de l'ensemble flou utilisé est l'ensemble flou trapézoidal.
- On définit trois ensembles flous selon la distance d'appariement : *mauvais*, *moyen*, *bon*.
- La sortie floue sera : *très mauvais*, *mauvais*, *moyen*, *bon*, *très bon*, *excellent*.

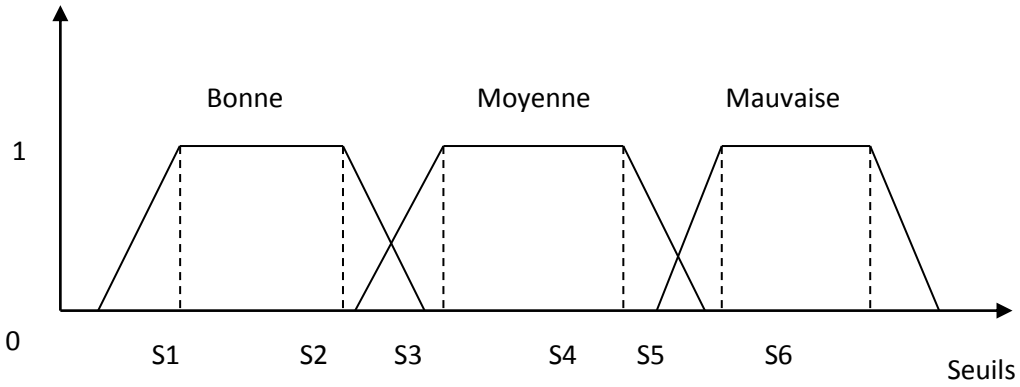


Figure 8.19 : Ensembles flous et Fonctions d'appartenances selon les seuils.

[S1, S2] c'est l'intervalle de seuils où l'image appartient à l'ensemble flou « Bonne ».

[S3, S4] c'est l'intervalle de seuils où l'image appartient à l'ensemble flou « Moyenne ».

[S5, S6] c'est l'intervalle de seuils où l'image appartient à l'ensemble flou « Mauvaise ».

Ces intervalles de seuils seront déterminés avec précision dans le chapitre d'implémentation, après avoir déroulé des tests intensifs et exhaustifs sur les bases de données utilisées.

- **Les règles floues**

La fusion des résultats d'appariement suit les règles floues suivantes :

Règle1 : Si (Finger est *mauvais*) et Iris est *mauvais*) alors (Fusion est *très mauvais*)

Règle 2 : Si (Finger est *mauvais*) et (Iris est *moyen*) alors (Fusion est *moyen*)

Règle 3 : Si (Finger est *mauvais*) et (Iris est *bon*) alors (Fusion est *très bon*)

Règle 4 : Si (Finger est *moyen*) et (Iris est *mauvais*) alors (Fusion est *mauvais*)

Règle 5 : Si (Finger est *moyen*) et (Iris est *moyen*) alors (Fusion est *bon*)

Règle 6 : Si (Finger est *moyen*) et (Iris est *bon*) alors (Fusion est *très bon*)

Règle 7 : Si (Finger est *bon*) et (Iris est *mauvais*) alors (Fusion est *moyen*)

Règle 8 : Si (Finger est *bon*) et (Iris est *moyen*) alors (Fusion est *très bon*)

Règle 9 : Si (Finger est *bon*) et (Iris est *bon*) alors (Fusion est *excellent*)

Le paragraphe suivant donnera plus de détails sur les valeurs de poids fixés pour chaque variable floue ainsi que les valeurs des distances d'appariements en relation avec chaque ensemble flou.

8.6. Résultats expérimentaux

Les tests ont été réalisés sur un PC portable HP 630 Processeur Intel CORE I3 CUP M370 de vitesse 2.4 GHz, avec 2 Giga octet de mémoire vive, et un disque dur de 320 Giga octet. La configuration minimale pour l'application est 512 Méga octet de RAM et 80 Giga octet de disque dur.

- **Le langage de programmation utilisé est Matlab 7.10.0.**

MATLAB et son environnement interactif est un langage de haut niveau qui permet l'exécution de tâches nécessitant une grande puissance de calcul, Il dispose de plusieurs

boites à outils en particulier celle du traitement d'images « *Image Processing ToolBox* » qui propose un ensemble d'algorithme et d'outils graphiques de référence pour le traitement, l'analyse, la visualisation et le développement d'algorithmes de traitement d'images. Ce langage possède également des outils de représentation et de traitement de la logique floue.

- **Les bases de données utilisées sont :**
  1. Base de données d'iris : CASIA-IRIS V1, CASIA-IRIS V2.
  2. Base de données d'empreintes digitales : FVC 2004.
  3. Base de données multimodale : conçue à partir d'un nombre égal d'images d'iris de CASIA-IRIS V2 et d'images d'empreintes de FVC 2004 (4 images). La taille de la base est 500 images.

8.6.1. Description des Bases de données utilisées

8.6.1.1. CASIA-Iris V1

Afin de promouvoir la recherche, le Laboratoire de reconnaissance des formes [CASIA1], Laboratory of Pattern Recognition (NLPR), Institut d'Automatisation (IA), l'Académie chinoise des Sciences (CAS) est le premier centre de recherche qui a fournit une base de données « CASIA » des Iris gratuitement à la demande pour les chercheurs de reconnaissance d'Iris, sur laquelle une partie de ce travail a été effectué. Les images Iris de CASIA version 1.0 (CASIA-IrisV1) ont été capturées avec un appareil photo fabriqué par le centre CASIA. Cet appareil photo constitué de Huit enlumineurs de 850nm, sont disposées circulairement autour du capteur afin d'assurer que l'Iris est uniformément et convenablement éclairé. Cette base de données est organisée sur 108 classes avec 7 instances par classes, soit au total 756 images d'iris. Les régions de pupilles de toutes les images d'Iris dans CASIA-IrisV1 ont été automatiquement détectée et remplacée par une zone circulaire d'intensité constante, pour masquer la réflexion spéculaire de la réflexion de la lumière sur les images avant la mettre à la disposition des chercheurs.

8.6.1.2. CASIA-Iris V2

Cette base inclue 2400 images de 120 classes d'yeux différentes. La base de données CASIA-Iris V2 inclut des images floues, avec différentes illuminations et le port des lunettes est autorisé. La résolution des images pour cette base est de 640*480 pixels. Cette base de données présente aussi la caractéristique particulière d'avoir été acquise avec deux capteurs différents le capteur OKI et le capteur Pattek.

8.6.1.3. FVC 2004

Quatre bases de données différentes (DB1_A, DB2_A, DB3_A et DB4_A), étaient conçues par l'utilisation des capteurs suivants :

DB1_A : capteur optique "V300" du CrossMatch.
DB2_A : capteur optique "U.are.U 4000" du Digital persona.
DB3_A : capteur thermique "FingerChip FCD4B14CD" du Atmel.

DB4_A : générateur des empreintes digitales synthétiques "SFinGe v3.0".

Chacune de ces bases de données contient 800 empreintes l'équivalent de cent (100) individus pour huit (08) essais.

Tableau 8.2 : Description de la base de données FVC2004.

	Type du capteur	Taille de l'image	Résolution	Nb d'empreintes
DB1_A	Capteur optique	640x480	500 dpi	800
DB2_A	Capteur optique	328x364	500 dpi	800
DB3_A	Capteur thermique	300x480	500 dpi	800
DB4_A	SFinGe v3.0	288x384	500 dpi	800

8.6.2. Motivation du choix de ces bases de données

La majorité des travaux de recherche sur l'iris portent leurs résultats sur la base de donnée CASIA –iris avec ses différentes versions, nous avons également noté que les articles scientifiques récents sur la reconnaissance des empreintes digitales présentent leurs résultats en utilisant les bases de données publiques collectées dans les compétitions de vérification d'empreinte FVC « *Fingerprint Verification Competition* ». Les Campagnes FVC (2000, 2002, 2004 et 2006) [Maio et al., 2000] [Maio et al., 2002] [Maltoni et al., 2004] ont été organisés dans le but de fournir tout chercheur intéressé par les bases de données d'empreintes digitales et de suivre la performance des algorithmes de la « state-of-the-art » d'empreintes digitales correspondants [Maltoni et al., 2009].donc l'utilisation de ces bases de données nous permet de comparer nos résultat avec celles rapportés par les chercheurs de la biométrie.

Une autre motivation pour notre choix de la base de données d'empreinte la FVC 2004 : cette base présente des empreintes digitales de mauvaise qualité (nombre non confident de minutie, mal capture de l'image d'empreinte, région d'intérêt « pattern area » non identifiée, image fortement bruitées), et ceci affecte beaucoup les résultats de la reconnaissance monomodale d'empreinte digitale en terme de la précision de la reconnaissance «*system accuracy* », et les taux d'erreurs relatives aux client imposteurs TFA et aux clients authentique TFR. Donc fusionner ces résultats avec celles d'un système biométrique monomodal agissant sur un autre trait biométrique plus robuste comme l'iris donnera éventuellement de meilleurs résultats.

8.6.3. Répartition de la base de données

Les bases de données utilisées par nos tests sont CASIA-Iris V1, CASIA-Iris V2 et FVC 2004.
La base de données CASIA-IrisV1 contient 756 images d'iris. Notre base de données sera répartie comme suit :

- 40% de la base de données, est réservé pour l'apprentissage, c'est-à-dire l'estimation des paramètres du modèle (classificateur).
- 60% de la base de données est utilisé comme ensemble de test. Cet ensemble qui n'a pas était utilisé dans l'élaboration du meilleur modèle (classificateur),

permet de déterminer la performance du meilleur modèle sélectionné dans la phase de validation.

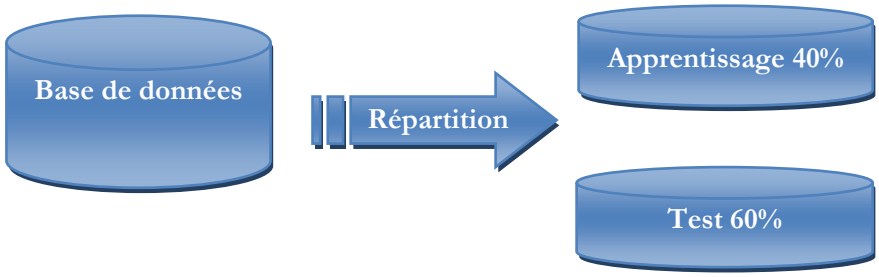


Figure 8.20 : Répartition de la base de données.

8.6.4. Les distributions intra classe et inter classes

Pour une base donnée quelconque, si c représente le nombre de classes, et n représente le nombre total d'images par classe, donc les combinaisons intra-classes sont calculées ainsi :

(n-1 x (n / 2) × c) [Abhyankar & Schuckers, 2010]

et les combinaisons interclasses sont calculées comme suit :

(c × (c -1) × n × n) [Abhyankar & Schuckers, 2010].

Par exemple, pour la base CASIA V1, les combinaisons intra-classes sont ((7-1) × (7/2) × 108)= 2268 et les combinaisons interclasses sont (108 × 107 × 7 × 7) = 566244.

Pour la base de données CASIA –V2, les combinaisons intra-classes sont ((20-1) × (20/2) × 120) = 22800 et les combinaisons interclasses sont (120 × 119× 20× 20) = 5712000.

pour la base de données FVC 2004, les combinaisons intra-classes sont ((800-1) × (800/2) × 4) = 1278400 et les combinaisons interclasses sont (4 × 3 × 800× 800) =7680000.

8.6.5. Résultats de la reconnaissance d'empreinte digitale

La figure 8.21 présente l'interface graphique de l'application permettant de réaliser la reconnaissance de l'empreinte digitale selon deux modes opératoires :

- **Le mode de vérification** : l'utilisateur choisi deux images d'empreintes de la base de sonnées, effectue la segmentation, visualise les minuties, puis le système affiche le résultat de la vérification « authentique » ou « imposteur » avec la distance d'appariement calculée.
- **Le mode d'identification** : l'utilisateur choisi une image de l'ensemble d'échantillon d'images réservé pour le test, ensuite il effectue la segmentation, visualise les minuties, et le système affichera le résultat de l'identification avec le seuil de décision.

L'utilisateur peut également visualiser les résultats graphiques de la binarisation, la squelettisation, les fausses minuties et les vraies minuties sur l'image de l'empreinte sélectionnée.

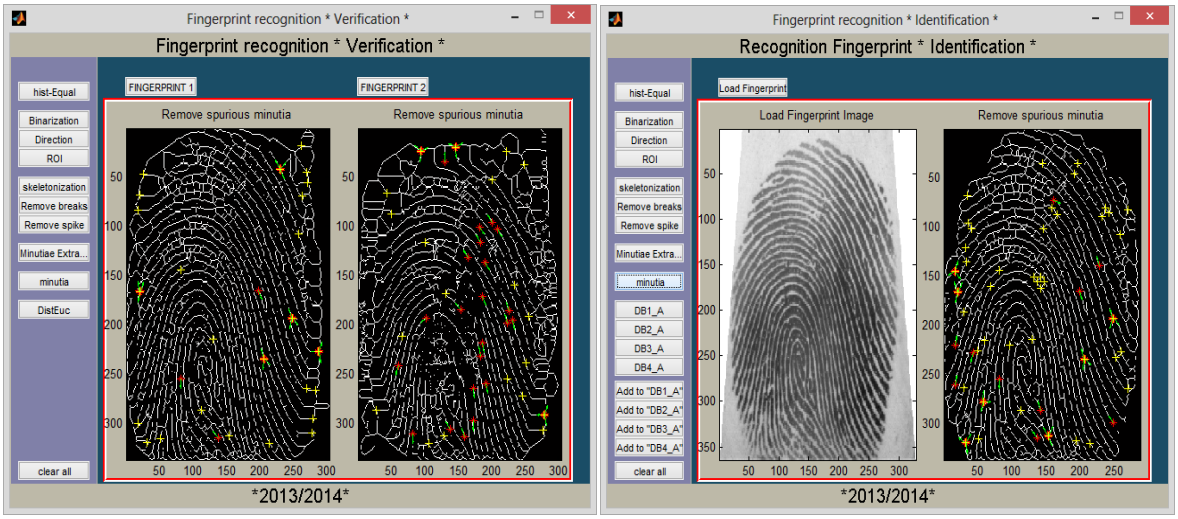


Figure 8.21 : L'interface graphique du système permettant de réaliser la reconnaissance d'empreinte digitale selon deux modes opératoire (la vérification et l'identification).

En effectuant des tests exhaustives sur 60% de la base de données d'empreintes digitales FVC 2004 (40% de la base est réservé à l'apprentissage), nous avons pu voir à quoi ressemble le nuage de points relative aux appariements authentiques et imposteurs (Cf. figure 8.22).

Il est à noter que

- Le but fondamental de tout système biométrique opérant au niveau score, est de pouvoir séparer au maximum les distributions de score des imposteurs et des authentiques.
- En minimisant la zone de recouvrement entre ces deux distributions, on améliore la performance globale du système en augmentant le taux de reconnaissance.

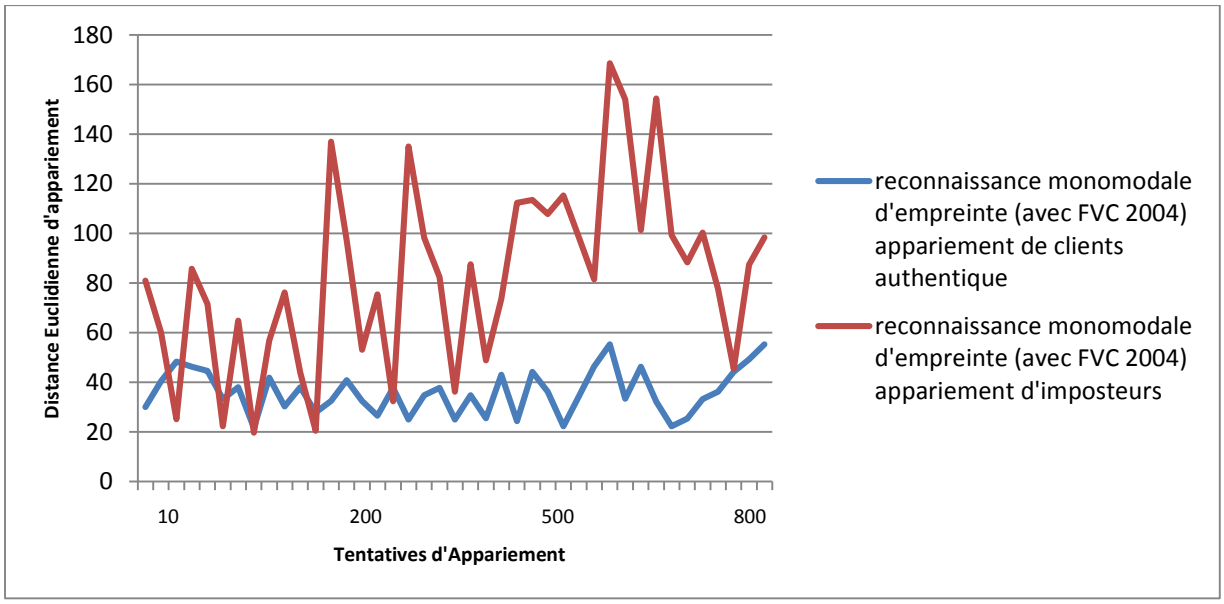


Figure 8.22 : Courbes d'appariement de clients authentiques et d'imposteurs de la reconnaissance monomodale d'empreinte en utilisant FVC2004

8.6.6. Résultats de la fusion par la *somme linéaire*

La figure 8.23 présente l'interface graphique de l'application permettant de réaliser la reconnaissance multimodale d'iris et d'empreinte. La fusion est effectuée par la *somme linéaire* des scores. L'interface graphique de l'application permet de visualiser les étapes de la segmentation et de l'appariement des deux modalités.

Comme les scores ne sont pas normalisés, une étape de normalisation par l'algorithme *Min-Max* est nécessaire.

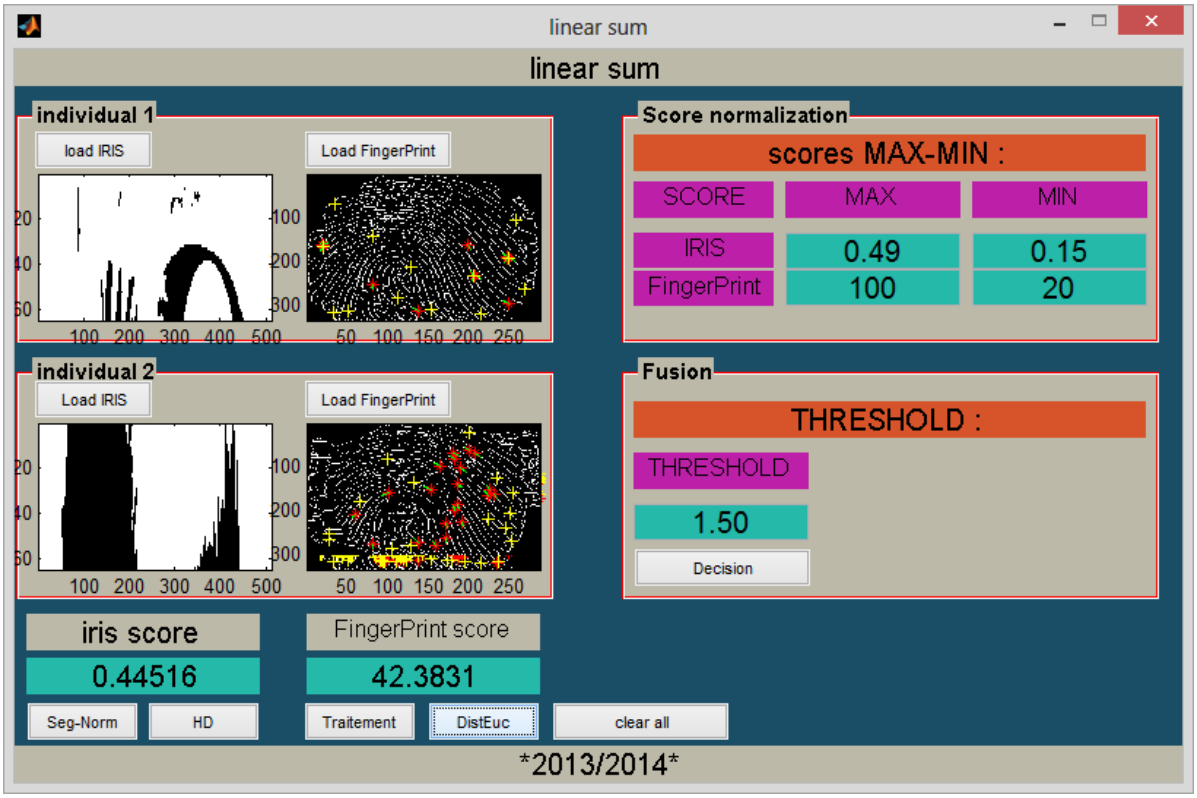


Figure 8.23 : Interface graphique de l'application permettant de réaliser la fusion par la *somme linéaire*

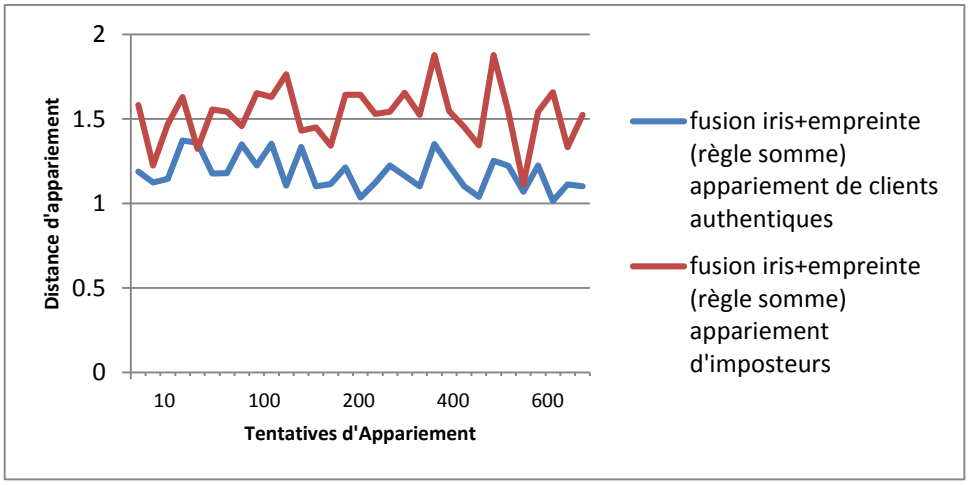


Figure 8.24 : Courbes d'appariements de clients authentiques et d'imposteurs de la reconnaissance multimodale en utilisant l'appariement par la *somme linéaire*.

8.6.7. Résultats de la fusion par la *somme linéaire pondérée*

La figure 8.25 présente l'interface graphique de l'application permettant de réaliser la reconnaissance multimodale d'iris et d'empreinte. La fusion est effectuée par la *somme linéaire* des scores.

Comme les scores ne sont pas normalisés, une étape de normalisation par l'algorithme *Min-Max* est nécessaire.

L'interface graphique de l'application permet de visualiser les étapes de la segmentation et de l'appariement des deux modalités.

Les paramètres α et β de la *Somme Linéaire Pondérée* sont fixés par l'utilisateur.

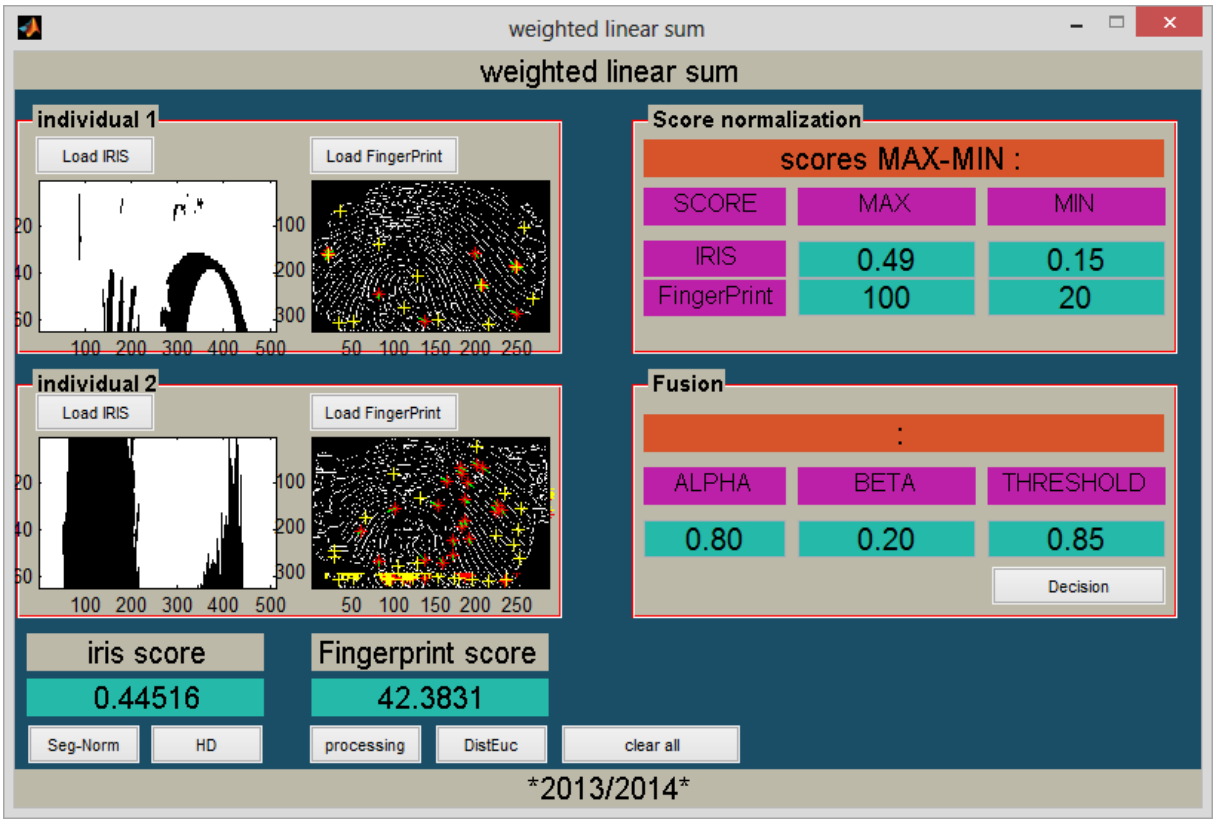


Figure 8.25 : Interface graphique de l'application permettant de réaliser la fusion par la *somme linéaire pondérée*.

Les distributions interclasses et intra-classes relatives à la reconnaissance de la fusion par la *Somme Linéaire Pondérée* sont présentées dans la figure 8.26.

On remarque que Les zones de recouvrement entres la distribution des clients authentique et celle des imposteurs sont minimes.

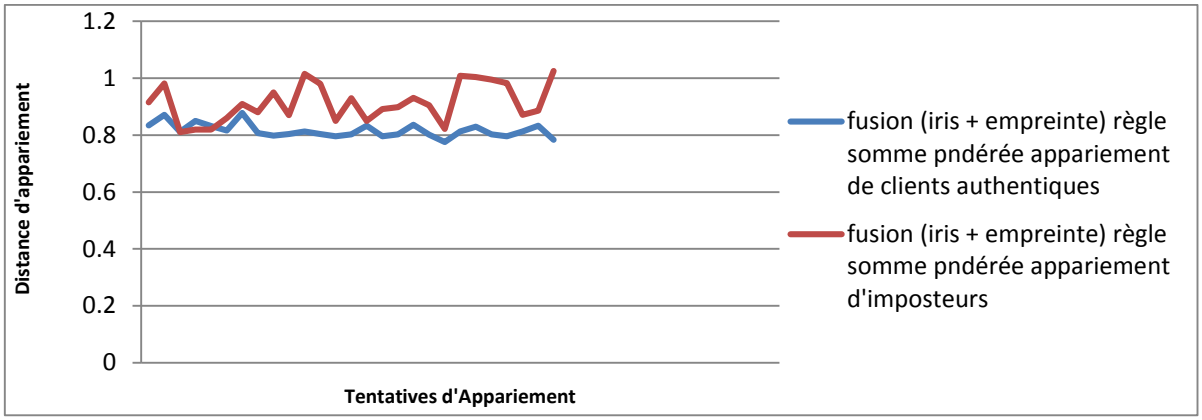


Figure 8.26 : Courbes d'appariements de clients authentiques et d'imposteurs de la reconnaissance multimodale en utilisant l'appariement par la *Somme Linéaire Pondérée*.

8.6.8. Résultats de la fusion par *la logique floue*

La figure 8.27 présente l'interface graphique de l'application permettant de réaliser la reconnaissance multimodale d'iris et d'empreinte. La fusion est effectuée par la *Logique Floue*.

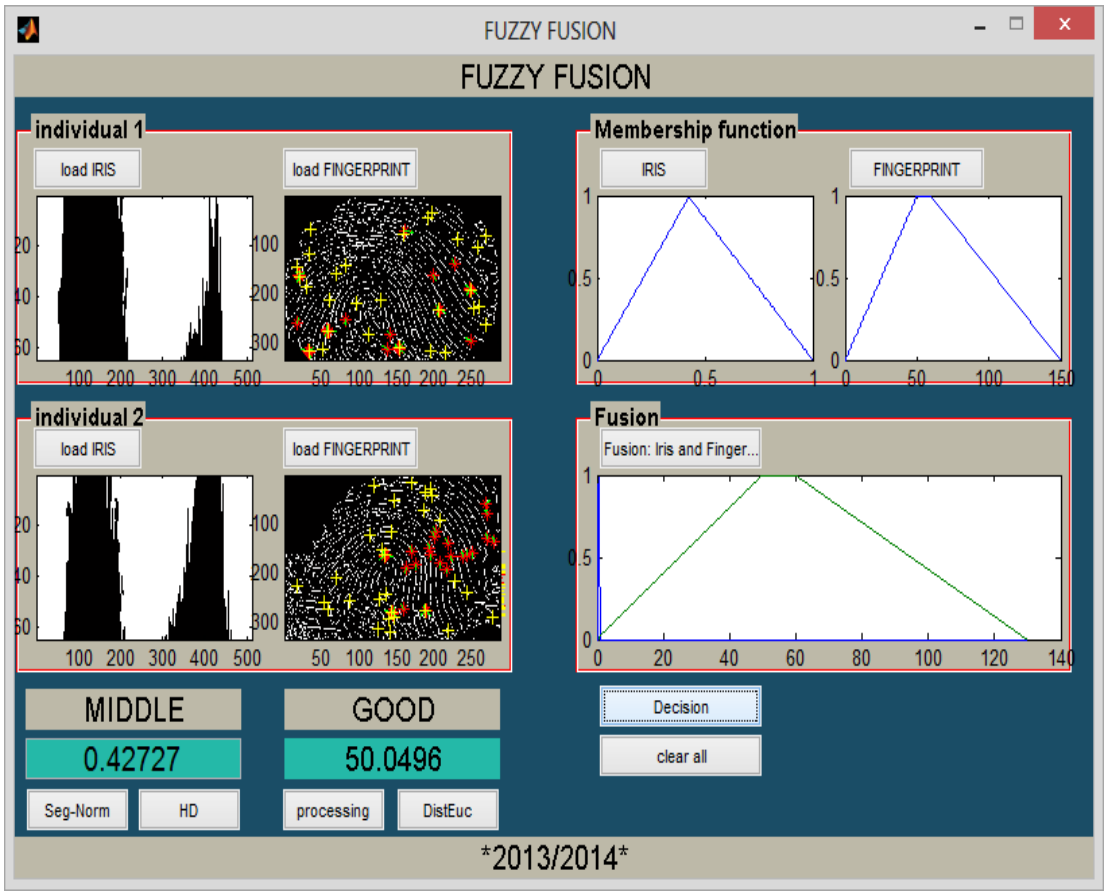


Figure 8.27 : Interface graphique de l'application permettant de réaliser la fusion par la *Logique Floue*.

Comme le montre la figure 8.27, les scores ne sont pas utilisés, seulement les décisions sont prises en compte. Les variables linguistiques floues représentent chaque décision du système. Ces variables sont représentées par des ensembles flous.

Les distributions interclasses et intra-classes relatives à la reconnaissance de la fusion par la *Logique Floue* sont présentées par le tableau 8.3.

Tableau 8.3 : Exemple de distributions intra-classes et interclasse de la reconnaissance multimodale en utilisant l'appariement par la logique floue.

	Individu 1			Individu 3		
Individu 1	bon	bon	moyen	mauvais	très mauvais	mauvais
	Très bon	bon	moyen	moyen	mauvais	très mauvais
Individu 2	très mauvais	moyen	très mauvais	mauvais	mauvais	mauvais
	moyen	mauvais	moyen	moyen	moyen	mauvais
Individu 3	moyen	mauvais	mauvais	bon	bon	bon
	Mauvais	Très mauvais	mauvais	Très bon	Moyen	Très bon
Individu 4	Mauvais	Mauvais	très mauvais	Très mauvais	Moyen	Moyen
	mauvais	mauvais	mauvais	Mauvais	Mauvais	mauvais
Individu 5	très mauvais	Moyen	Mauvais	Très mauvais	Mauvais	Mauvais
	Mauvais	Mauvais	très mauvais	Mauvais	Mauvais	Mauvais

La décision « moyen » signifie que

- soit la reconnaissance d'empreinte est « mauvaise » et la reconnaissance d'iris est « moyenne »
- soit la reconnaissance d'empreinte est « bonne » et la reconnaissance d'iris est « mauvaise »

Si on accepte la décision « moyen » comme étant une reconnaissance vraie de l'individu donc on aura :

TFA =0.16 et TFR =0.0

Si on rejette les décisions « moyen » on aura :

TFA =0.0 et TFR =0.05

Donc on aura un Taux d'erreur égal TEE = 0.038.

8.6.9. Estimation du temps d'exécution

Le tableau 8.4 présente le Temps d'exécution d'appariement pour les différentes techniques de reconnaissance implémentées.

Tableau 8.4: Estimation du temps d'exécution de toutes les expériences par mode opératoire.

	Vérification (s)	Identification(s)
Expérience 1 : Iris (CASIA-Iris-V2)	0.155	0.298
Expérience 2 Iris (CASIA-Iris V1)	0.138	0.1797
Expérience 3 Empreinte (FVC2004)	0.087	0.15876
Expérience 4 Fusion (*Somme linéaire*)	0.256	/
Expérience 5 Fusion (*Somme linéaire pondérée*)	0.2487	/
Expérience 6 Fusion (*Logique Floue*)	**0.1754**	/

Les méthodes implémentées sont :

Expérience 1 : Reconnaissance monomodale d'iris avec CASIA-Iris V1.
Expérience 2 : Reconnaissance monomodale d'iris avec CASIA-Iris V2
Expérience 3 : Reconnaissance monomodale d'empreinte avec FVC2004.
Expérience 4 : Reconnaissance multimodale par *fusion de scores* avec la *somme linéaire*.
Expérience 5 : Reconnaissance multimodale par *fusion de scores* avec la *somme linéaire pondérée*.
Expérience 6 : Reconnaissance multimodale par *fusion de décisions* avec la *logique floue*.

On remarque que la méthode de reconnaissance la plus rapide concernant le temps d'appariement est la méthode de la reconnaissance monomodale d'empreinte digitale et cela est due principalement à l'utilisation de la distance *Euclidienne* dans la phase d'appariement.

On constate que le temps d'appariement par la fusion de décisions par la logique floue est meilleur que celui de la fusion de scores par la méthode de la somme linéaire et de la somme linéaire pondérée.

8.6.10. Estimation des taux d'erreur TFA , TFR et TEE

Tableau 8.5 : Estimation des taux TFA et TFR de la reconnaissance d'iris (CASIA-Iris V-1).

Seuil	0.20	0.25	0.30	0.35	**0.40**	0.45	0.50
TFA (%)	0.000	0.000	0.000	0.000	**0.005**	7.599	99.499
TFR (%)	99.047	82.787	37.880	5.181	**0.238**	0.000	0.000

Tableau 8.6 : Estimation des taux TFA et TFR de la reconnaissance d'iris (CASIA-Iris V-2).

Seuil	0.20	0.25	0.30	0.35	0.40	**0.45**	0.50
TFA (%)	0.000	0.000	0.000	0.000	0.01	**0.099**	99.499
TFR (%)	99.9	95.80	57.78	20.43	9.89	**4.09**	0.000

Tableau 8.7 : Estimation des taux TFA et TFR de la reconnaissance d'empreinte (FVC 2004).

Seuil	10	20	30	40	50	60	70	**80**	90	100
TFA (%)	0.000	0.005	0.10	0.60	10	13.43	13.95	**14.01**	67.87	90.89
TFR (%)	99	95.80	70.29	56.78	30.89	28.78	26.77	**15.98**	50.76	12.67

Tableau 8.8 : Estimation des taux TFA et TFR de la fusion par la *Somme Linéaire*.

Seuil	1.0	1.10	1.20	1.30	**1.40**	1.50	1.60	1.70	1.80	1.85	1.90
TFA (%)	0.000	0.08	0.90	2.7	**10**	12.83	20.95	45.01	70.87	92.81	99.98
TFR (%)	99.30	93.56	60.89	60.58	**26.89**	25.78	24.77	10.98	9.60	1.67	000

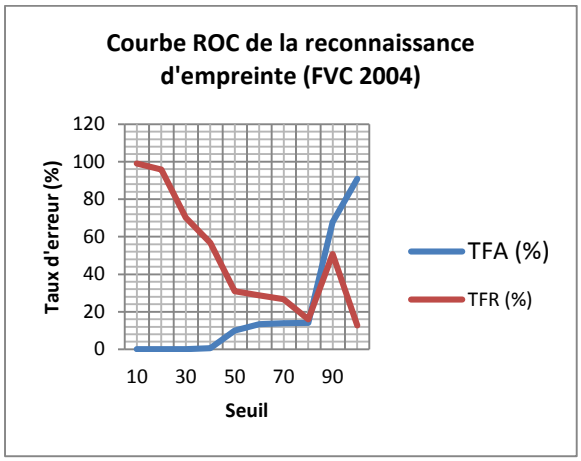
Tableau 8.9 : Estimation des taux TFA et TFR de la fusion par la *Somme Linéaire Pondérée*.

Seuil	0.7	0.75	0.78	0.80	**0.83**	0.85	0.88	0.90	0.95	1.00	1.5
TFA (%)	0.000	0.05	0.07	0.2	**7**	20	30.47	45.54	60.541	90.8	99.99
TFR (%)	80.0	76.25	40.23	30	**10**	9.78	8.25	8	3.25	1.87	000

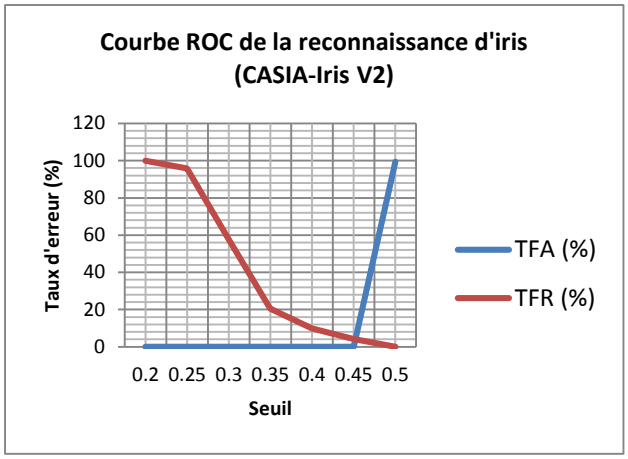
Selon les tableaux présentés ci-dessous, on remarque :

1. la reconnaissance par l'iris, en utilisant la base de données CASIA-Iris V1, présente des taux d'erreurs meilleurs que ceux calculés pour la reconnaissance par l'iris en utilisant la base de données CASIA-Iris V2. Ce fait est du principalement à la qualité d'images d'iris dans CASIA-Iris V2, cette base de données stocke des diversités d'images d'iris dont la plupart sont détériorées.
2. La reconnaissance par l'empreinte digitale présente un compromis acceptable entre le taux des fausses acceptations et le taux de faux rejets.
3. La reconnaissance par fusion multimodale d'iris et d'empreinte digitale est meilleure que la reconnaissance monomodale d'iris ou d'empreinte digitale.

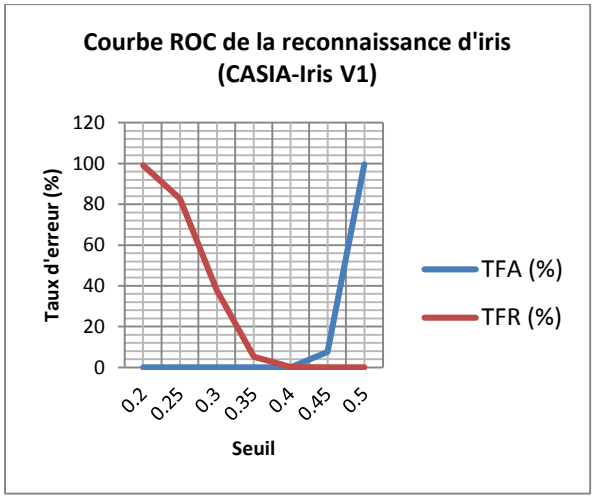
Courbes ROC des taux d'erreurs



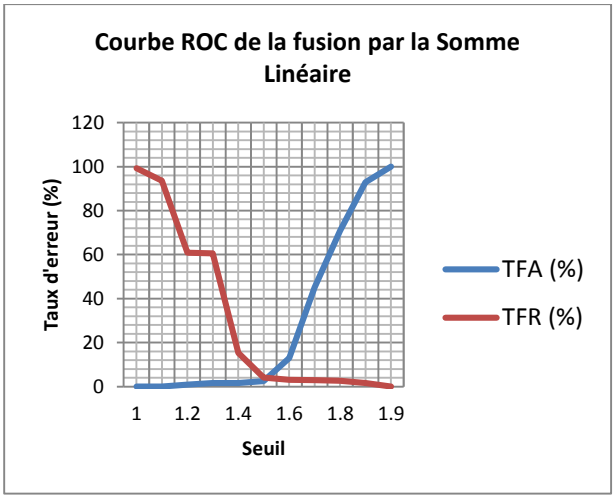
(a)



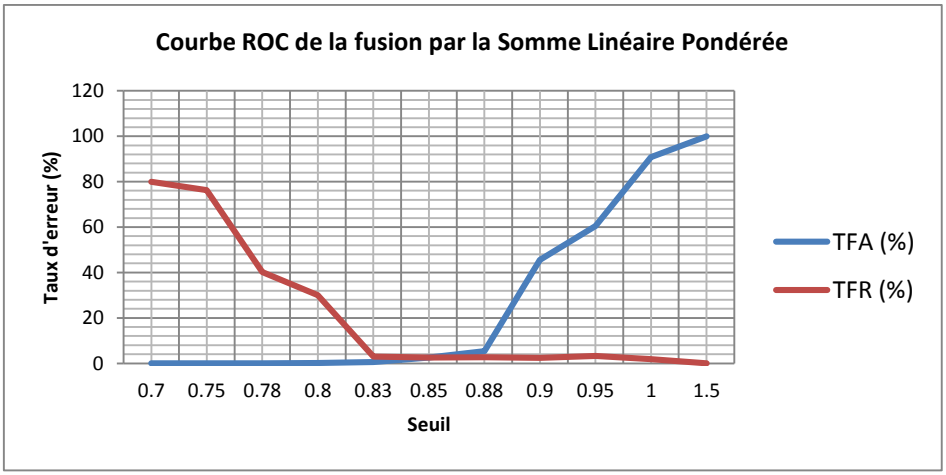
(b)



(c)



(d)



(e)

Figure 8.28 : Courbes ROC relatives aux expériences (a : reconnaissance d'empreinte, b : reconnaissance d'iris avec CASIA-Iris V2, c : reconnaissance d'iris avec CASIA-Iris V1, d : fusion par la Somme Linéaire, e : Fusion par la Somme Linéaire Pondérée)

8.7. Comparaison des résultats

Le tableau 8.10 présente une comparaison des différentes méthodes de reconnaissance implémentées en terme de taux d'erreur égal TEE, on constate que la fusion par la logique floue est meilleure suivie de la fusion par la somme linéaire pondérée et enfin la fusion par la somme linéaire classique.

Tableau 8.10 : Comparaison de Taux d'Egal Erreur TEE

Expérience	TEE
Reconnaissance par l'Iris (CASIA-V2)	0.45
Reconnaissance par l'Iris (CASIA-V1)	0.40
Reconnaissance d'Empreinte (FVC2004)	0.5
Iris +empreinte (*Somme linéaire*)	1.55
Iris +empreinte (*Somme linéaire pondérée*)	0.83
Iris +empreinte (Logique floue)	**0.038**

On constate que la précision de la méthode de la fusion de décision par la logique floue est meilleure que les autres techniques (Cf. Tableau 8.11).

Tableau 8.11: Comparaison de la précision de la reconnaissance (*Accuracy*) des différentes méthodes implémentées.

Expérience	Précision de la reconnaissance
Reconnaissance par l'Iris (CASIA-V2)	99.87%
Reconnaissance par l'Iris (CASIA-V1)	97.9%
Reconnaissance d'Empreinte (FVC2004)	85%
Iris +empreinte (Somme linéaire)	80.69%
Iris +empreinte (Somme linéaire pondérée)	91.5%
Iris +empreinte (Logique floue)	**99.975**

La précision « Accuracy » = 100- ((TFA+TFR)/2)

Tableau 8.12: Comparaison des résultats de la méthode proposée avec ceux des travaux récents portant sur la fusion Iris-Empreinte.

Référence	Niveau de fusion	Base de données	Algorithme d'extraction de caractéristique	Appariement	Résultat
[Kankrale et al, 2012]	Extaction de caractéristique	500 images de 50 sujets (CASIA-fingerprint V5 et CASIA-iris V1)	Approche basée minutie + Approche de Daugman	Règle AND	TFA =0%, TFR= 5.12% Temps d'appariement=3.56s
[Gawande et al, 2012]	Extaction de caractéristique	500 images de 50 sujets	Filtre 1D Log gabor pour les deux modalités	distance de Hamming	TFA =0%, TFR= 4.3% Temps d'appariement=0.14s
[Abdulahi et al, 2013]	Décision	/	Approche basée minutie modifiée	Règles floue et codes pondérés	TFA=TFR=2%
L'approche proposée [Benaliouche & Touahria, 2014]	Décision	500 images de 50 sujets (FVC2004 et CASIA-Iris V2)	Minutia based extractor + Daugman's iris extractor	Règles floue Si Alors	**TFA=0%** **TFR=0.05%** **Temps d'appariement=0.1754s**

D'après le tableau comparatif 8.12, on constate que l'approche proposée basée sur la fusion multimodale d'iris et d'empreinte par la logique floue est meilleure que celles de [Kankrale et al, 2012], [Gawande et al, 2012] et de [Abdulahi et al, 2013] en terme de temps d'appariement, de taux d'erreur TFA et TFR et de Précision.

8.8. Conclusion

Dans ce chapitre, nous avons présenté en détail la conception et l'implémentation de l'approche proposée: la reconnaissance par fusion multimodale d'iris et d'empreinte digitale au niveau *décision*, en utilisant la logique floue.

Nous avons détaillé par des diagrammes de flots de données les différents processus qui y régissent (*l'apprentissage*, *l'identification* et la *vérification*) ensuite nous avons dégagé les principaux modules du système multimodal d'iris et d'empreinte, à savoir :

- Le module de reconnaissance d'iris.
- Le module de reconnaissance d'empreinte.
- Le module d'appariement par fusion multimodale.

Cette structure modulaire est adéquate pour une réalisation dans un langage pluridisciplinaire.

Au niveau score, deux expériences ont été réalisées pour servir de comparaison avec la méthode proposée.

La première expérience réalise la fusion des deux modalités (l'iris et l'empreinte digitale) en utilisant la règle *Somme Linéaire*.

La deuxième expérience réalise la fusion des deux modalités (l'iris et l'empreinte digitale) en utilisant la règle *Somme Linéaire Pondérée*.

Plusieurs expériences ont été menées sur des bases de données d'iris (CASIA-Iris V1 et CASIA-Iris V2) et d'empreinte digitale (FVC 2004). Une base multimodale réelle de 500 sujets a été conçue et réalisée pour tester les algorithmes.

Les résultats expérimentaux montrent que la méthode de la fusion de décision par la *logique floue* est meilleure que les autres techniques en termes de temps d'exécution et de précision.

CONCLUSION GÉNÉRALE ET PERSPECTIVES

La biométrie, définit comme l'étude quantitative des caractéristiques biologiques, morphologiques ou comportementales de l'humain, est un champ de recherche très actif. A l'heure actuelle, les technologies biométriques sont basées le plus souvent sur les modalités d'empreintes digitales ou d'iris, qui sont pour l'instant réputées les plus fiables en contrepartie de leur caractère intrusif.

Les systèmes biométriques unimodaux souffrent de plusieurs problèmes qui sont à l'origine de l'utilisation d'un seul trait biométrique susceptible au bruit, à la mauvaise capture, à la pauvreté en matière de points biométriques confidents et notamment à la détérioration de la qualité de l'entrée biométrique. L'introduction de systèmes biométriques multimodaux est une solution à ces problèmes.

L'étude présentée dans cette thèse traite l'authentification automatique d'individus basée sur des multimodalités biométriques reliées à l'iris et à l'empreinte digitale.

L'utilisation conjointe de deux traits biométriques ou plus est une tendance actuelle pour renforcer les systèmes biométriques sur les plans de *sécurité*, *fiabilité* et *pertinence*. En effet, La fusion des méthodes biométriques constitue une solution adéquate et prometteuse aux problèmes posés par les systèmes biométrique monomodaux. Plusieurs travaux de recherche ont déjà montré que la combinaison de plusieurs modalités biométriques permet d'améliorer de manière significative les performances des systèmes basés sur une seule modalité.

La fusion présente les avantages de bénéficier des points forts offerts par chacune des modalités fusionnées, tout en préservant l'indépendance et la séparabilité des variations statistiques de chaque trait biométrique

Après avoir introduit les concepts généraux en biométrie multimodale, où nous avons détaillé les différents niveaux de fusion et de nombreuses techniques de fusion possibles dans un système biométrique multimodal, nous avons présenté un état de l'art en reconnaissance d'empreinte digitale, en reconnaissance de l'iris et en intelligence artificielle. Nous avons également montré les liens qui peuvent exister entre le fonctionnement du cerveau pour identifier et reconnaître des personnes et les concepts fondamentaux de la logique floue.

Ensuite, nous avons présenté trois approches traitant chacune une facette de la biométrie multimodale (chapitre 6, chapitre 7 et chapitre 8). Les trois contributions proposées et détaillées dans ce manuscrit montrent trois formes de la multimodalité biométrique, à savoir,

1. La multimodalité par *fusion d'algorithmes multiples*.
2. La multimodalité par fusion *d'instances répétées et multiples*.
3. La multimodalité par *fusion de traits biométriques différents*.

Nous avons étudié l'apport de la logique floue, en premier lieu, dans un système de reconnaissance monomodale (Chapitre 6), et en second lieu, dans un système de reconnaissance bimodal d'empreinte et d'iris (chapitre 8).

La logique floue est une théorie assez récente, destinée à traiter l'imprécis et l'incertain. Elle est fondée sur des règles théoriques logiques permettant à un système informatique de mimer le raisonnement de l'être humain. La logique floue peut être vue comme une extension de la logique classique aux raisonnements approchés. Par ses aspects numériques, elle s'oppose aux logiques modales. Dans ce travail nous avons utilisé les notions de la logique floue suivantes :

1. Les variables linguistiques floues : nous avons réalisé la modélisation des décisions de la reconnaissance par des variables linguistiques floues.
2. Ensembles flous : nous avons modélisé les classes de la qualité d'images biométriques par des ensembles flous, en transformant l'intervalle (*crisp set*) en un sous ensemble flou (*fuzzy set*).
3. La fuzzification et la deffuzzification : nous avons utilisé ces deux notions pour réaliser l'entrée et la sortie du système d'inférence flou.
4. L'inférence floue par des règles *Si-Alors* : la conception de l'algorithme d'inférence flou est très délicate car chaque règle d'inférence floue a son propre influence sur la décision du système. Nous avons eu recours à une étude exhaustive des distributions des clients authentiques et imposteurs portant sur une large base de données, pour pouvoir déterminer, avec précision, les règles floues du système d'inférence. Tout en préservant la séparabilité et l'indépendance des distributions d'appariements, qui mène à un meilleur compromis entre le taux de fausses acceptations et le taux de faux rejets.
5. La classification floue : Ce procédé permet d'affecter une donnée biométrique à une classe donnée selon un degré d'appartenance. La classification est utilisée par exemple par certains systèmes de reconnaissance d'empreintes digitales (avec des classes telles que : *boucles*, *arches* ou *tourbillons*), dans le but d'accélérer les identifications. En effet, la séparation des données en plusieurs classes permet de réduire la taille de la base de recherche et donc d'accélérer le processus.

Trois niveaux de fusion ont été étudiés dans ce travail :

1. La fusion au niveau S*core*

L'objectif principal des analyses statistiques est d'étudier les distributions des scores en sortie des modules de la reconnaissance biométrique, afin de pouvoir les modéliser mathématiquement. Les distributions des scores varient d'un utilisateur à un autre (variation interclasse) et varient aussi au sein de chaque utilisateur (variation intra-classe). On cherche toujours à

- Maximiser la variation interclasse.
- Minimiser la variation intra-classe.

La variation interclasse est causée par le fait qu'un système biométrique construit un modèle de référence dédié pour chaque utilisateur. Maximiser cette variation revient à construire le model ou la référence la plus optimal pour chaque utilisateur.

Le but fondamental de tout système biométrique opérant au niveau score, est de pouvoir séparer au maximum les distributions de score des imposteurs et des authentiques.

Nous avons choisi l'approche par combinaison de scores pour les raisons suivantes :

- Les scores de données contiennent l'information la plus riche à propos du modèle d'entrée.
- la fusion au niveau score donne le meilleur compromis entre la richesse d'information et la facilité d'implémentation.
- il est facile d'accéder et de combiner les scores générés par les différents classificateurs (*matchers*).

Deux méthodes de fusion de scores ont été implémentées, la fusion d'iris et d'empreinte par la *Somme Linéaire*, et la fusion d'iris et d'empreinte par la *Somme Linéaire Pondérée* (Cf. Chapitre 8). Les résultats expérimentaux de ces deux méthodes classiques ont été utilisés comme référence dans la comparaison des résultats.

2. La fusion au niveau *Caractéristique*

La fusion au niveau caractéristique consiste à combiner différents vecteurs de caractéristiques ("*feature vectors*") qui sont obtenus à partir d'une des sources suivantes :

1. Plusieurs *capteurs* du même trait biométrique.
2. Plusieurs *instances* du même trait biométrique.
3. Plusieurs *unités* du même trait biométrique.
4. Plusieurs *traits* biométriques.

Les techniques basées sur la fusion au niveau d'extraction de caractéristiques sont meilleures par apport aux autres techniques à cause de la préservation des caractéristiques biométriques discriminantes des différents traits fusionnés. Cependant, l'opération de la fusion multimodale à ce niveau est difficile.

Dans l'approche concernant la fusion d'empreintes digitales au niveau caractéristique (chapitre 7), nous avons montré que :

- Lorsque les vecteurs de caractéristiques sont **homogènes** (par exemple, plusieurs images d'empreinte digitale du doigt d'un utilisateur), un unique vecteur de caractéristiques résultant peut être calculé comme une somme pondérée des vecteurs de caractéristiques individuels.
- Lorsque les vecteurs de caractéristiques sont **hétérogènes** (par exemple, des vecteurs de caractéristiques de différents doigts), nous pouvons les concaténer pour former un seul vecteur de caractéristiques.

Les mesures de performance du matcher (l'algorithme de fusion des vecteurs de caractéristiques) sont la *Spécificité* P et la *Sensibilité* S. l'étude statistique a montré que :

- Le critère de la S*ensibilité* S, qui mesure la capacité de l'extracteur de détecter de vraies minuties, s'améliore à chaque fois en fusionne plus d'empreinte par doigt.
- Le critère de la *Spécificité* , qui mesure la capacité de l'extracteur à éviter les fausses détections, s'améliore à chaque fois en fusionne plus d'empreinte par doigt.

Nous avons conçu les deux parties de reconnaissance uni-modale de l'empreinte et de l'iris avec deux modes opératoires : le mode de vérification qui consiste à comparer l'identité qui se présente avec l'identité proclamée et le mode d'identification qui consiste à rechercher l'identité du client qui se présente dans la base de données. Les résultats obtenus de la vérification et de l'identification ont servi de comparaison avec les travaux de recherche en relation.

L'implémentation des algorithmes du système de reconnaissance d'empreinte digitale basé sur la fusion de codes au niveau caractéristique sont faits sous JAVA. Un train de test a été réalisé sur la base de données d'empreintes digitales FVC 2000. Cette base est caractérisée par des ensembles d'images d'empreintes de mauvaise qualité. Les résultats expérimentaux ont donné un TEE égal à 2.5% avec une précision de 88.75% pour l'expérience réalisant une fusion de huit impressions par doigt [Benaliouche et Benmohamed, 2012].

3. La fusion au niveau *Décision*

La fusion d'information au niveau *décision* peut être mis en place lorsque chaque matcher biométrique décide individuellement de la meilleure correspondance possible selon l'entrée qui lui est présentée. Cette fusion est souvent utilisée pour sa simplicité.

Nous avons proposé deux stratégies de fusion au niveau décision par la logique floue, en premier lieu, dans un système de reconnaissance monomodale (Chapitre 6), et en second lieu, dans un système de reconnaissance bimodal d'empreinte et d'iris (chapitre 8). En effet, le système d'inférence floue ajuste le poids de pondération pour chaque trait biométrique (l'iris et l'empreinte) selon l'importance de chaque trait (ici le score de l'iris est plus confiant que celui de l'empreinte).
Le poids de pondération n'est rien qu'une appréciation attribuée à la décision du système de reconnaissance, en utilisant des valeurs linguistiques modélisées par des ensembles flous, comme par exemple *Mauvais, Moyen, Bon, excellent*, et les règles floues produisent des décisions selon la distance d'appariement calculée pour chaque trait biométrique

Nous avons tenu à concevoir un système biométrique avec des parties supervisées par l'utilisateur afin de comparer les résultats émis par des entrés différentes de paramètres et par conséquences déduire les paramètres optimaux du système, les parties supervisées touchent le module d'appariement de la fusion par la méthode de la somme linéaire pondérée « *weighted sum rule* » et le module d'appariement par la méthode de la logique floue « *fuzzy logic matching* ».

La classification floue

Un des problèmes majeurs soulevés par les systèmes d'identification est le **temps de réponse** du système dans le processus d'identification, dans ce travail, nous avons proposé une solution facile et pertinente, il s'agit de :

La **classification floue** par la distance *Euclidienne* et la *logique floue*, En effet, l'appariement par la distance *Euclidienne* présente l'avantage de réaliser l'opération d'authentification ou d'identification dans un temps beaucoup moins long que les autres distances mathématiques employées dans l'appariement des vecteurs biométriques comme par exemple la distance de *Hamming*. Les tests expérimentaux ont démontré un gain de temps

de réponse de la phase d'identification de 60% [Benaliouche et Touahria, 2011], [Benaliouche et Touahria, 2013]. Par ailleurs, la distance *Euclidienne* est plus rapide que la distance de *Hamming* de 2.5 fois. (Cf. Chapitre 6).

L'implémentation des différents algorithmes du système de reconnaissance monomodal d'iris, et du système multimodal de fusion d'iris et d'empreinte, ainsi que le déroulement des tests on été réalisés sous Matlab. Les bases de données officielles d'iris (CASIA) et d'empreinte digitale (FVC) ont servi à pratiquer les tests de fusion.

Les résultats expérimentaux ont montrés que la fusion de décisions par la *logique floue* est meilleure que celle de la fusion de scores par la méthode de la *somme linéaire* et celle de la fusion par la *somme linéaire pondérée*.

Les résultats expérimentaux ont été rapportés sous forme de courbes ROC. Dans le cadre biométrique, cette courbe représente l'évolution du FRR en fonction du FAR. L'étude de cette courbe permet de déterminer les performances d'un système biométrique. Les tests menés et les résultats obtenus témoignent de l'efficacité de nos propositions. En effet, Nous avons pu concevoir :

- Un système de vérification d'empreinte avec un taux d'égale erreur de 2,5% seulement.
- Un système de vérification d'iris avec un taux d'égale erreur de 0.28% seulement.
- Un système bimodal de fusion d'iris et d'empreinte avec une précision de 99.975% et un zéro-TFR de 0.05%.

Pour que des conclusions fiables soient tirées, cette thèse, s'est appuyée sur une série d'expérimentation et ce, sans perdre de vue, les résultats fournis par les autres méthodes existantes.

Les résultats obtenus sont satisfaisants. En effet, nous avons pu avoir des performances en termes de EER entre 0.28% et 3.8%. La comparaison de notre travail avec quelques travaux récents sur la fusion bimodale d'iris et d'empreinte digitale, a montré notre apport et a indiqué sa valeur ajoutée [Benaliouche & Touahria, 2014].

Perspectives

Il existe quelques perspectives intéressantes en biométrie : par exemple, l'étude la reconnaissance comportementale, souvent peu intrusive, elle est bien admise par le public. En plus son coût est beaucoup plus faible par rapport aux techniques de la biométrie morphologique et biologique.

En ce qui concerne les techniques de fusion, on pourrait par exemple fusionner plus de deux modalités en vue d'accroitre la pertinence et la fiabilité de l'authentification. On peut également envisager des évolutions des stratégies de fusion intégrant les progrès réalisés dans d'autres domaines comme l'intelligence artificielle. Comme l'apport d'informations sur la qualité du trait biométrique, ou des données personnelles, ou même l'adaptation du système de reconnaissance à chaque utilisateur, et pourquoi pas une biométrie personnalisée.

Nous avons travaillé durant cette thèse sur les *scores*, les *décisions* et les *caractéristiques* issus des systèmes monomodaux, à la fois pour la fusion, et pour l'analyse statistique des distributions authentiques qu'on a souhaité au maximum les séparés de celles des imposteurs.

Si l'on souhaite améliorer d'avantage les performances en fusion ou affiner notre analyse, il faudrait se placer dans un espace contenant plus d'information. Les perspectives d'évolution de ce travail sont alors multiples :

- l'application d'une représentation plus condensées comme les ondelettes.
- l'étude plus approfondie pour choisir l'algorithme de reconnaissance le plus performant et le mieux adapté, ainsi que l'optimisation de la chaine de traitement.
- L'investigation de l'emploi des méthodes bio-inspirées pour améliorer la qualité de la donnée biométrique.

Références bibliographiques

A

[Abhyankar & Schuckers, 2010]	Aditya abhyankar, Stephanie Schuckers , "a novel biorthogonal wavelet network system for off-angle iris recognition", pattern recognition 43, pp. 987-1007, 2010.
[Achermann & Bunke, 1996]	B. Achermann, H. Bunke, "Combination of classifiers on the decision level for face recognition". Technical report, University of Bern, 1996.
[Ailsto et al, 2006]	Heikki Ailisto, Elena Vildjiounaite, Mikko Lindholm, Satu-Marja Makela, Johannes Peltola, "Soft biometrics—combining body weight and fat measurements with fingerprint biometrics", Pattern Recognition Letters 27, pp. 325–334, 2006.
[Alonso-Fernandez et al., 2008]	F. Alonso-Fernandez, F. Roli, G. Marcialis, J. Fierrez, J. Ortega-Garcia and J. Gonzalez-Rodriguez, "Performance of fingerprint quality measures depending on sensor technology", SPIE Journal of Electronic Imaging, Special Section on Biometrics: Advances in Security, Usability and Interoperability, Vol. 17, n. 1, January-March 2008.
[Alonso-Fernandez et al., 2010]	F. Alonso-Fernandez, J. Fierrez, D. Ramos and J. Gonzalez-Rodriguez, "Quality-Based Conditional Processing in Multi-Biometrics: application to Sensor Interoperability", IEEE Tansactions on Systems, Man and Cybernetics Part A, Vol. 40, n. 6, pp. 1168-1179, 2010.
[Alonso-Fernandez et al., 2012]	F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, "Quality Measures in Biometric Systems", *IEEE Security & Privacy*, Vol. 10, n. 9, pp. 52-62, December 2012.
[Audibert, 2013]	Laurent Audibert, « Cours UML », accessible via le site http://laurent-audibert.developpez.com/Cours-UML/html/Cours-UML.html, date d'accès Mai 2013.

B

[Babler; 1991]	W.J. Babler, "Embryologic Development of Epidermal Ridges and Their Configurations", Dermatoglyphics: Science in transition. Birth defects, New York, Wiley-Liss, pp. 95-112, 1991.
[Bachimont, 1994]	Bruno Bachimont, "Le contrôle dans les systèmes à base de connaissances ; contribution à l'épistémologie de l'intelligence artificielle". Hermès. 1994.
[Baig et al, 2009]	A. Baig, A. Bouridane, F. Kurugollu, Gang Qu, "Fingerprint – Iris Fusion based Identification System using a Single Hamming Distance Matcher", International Journal of Bio Science and Bio Technology, vol. 1 no 1, pp. 47-58, 2009.
[Bajaj & Chaudhury, 1997]	R. Bajaj, S. Chaudhury, "Signature verification using multiple neural Classifiers". Pattern Recognition, Vol. 30(1), pp. 1–7, 1997.
[Balacheff, 1994]	Balacheff N, "Didactique et intelligence artificielle". Recherches en didactique des mathématiques, 14 (1/2), pp. 9-42. 1994.

[Bansal et al., 2010]	R. Bansal, P. Sehgal, P. Bedi, "Effective Morphological Extraction of True Fingerprint Minutiae based on the Hit or Miss Transform", International Journal of Biometrics and Bioinformatics(IJBB), vol. 4, pp. 71-85. 2010.
[Bansal et al., 2011]	R. Bansal, P. Sehgal, P. Bedi, "Minutiae extraction from Fingerprint images, a review", International Journal of Computer science issues(IJCSI), vol. 8, Issue. 5, No. 3, pp. 74-85, 2011.
[Barett, 1997]	W.A. Barrett, "A survey of face recognition algorithms and testing results", Conference Record of the Thirty-First Asilomar Conference on Signals, Systems & Computers, pp. 301-305, 1997
[Benaliouche & Touahria, 2011]	Houda Benaliouche, Mohammed Touahria, "Supervised fuzzy logic decision in an automatic iris recognition system", the second international conference on complex systems CISC'2011, Jijel, Algérie, pp. 6-8, Decembre 2011.
[Benaliouche & Benmohamed, 2012]	Houda Benaliouche, Mohammed Benmohamed, "Improving specificity and sensitivity in a fingerprint multi instances and multi measures biometric recognition", the first international conference on advanced communication and information system ICACIS'12, Batna, Algérie, pp. 41-47, 12-13- Decembre 2012,
[Benaliouche & Touahria, 2013]	Houda Benaliouche, Mohammed Touahria, "Reducing the false rejection rate using an iris recognition algorithm based on fuzzy logic », première Journée Informatique de BBA JIBBA'13, Borj Bou Aririge, Algérie, 4 Decembre 2013.
[Benaliouche & Touahria, 2014]	Houda Benaliouche, Mohammed Touahria, "Comparative study of multimodal biometric recognition by fusion of iris and fingerprint", The Scientific World Journal, Special issue on Recent Advances in Information Technology, Volume 2014, article ID 29369, 13 pages, DOI http://dx.doi.org/10.1155/2014/829369.
[Bertillon, 1985]	A. Bertillon, "la couleur de l'iris, Revue scientifique", France, 1885.
[Besbes et al., 2008]	F. Besbes, H. Trichili, B. Solaiman, "Multimodal biometric system based on fingerprint identification and Iris recognition", 3rd International IEEE Conference Inf. Commun. Technol.: From Theory to Applications (ICTTA 2008), pp. 1–5. DOI: 10.1109/ICTTA.2008.4530129.
[Boles & Boashash, 1998]	W.W. Boles, B. Boashash, "A Human Identification Technique Using Images of the Iris and Wavelet Transform", IEEE Trans. on Signal Processing, Vol. 46(4), pp.1185-1188, 1998.
[Bowyer et al., 2008]	Kevin W. Bowyer, Karen Hollingsworth, Patrick J. Flynn, "Image understanding for iris biometrics: A survey", Computer Vision and Image Understanding, Vol. 110, pp 281–307, 2008.
[Broussard & Ives, 2011]	Randy P. Broussard, Robert W.Ives, "improving identification accuracy on low resolution and poor quality iris images using an artificial neural network-based matching metric", Journal of electronic imaging, Vol. 20, No. 1, 013013, 2011.
[Brunelli & Falavigna, 1995]	R. Brunelli, D. Falavigna, "Person identification using multiple cues", *IEEE Trans. on PAMI*, Vol. 17, No. 10, pp. 955-966, 1995.
[Butler, 1863]	Samuel Butler, "Darwin Among the Machines", Christchurch, the Press, Juin 1863.

C

[Canny, 1986]	Canny, J., "A Computational Approach To Edge Detection", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 8, pp. 679-714, 1986.
[CASIA]	CASIA Iris Images database, www.sinobiometrics.com
[Chen et al., 1997]	K. Chen, L. Wang, H. Chi, "Methods of combining multiple classifiers with different features and their applications to text-independent speaker identification". Pattern Recognition and Artificial intelligence, Vol. 11, No. 3, pp.417-445, 1997.
[Chibelushi et al., 1993]	C. Chibelushi, J. Mason, F. Deravi, "Integration of acoustic and visual speech for speaker recognition", Eurospeech, pp. 157-160, 1993.
[Chen et al., 2005]	Y. Chen, S. Dass, and A. Jain. "Fingerprint Quality Indices for Predicting Authentication Performance". Fifth International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA), New York, NY, USA, pp. 160– 170, July 2005.
[Chowhan et al., 2011]	S. Chowhan, U. V. Kulkarni, G. N. Shinde, "Iris recognition using modified fuzzy Hyperline segment neural network", Journal of computing, volume 3, issue 6, June 2011, ISSN 2151-9617.
[Crampes, 2013]	Jean Bernard Crampes, « définition du génie logiciel », accessible via le site http://www.jbcc.fr/definitionGL_Fr.php, date d'accès 2013.
[Crevier, 1993]	Daniel Crevier, "AI: The Tumultuous Search for Artificial Intelligenc e", New York, BasicBooks, 1993, (ISBN 0-465-02997-3).

D

[Daugman, 1993]	J. Daugman, "High Confidence Visual Recognition of Persons by a Test of Statistical Independence" *IEEE* Transactions on Pattern Analysis and Machine Intelligence, vol. 15, No. 11, pp. 1148-1161, November 1993.
[Daugman, 1994]	J. Daugman, "Biometric personal identification system based on iris analysis", US PATENT, 5291560, March 1, 1994.
[Daugman, 1998]	J. Daugman. "Combining Multiple Biometrics". 1998. Disponible sur http://www.cl.cam.ac.uk/~jgd1000/combine/combine.html.
[Daugman, 2002]	J. Daugman, "How Iris Recognition Works", Proceedings of 2002 International Conference on Image Processing, Vol. 1, 2002.
[Dobes et al., 2003]	M. Dobes, L. Machala et P. Tichavsky, "human eye iris recognition using mutual information", Optik, Vol. 115, No. 9, pp. 399-404, 2003.
[Dreyfus, 1984]	Dreyfus, H, « Intelligence artificielle : mythes et limites », Flammarion. 1984
[Dugelay et al, 2002]	J.L. Dugelay, J. -C. Junqua, C. Kotropoulos, R. Kuhn, F. Perronnin, I. Pitas, "Recent Advances in Biometric Person Authentication", IEEE mi. Conf on Acoustics Speech and Signal Processing (ICASSP), Orlando, Florida, May 2002.

F

[Feng et al., 2004]	Guiyu Feng, Kaifeng Dong, Dewen Hu, David Zhang. "When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy". Lecture Notes in Computer Science, , Proceedings of First International Conference on Biometric Authentication, ICBA'2004, Hong Kong, China, Vol. 3072, pp. 701 – 707, July 15-17, 2004.
[Flom & Safir, 1987]	L. Flom, A. Safir, "Iris recognition system", US PATENT, 4,641,349, February 3, 1987.

G

[Galbally et al., 2012]	J. Galbally, F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, "A High Performance Fingerprint Liveness Detection Method Based on Quality Related Features", Future Generation Computer Systems, Vol. 28, pp. 311-321, January 2012.
[Galbally et al., 2014]	J. Galbally, S. Marcel, J. Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition", IEEE Trans. on Image Processing, Vol. 23, No. 2, pp. 710-724, February 2014.
[Garcia-Salicetti et al, 2003]	S. Garcia-Salicetti, C. Beumier, G. Chollet, B. Dorizzi, J.L. les Jardins, J. Lunter, Y. Ni, D. Petrovska-Delacrétaz, "BIOMET : a multimodal person authentication database including face, voice, fingerprint, hand and signature modalities", Lecture Notes in Computer Science, Publisher: Springer-Verlag GmbH, Vol. 2688, pp. 845-853, 2003.
[Giacinto et al, 2005]	Giacinto, G., Roli, F., Tronci, R.: "Score Selection Techniques for Fingerprint Multi-Modal Biometric Authentication", 13th international conference on image analysis and processing ICIAP 2005. pp. 1018-1025, 2005.
[Giot & Rosenberger, 2012]	Romain Giot, Christophe Rosenberger, "Genetic programming for multibiometrics", Expert Systems with Applications, Vol. 39, pp.1837–1847, 2012.

H

[Hanley & McNeil, 1982]	Hanley, J., McNeil, B. "The meaning and use of the area under the receiver operating characteristic (roc) curve". Radiology, Vol. 143, pp. 29–36, 1982.
[Haugeland, 1989]	Haugeland J,. " L'esprit dans la machine ; Fondements de l'intelligence artificielle". Odile Jacob. 1989.
[Hawkins & Blakeslee, 2004]	Jeff Hawkins, Sandra Blakeslee, "On Intelligence", New York, Owl Books, 2004 , ISBN 0-8050-7853-3.
[Humbe et al., 2007]	V. Humbe, S. S. Gornale, R. Manza and K. V. Kale, "Mathematical Morphology approach for Genuine Fingerprint Feature Extraction", Int. Journal of Computer Science and Security (IJCSS), vol. 1, pp. 53-59, 2007.

I

[IBG, 2013]	International Biometric Group, homepage www.biometricgroup.com date d'accès 2013.
[Ito et al., 2005]	Koitchi Ito; Ayumi Morita, Takafomi aoki, Tatsuo Hoguchi;Hiroshi nakajima, Koji Kobayashi, "a fingerprint recognition algorithm using phase-base image matching for low-quality fingerprint", IEEE trans 0-7803-9143-9, 2005.

J

[Jagadeesan et al., 2010]	Jagadeesan, A., Thillaikkarasi, T., Duraiswamy, K.: "Cryptographic Key Generation from Multiple Biometric Modalities": Fusing Minutiae with Iris Feature", International journal of computer applications, Vol. 2, No. 6, pp. 16-26. June 2010.
[Jain et al., 1997]	Jain, A, .Hong, .Pankanti, .Bolle.: "An Identity-Authentification system Using Fingerprints", Proceedings of the IEEE, Vol. 85, pp. 1365-1388, September 1997.
[Jain et al., 1998]	A.K. Jain, R. Bolle et S. Pankanti, "Personal Identification in Networked Society ", Kluwer Academic, 1998.
[Jain et al., 1999]	A.K. Jain, A. Ross, , S.Pankanti, "A prototype hand geometry-based verification system", International conference on Audio- and Video-based Biometric Person Authentication, pp. 166-171, March 1999.
[Jain et al, 2001]	A.K. Jain, S. Prabhakar S. Pankanti, "Twin Test: On Discriminability of Fingerprints", 3rd International conference on Audio- and Video-Based Person Authentication, pp. 211-216, Sweden, June 6-8, 2001.
[Jain & Prabhakar, 2002]	Anil K Jain, Salih Prabhakar, "Decision-level fusion in fingerprint verification", Elsevier pattern recognition, Vol. 35, pp. 861-874. 2002.
[Jain & Ross, 2004]	A. K. Jain, A. Ross. "Multibiometric systems ". communications of the ACM, special issue on multimodal interfaces, Vol. 47, No. 1, pp. 34–40, January 2004.

K

[Kang et al., 2010]	Kang, Byung Jun; Park, Kang Ryoung; Yoo, Jang-Hee; Moon, Kiyoung "Fuzzy difference-of-Gaussian-based iris recognition method for noisy iris images". Optical Engineering, Vol. 49, Issue 6, 067001, 2010.
[Kittler et al, 1998]	J. Kittler, M. Hatef, R.P. Duin, J.G. Matas, "On combining classifiers", IEEE Transactions on Pattern Analysis and Machine Intelligence Vol. 20, No. 3, pp. 226–239, 1998.
[Kodituwakku et al., 2010]	Kodituwakku, S.R., Fazeen; M.I.M, " offline fuzzy based approach for iris recognition with enhanced feature detection"; Advanced techniques in computing sciences and software engineering, Springer science + business media; B.V, pp. 39, 2010, ISBN 978-90-481-3659-9
[Kumar et al., 2003]	A. Kumar, D.C.M. Wong, H.C. Shen, A.K. Jain. "Personal Verification Using Palmprint and Hand Geometry Biometric". Lecture Notes in Computer Science Publisher: Springer-Verlag

	GmbH, Vol. 2688, pp. 668-678, 2003.
[Kumar & Passi, 2010]	Ajay Kumar, Arun Passi, "Comparison and combination of iris matchers for reliable personal authentication", Pattern Recognition, Vol. 43, pp. 1016–1026, 2010.

L

[Lahane & Ganorkar, 2012]	P.U.Lahane, S.R.Ganorkar , "Fusion of Iris & Fingerprint Biometric for Security Purpose", International Journal of Scientific & Engineering Research Vol. 3, Issue 8, pp. 1-5; August-2012.
[Lam & Suen, 1997]	L. Lam, C. Suen. "Application of majority voting to pattern recognition: an analysis of its behavior and performance". IEEE Transactions on Systems, Man and Cybernetics, Part A, Vol. 27, No. 5, pp. 553–568, September 1997.
[Langdon & Buxton, 2001]	Langdon, W., Buxton, B. "Evolving receiver operating characteristics for data fusion". 4th European Conference, EuroGP, pp. 87–96, 2001.
[Latha & Thangasamy, 2010]	L.Latha, S.Thangasamy, "A Robust Person Authentication System based on Score Level Fusion of Left and Right Irises and Retinal Features", Procedia Computer Science 2, pp. 111–120, 2010.
[Liau & Isa, 2011]	Heng Fui Liau, Dino Isa, « Feature selection for support vector machine-based face-iris multimodal biometric system", Expert Systems with Applications 38, pp. 11105–11111, 2011.
[Lumini & Nanni, 2007]	Alessandra Lumini, Loris Nanni, "When Fingerprints Are Combined with Iris – A Case Study: FVC2004 and CASIA", International Journal of Network Security, Vol.4, No.1, pp. 27–34, Jan. 2007.
[Lumini & Nanni, 2008]	Alessandra Lumini, Loris Nanni, "Advanced methods for two-class pattern recognition problem formulation for minutiae-based fingerprint verification", Pattern Recognition Letters Vol. 29, pp. 142–148, 2008.

M

[Ma et al., 2002]	L. Ma, Y. Wang, T. Tan, **"**Iris recognition using circular symmentric filters », Proc. Of ICPR'02, Québec city, Canada, 11-25 August 2002.
[Ma et al., 2004]	Li Ma, Tieniu Tan, Yunhong Wang, Dexin Zhang, "Efficient iris recognition by characterizing Key Local Variations", IEEE Transaction On Image Processing, Vol. 13, N°6, June 2004.
[Maio et al., 2000]	Maio D., Maltoni D., .Cappelli R., Wayman J.L.and Jain A.K. "FVC2000 Fingerprint Verification Competition". IEEE transactions on pattern analysis machine intelligence, Vol. 24, No 3, pp. 402-412, march 2002. http://bias.csr.unibo.it/fvc2000
[Maio et al., 2002]	Maio, D. Maltoni, R. Cappelli, J.L.Wayman, Jain, A.K. "FVC2002 second fingerprint verification competition", in proceeding 16th international conference on pattern recognition ICPR2002, québec city, Vol. 3, pp. 811-814., 2002. http://bias.csr.unibo.it/fvc2002

[Maltoni et al., 2004]	Maltoni,D, Cappelli, R, J.L.Wayman and A.K. Jain," FVC2004 third fingerprint verification competition", International conference on biometric authentication ICBA04, Hong Kong , pp. 1-7, July 2004. http://bias.csr.unibo.it/fvc2004.
[Maltoni et al., 2009]	Maltoni D., Maio D., Jain A. K., "Handbook of fingerprint recognition" page 228, 2009. Accessible sur Books.google.fr/books?isbn=1848822537
[Mane et al, 2011]	Arjun V Mane, Yojesh S Rode, K V Kale, "novel multiple impression based multimodal fingerprint recognition system", international journal of computer applications (0975-8887) Vol. 27 No. 8, pp 26-31, august 2011..
[Martin et al., 1997]	A. Martin, G. Doddington, T. Kamm, M. Ordowski, M. Przybocki, "The DET Curve in Assessment of Detection Task Performance", EUROSPEECH'97, Vol. 4, pp. 1895-1898, 1997.
[Masek & Koveski, 2003]	L. Masek, P. Koveski. "MATLAB Source Code for a Biometric Identification System based on Iris Patterns" ,The University of Western Australia, 2003. www.csse.uwa.edu.au/pk/studentprojects/libor
[Matsumoto et al., 2002]	T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of artificial 'gummy' fingers on fingerprint systems", Proceedings of SPIE, vol. 4677, January 2002.
[Masek, 2003]	Libor Masek, "Recognition of Human Iris Patterns for Biometric Identification", thesis of Bachelor of Engineering degree of the School of Computer Science and Software Engineering, The University of Western Australia, 2003.
[McCorduck, 2004]	Pamela McCorduck, "Machines Who Think", Natick, A. K. Peters, Ltd., 2004, 2nd edition, (ISBN 1-56881-205-1).
[Meenakshi & Padmabathi, 2010]	V.S.Meenakshi, G.Padmavathi, "Security Analysis of Password Hardened Multimodal Biometric Fuzzy Vault with Combined Feature Points Extracted from Fingerprint, Iris and Retina for High Security Applications", Procedia Computer Science, Vol. 2, pp. 195–206, 2010.
[Mendal et al, 2006]	Jerry M. Mendel, Robert I. John, Feilong Liu, "Interval Type-2 Fuzzy Logic Systems Made Simple", IEEE Transactions on fuzzy systems, Vol. 14, No. 6, December 2006.
[Metz, 1978]	Metz, C. "Basic principles of roc analysis", Seminar Nuclear Med, VIII, Vol. 4, pp. 283-298, 1978.
[Mitchell, 1997]	Tom M. Mitchell, "Machine Learning", McGraw-Hill International Editions, pp. 367-390, ISBN 0-07-115467-1. 1997.
[Moon et al., 2004]	Y. Moon, H. Yeung, K. Chan, S. Chan. "Template synthesis and image mosaicking for fingerprint registration: An experimental study", IEEE International Conference on Acoustics, Speech, and Signal Processing, pp. 409–412, 2004.
[Muron et al., 2001]	A. Muron, P. Kois, J. Pospisil, "Identification of persons by means of the Fourier spectra of the optical transmission binary models of the human irises", Optics Communication by Elsevier Science, Vol. 192, pp. 161-167, 2001.

N

[Nanni & Lumini, 2009]	Loris Nanni, Alessandra Lumini, « Descriptors for image-based fingerprint matchers », Expert Systems with Applications, Vol. 36, pp. 12414–12422, 2009.
[Newell, 1990]	Newell, A., 1990. "Unified Theories of Cognition". Harvard University Press.
[Nicolle, 1996]	Anne Nicolle, « L'expérimentation et l'intelligence artificielle », Intellectica, Vol. 1, No. 22, pp. 9-19, 1996.
[NIST, 2002]	"NIST report to the United States Congress. Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability". 2002. ftp://sequoyah.nist.gov/pub/nist_internal_reports/NISTAPP_Nov02.pdf
[NIST]	Site web de "the National Institute of Standards and Technologies" NIST, USA accessible via http://www.nist.gov.
[Noh et al., 2002]	S. I. Noh, K. Pae, C. Lee et J. Kim, "Multi-resolution independent component analysis for iris identification", Proc. Of International and Technichal Conf. on circuits/Systems & Communication, Phuket, Thaïland, July 2002.

O

[Ong et al., 2003]	I.G.K. Ong, T. Connie, A.T.B. Jin, "A single-sensor hand-eometry and almprint verification system", *Proc. of ACM SIGMM Workshop on Biometrics lethods and Applications*, pp. 100-106, Berkley, California, USA, 2003.

P

[Park & Park, 2007]	Hyun-Ae Park, Kang Ryoung Park, "Iris recognition based on score level fusion by using SVM", Pattern Recognition Letters, Vol. 28, pp. 2019–2028, 2007.
[Partridge & Wilks, 1990]	Partridge, D., Wilks, Y. "The Foundations of Artificial Intelligence": A Source Book. Cambridge University Press. 1990.
[Ponce-Cruz, 2010]	P. Ponce-Cruz, F. D. Ramirez-Figueroa, "Intelligent Control Systems with LabVIEW™" © Springer 2010. ISBN 978-1-4888-2-683-0.

R

[Radha & Kavitha, 2012]	N. Radha, A. Kavitha, "Rank level fusion using fingerprint and iris biometrics", Indian Journal of Computer Science and Engineering, vol. 2, No. 6, pp. 917-923, January 2012.
[Radman et al, 2012]	Abduljalil Radman, Kasmiran Jumari, Nasharuddin Zainal , « Iris Segmentation in Visible Wavelength Environment", Procedia Engineering, Vol. 41, pp. 743 – 748, 2012.
[Ren et al, 2009]	Chunxiao Ren, Yilong Yin, Jun Ma, Jongping Yang, "a novel method of score level fusion using multiple impressions for fingerprint verification", proceeding of the 2009 IEEE international conference on systems, man and cybernetics, San Antonio, USA October 2009.
[Rosental, 1998]	Claude Rosental, "Histoire de la logique floue. Une approche sociologique des pratiques de démonstration", Revue de Synthèse, Vol. 4, pp. 575-602, Octobre-Décembre 1998.
[Ross & Jain, 2002]	Arun Ross, Anil K Jain, "Fingerprint Mosaicking". IEEE International Conference on Acoustic Speech and Signal Processing, May 2002

[Ross & Jain, 2004]	Arun Ross, Anil K Jain, "multimodal biometrics: an overview", 12th European signal processing conference (EUSIPCO), Vienna Austria, pp. 1221-1224, September 2004.
[Ross et al, 2006]	A. Ross, K. Nandakumar, A.K. Jain, "Handbook-of-Multibiometrics", Springer Publishers, 2006.
[Russell & Norvig, 2003]	Stuart Russell, Peter Norvig, "Artificial Intelligence: A Modern Approach", Upper Saddle River, Prentice Hall, 2003, 2e édition. ISBN 0-13-790395-2
[Russell & Norvig, 2010]	Stuart Russell, Peter Norvig, "intelligence artificielle", Pearson Education France 2010, ISBN 978-0-13-604259-4.

S

[Sabourin & Genest, 1994]	M. Sabourin, G. Genest. « Coopération de classifieurs pour la vérification automatique des signatures ». 3eme Colloque National sur l'Ecrit et le Document, pp. 89-98, Rouen, 1994.
[Sasidhar et al, 2010]	k.Sasidhar, Vijaya L Kakulapati, Kolikipogu Ramakrishna, K.KailasaRao, "multimodal biometric systems – study to improve accuracy and performance", International journal of computer science and engineering survey (IJCSES), Vol. 1, No. 2, pp 54-60, November 2010,.
[Sha et al, 2007]	Lifeng Sha, Feng Zhao, Xiaoo Tang, "a two stage fusion scheme using multiple fingerprint impressions", Proceedings of the international conference on image processing ICIP2007, San Antonio, Texas USA, September 2007.
[Shi & Govindaraju, 2006]	Zhixin Shi , Venu Govindaraju, "A chaincode based scheme for fingerprint feature extraction", Pattern Recognition Letters, vol. 27, pp. 462–468. 2006.
[Simon-Zorita et al., 2003]	D. Simon-Zorita, J. Ortega-Garcia, J. Fierrez-Aguilar, J. Gonzalez-Rodriguez; "Image quality and position variability assessment in minutiae-based fingerprint verification"; 2003.

T

[Tan & Schuckers, 2010]	Bozhao Tan, Stephanie Schuckers, "Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise », Pattern Recognition Vol. 43,pp. 2845–2857, 2010.
[Tax et al, 2000]	D.M.J. Tax, M.V. Breukelen, R.P.W. Duin, J. Kittler, "Combining multiple classifiers by averaging or combining", Pattern Recognition Vol. 33, pp. 1475–1485, 2000.
[Toh et al, 2003]	K-A, Toh, W. Xiong, W-Y, Yau, X. Jiang, "Combining fingerprint and Handgeometry verification decisions", Lecture Notes in Computer Science, Publisher: Springer-Verlag BmbH, Vol. 2688, pp. 688-696, 2003.
[Toh et al , 2004]	Kar-Ann Toh, Xudong Jiang, Wei-Yun Yau, "Exploiting Global and Local Decisions for Multimodal Biometrics Verification", IEEE Transactions on signal processing, Vol. 52, No. 10, pp. 3059-3072, October 2004.

U

[UBATH]	base de données d'iris UBATH http://www.bath.ac.uk/elec-eng/pages/sipg/irisweb/index.htm
[UPOL]	base de données d'iris UPOL e, www.inf.upol.cz/iris/
[URIBIS]	base de données d'iris URUBIS http://iris.di.ubi.pt/

V

[Vasta et al, 2009]	Mayank Vatsa, Richa Singh, Afzel Noore, Max M. Houck, "Quality-augmented fusion of level-2 and level-3 fingerprint information using DSm theory", International Journal of Approximate Reasoning, Vol. 50, pp. 51–61, 2009.
[Verlinde et al., 1998]	P. Verlinde, D. Genoud, G. Gravier, G. Chollet. "Proposition d'une stratégie de fusion de données à trois niveaux pour la vérification d'identité. XXXIII èmes journées d'études de la parole, Martigny, Switzerland, Juin 1998.

W

[Wikipédia , 2013]	Wikipédia : l'encyclopédie libre, http://fr.wikipedia.org/ date accès 2013.
[Wildes et al., 1994]	R.P. Wildes, Asmuth, J.C. ,"A System for Automated Iris Recognition", Proceeding of the Second IEEE Workshop on Applications of Computer Vision, pp.1211-1218, 1994.
[Winograd & Flores, 1989]	Winograd, T., Flores, F., "L'intelligence artificielle en question », Presses Universitaires de France, 1989.
[Wu & Mendel, 2002]	Hongwei Wu & Jerry M. Mendel, "Uncertainty Bounds and Their Use in the Design of Interval Type-2 Fuzzy Logic Systems », IEEE Transactions on fuzzy systems, Vol. 10, No. 5, October 2002.

Y

[Yang & Zhang, 2012]	Jinfeng Yang, Xu Zhang, "Feature-level fusion of fingerprint and finger-vein for personal identification", Pattern Recognition Letters, Vol. 33, pp. 623–628, 2012.
[Yu et al., 2000]	K. Yu, X. Jiang, H. Bunke, "Combining acoustic and visual-classifiers for the recognition of spoken sentences", Int. Conf. in Pattern Recognition (ICPR), Vol. 2, pp. 491-498, Barcelona, 2000.

Z

[Zadeh, 1996]	Lotfi A. Zadeh, "Fuzzy Logic = Computing with Words", IEEE Transactions on fuzzy systems, Vol. 4, No. 2, pp. 103-111, May 1996.
[Zadeh, 1997]	Lotfi A. Zadeh, "Toward a theory of fuzzy information granulation and its centrality in human reasoning and fuzzy logic", Fuzzy Sets and Systems, Vol. 90, pp. 111-127; 1997.
[Zadeh, 2008]	Lotfi A. Zadeh, "Is there a need for fuzzy logic?", Information Sciences, Vol. 178, pp. 2751-2779, 2008.
[Zenzo et al., 1996]	Zenzo, L. Cinque, and S. Levialdi, "Run-Based Algorithms for Binary Image Analysis and Processing", IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 18, no. 1, pp. 83-88. 1996.

[Zhu et al., 1999]	Y. Zhu, T. Tan, Y. Wang, "Biometric Personal Identification Based on Iris Patterns". Chinese patent Application, No. 9911025, 1999.
[Zois & Anatassopoulos, 1999]	E. Zois, V. Anastassopoulos, "Fusion of correlated decisions for writer verification". Pattern Recognition, Vol. 32, pp. 1821-1823, 1999.
[Zuev & Inavov, 1999]	Zuev, Y., Ivanov, S. "The voting as a way to increase the decision reliability". Journal of the Franklin Institute, Vol. 336(2), pp. 361–378. 1999.

Distributions intra-classe et interclasse relatives à l'appariement d'iris basé sur la distance Euclidienne.
Seuil pour l'individu 3=4.64555 Seuil pour l'individu 13 = 6.5397

	Individu 3			Individu 13		
Individu 1	6.1642	6.1912	5.9249	7.8046	7.4898	7.9505
	5.6440	5.9047	5.8828	7.9189	7.6587	7.9741
Individu 2	11.0458	10.7826	10.7921	10.6075	10.2021	10.7839
	7.5016	7.1717	6.7243	7.7663	6.7103	7.2258
Individu 3	3.2464	3.3458	3.1703	7.4195	7.2086	7.4046
	3.5243	3.6471	3.2691	7.4269	7.2852	7.6282
Individu 4	6.8552	6.9671	7.1480	7.2790	6.9143	7.4574
	6.7694	6.8339	6.9947	7.3203	6.8507	7.3797
Individu 5	7.1256	7.1845	6.7837	7.3562	6.8528	7.1213
	6.1224	6.0744	5.9830	6.5208	5.9945	6.5842
Individu 6	7.8392	7.8485	7.3227	7.4597	7.3984	7.7100
	7.6582	7.6037	7.3261	6.2697	6.4482	6.8054
Individu 7	7.4642	7.5762	7.1741	6.7999	6.6111	6.9448
	6.5937	6.4564	6.1590	6.3982	5.6754	6.0378
Individu 8	5.8544	5.5461	5.2234	7.4297	7.0634	7.4612
	7.2455	7.0964	6.7185	5.8668	6.0156	6.3267
Individu 9	7.7880	7.5691	7.4474	7.5929	6.7635	6.8271
	7.6306	7.4820	7.4977	7.3889	6.8787	7.1512
Individu 10	8.5065	8.5421	8.3387	7.8739	7.1342	7.3267
	7.8872	7.7662	7.6709	7.0762	5.9400	6.7923
Individu 11	6.4159	6.2190	6.1311	7.2543	6.7824	7.2563
	7.9588	8.0435	7.2610	7.8927	7.3819	8.0723
Individu 12	7.1083	7.1673	7.0464	7.0846	6.8354	7.0694
	7.0798	7.1629	6.6763	6.5083	6.0299	6.3909
Individu 13	8.1977	8.1206	7.8216	6.5718	4.3468	4.1815
	6.4234	6.1873	5.9757	5.9930	6.8093	7.4586

	Individu 4			Individu 5		
Individu 1	6.8784	6.8522	8.1648	6.5599	6.0938	6.1310
	6.8292	6.5105	7.5922	6.0192	5.9995	5.9994
Individu 2	10.1332	10.1246	10.4003	10.5222	9.9727	10.1240
	7.6843	7.4394	7.8794	7.3087	7.2629	7.1171
Individu 3	6.4790	6.0550	7.0484	5.7271	5.7847	5.8886
	6.9572	6.3116	6.9947	5.8762	5.8978	5.9830
Individu 4	5.3299	4.2992	3.3175	5.2763	5.9096	5.6643
	4.0716	4.3871	5.3809	5.1791	5.4759	5.5127
Individu 5	6.6208	5.7079	5.8739	5.1692	5.7655	5.5461
	5.1300	5.1688	5.5920	3.5538	4.0557	3.8264
Individu 6	6.6851	6.9822	7.4721	6.6923	6.6488	6.5073
	6.2348	6.4628	7.2690	6.1699	6.0418	6.0124
Individu 7	5.5378	5.7728	7.0902	5.7769	5.6910	5.7525
	5.6935	5.6568	6.7957	5.4663	5.4299	5.4264
Individu 8	7.1162	6.2086	6.5991	5.8436	5.8355	5.8155
	6.2676	6.2383	6.8332	6.1544	6.0956	6.1488
Individu 9	6.9340	7.0759	7.7041	6.8182	6.8688	6.5546
	5.6521	6.4121	7.4502	6.3881	6.2711	6.3122
Individu 10	6.9864	7.2003	7.9693	7.1016	7.0094	6.8398
	5.8881	6.1420	7.0724	6.0769	6.0534	5.8744
Individu 11	6.4365	5.5083	5.7436	5.1017	5.7298	5.5861
	6.8546	5.9271	6.0497	5.3811	6.1810	6.0376

Seuil pour l'individu 4 =5.22995 **Seuil pour l'individu 5= 5.4723**

Seuil pour l'individu 6=6.129555 **Seuil pour l'individu 7 = 5.8832**

	Individu 6			Individu 7		
Individu 1	7.1230	7.2854	7.6056	6.3768	5.8649	6.7347
	7.1132	7.6947	7.6856	6.7337	6.0472	6.2774
Individu 2	8.0358	8.1544	8.2887	7.3032	6.5483	6.1630
	8.0842	8.4461	8.1827	8.3226	7.1728	5.8100
Individu 3	7.1680	7.4942	6.9522	6.5385	5.8673	6.1625
	7.3499	7.7025	7.3261	7.0173	5.9139	6.1590
Individu 4	6.9467	7.7216	7.3553	6.6096	6.8967	6.2590
	6.0502	6.7361	6.4278	6.0081	6.5157	6.0524
Individu 5	6.6354	7.0155	6.3900	6.7117	6.7507	6.5269
	6.0732	6.6704	5.9504	5.9273	5.8779	5.6804
Individu 6	5.2714	6.3087	6.6545	6.2235	6.5680	6.5915
	3.6126	3.7722	5.1897	5.4756	6.1358	6.3369
Individu 7	5.9680	6.4732	6.5166	3.5073	5.1169	5.3068
	5.9710	6.4467	6.5425	6.2908	5.8683	5.9992
Individu 8	7.1450	7.5157	7.2584	7.0343	6.1790	5.8732
	6.4000	6.8776	6.6855	6.4335	6.6372	5.9141
Individu 9	7.2903	7.7511	7.7359	7.0443	6.8908	5.7345
	6.2712	6.8246	6.6246	6.2598	6.4276	6.7383
Individu 10	8.1985	8.5006	8.5164	7.6763	7.5483	7.2666
	6.6192	7.0052	7.0717	6.0019	6.1058	5.9253
Individu 11	6.9841	7.0792	6.5904	6.7729	6.2454	6.0511
	7.0594	7.1620	6.5453	7.2164	6.8493	6.5993
Individu 12	6.6872	7.1466	6.9252	6.6378	6.9030	6.1946
	6.7649	7.0573	6.9679	6.2828	6.5970	5.8843

Seuil pour l'individu 8=6.3817 **Seuil pour l'individu 9 = 7.1197**

	Individu 8			Individu 9		
Individu 1	6.5763	6.9206	6.9349	7.6545	7.2264	7.3199
	6.0808	6.5874	6.4624	7.3311	7.1956	6.9459
Individu 2	9.4064	9.7652	9.3225	9.9519	9.7301	10.4682
	6.5244	7.1892	7.0650	7.9527	7.8017	7.8087
Individu 3	5.3258	6.2332	6.4204	7.0503	6.4548	6.8935
	5.2509	6.4905	6.7185	7.2021	6.7979	7.4977
Individu 4	6.6075	6.6437	6.7457	7.0518	7.4789	7.4772
	6.4677	5.9531	5.4890	6.5040	6.8305	5.9370
Individu 5	6.5151	6.0752	6.6151	7.4898	8.2449	7.0416
	5.4745	5.2267	5.0401	6.3329	6.2635	5.9943
Individu 6	6.7882	6.8919	6.0448	7.1584	7.1775	6.8529
	6.5768	6.3701	5.8554	6.8879	6.9794	6.6537
Individu 7	7.1399	6.3917	6.3242	7.0372	7.0943	6.2949
	6.2184	5.973	5.6904	6.6368	6.7633	6.4104
Individu 8	4.7876	5.0894	5.6477	7.1255	7.1824	7.2046
	6.9629	5.3437	5.0137	6.9848	7.1700	6.9801
Individu 9	7.0893	7.4403	6.9360	7.9445	7.1494	6.2418
	6.5223	6.7253	6.2277	5.0354	5.0657	7.2921
Individu 10	7.8564	7.0073	7.0048	7.8143	7.1876	6.9223
	6.8819	6.4828	6.1658	7.1158	6.4028	6.1473
Individu 11	5.8005	5.6711	6.1323	7.1761	7.5799	6.9084
	5.8679	5.9848	6.4343	7.3404	7.8040	7.2491
Individu 12	6.0553	5.9711	5.8195	6.9488	6.8495	6.5490
	6.0015	5.8784	6.0946	6.5032	6.5206	6.7377

Seuil pour l'individu 10=5.92355 **Seuil pour l'individu 11** = 4.95855

	Individu 10			Individu 11		
Individu 1	8.0436	7.5745	7.3399	6.7184	8.5430	7.4397
	8.1212	7.6359	7.3554	6.5295	7.7346	6.8836
Individu 2	10.7662	10.5245	9.9086	10.5255	10.0839	10.8574
	8.4050	7.9292	7.3735	7.1003	6.9308	8.9191
Individu 3	8.0450	7.8529	7.4782	5.7454	7.3199	7.4852
	8.6024	8.2676	7.6709	5.6008	7.1933	7.3836
Individu 4	8.0373	8.1899	7.5065	6.5579	6.9242	6.9362
	7.0649	6.8488	6.5031	6.5650	6.8535	6.5095
Individu 5	8.8715	8.5622	8.4453	6.2595	7.1928	6.5792
	7.0510	7.2788	6.4066	5.1097	5.7962	6.2832
Individu 10	3.2222	4.0844	6.0424	8.1445	7.9261	8.1664
	5.1382	5.4405	4.7958	6.8440	7.2733	7.2553
Individu 11	8.0874	8.0562	7.5752	4.1332	4.2059	6.8536
	8.5125	8.4862	8.0192	4.1634	4.8074	7.2955

Seuil pour l'individu 12=5.3539 **Seuil pour l'individu 14 = 4.5406**

	Individu 12			Individu 14		
Individu 1	7.4568	6.5539	6.9914	7.0862	7.1272	7.8201
	7.2050	6.8120	7.0809	6.7968	7.0961	7.6777
Individu 2	7.2951	7.2300	7.3037	7.7835	7.8800	8.0804
	7.4485	8.6084	8.4308	6.6881	7.3414	8.2800
Individu 3	6.8359	5.9565	6.3526	5.9585	6.1927	7.1394
	7.4114	6.6194	6.9780	6.1438	6.3963	7.3798
Individu 4	6.3009	6.8614	6.6926	6.6762	6.8183	6.3848
	5.2399	6.2220	5.6298	6.0195	6.0731	5.9964
Individu 5	6.9908	6.8387	6.6248	6.2081	6.5115	6.3959
	5.4316	5.7977	5.1415	5.2313	5.5727	5.8524
Individu 12	4.7351	5.5239	5.7033	5.6740	6.2982	6.0871
	4.5892	5.5663	6.0089	5.7542	6.2303	6.4892
Individu 14	5.7772	6.4536	6.5104	3.7710	3.6539	6.2737
	5.8857	6.5983	6.4809	3.8499	3.5937	5.9782

Seuil pour l'individu 15=5.50835 **Seuil pour l'individu 16 = 6.5389**

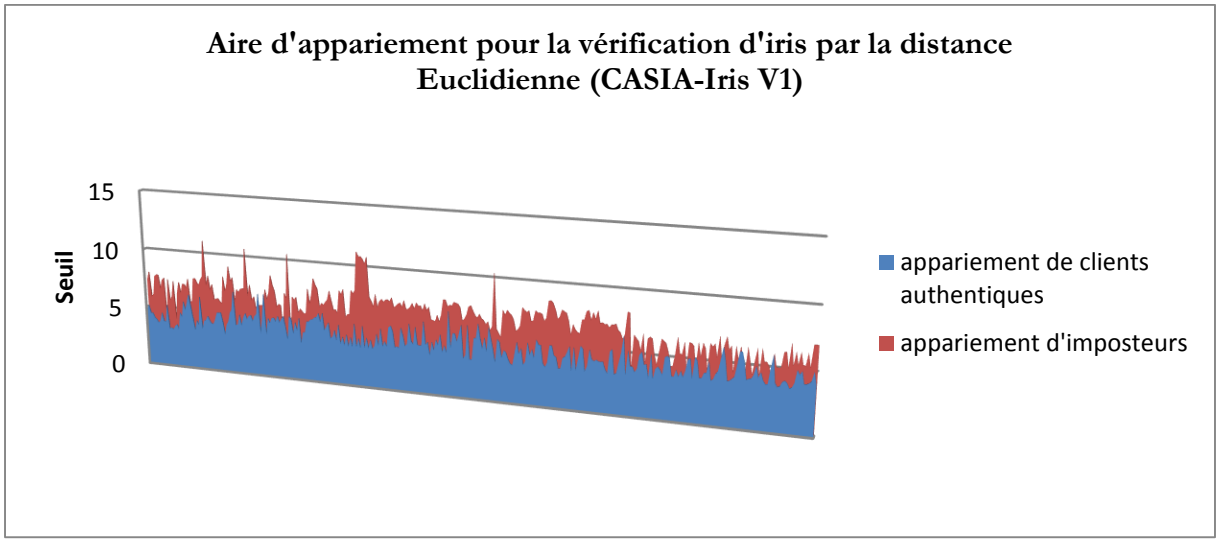
	Individu 15			Individu 16		
Individu 1	5.8773	7.1776	7.1270	7.3287	8.2570	8.0513
	6.2383	6.4350	6.9934	7.3944	8.1215	7.8314
Individu 2	7.0664	7.6648	6.9918	7.6756	7.4831	8.3037
	7.3933	6.8703	5.9322	7.5307	6.9252	7.4678
Individu 3	5.3782	6.1965	6.3651	6.8266	7.5572	7.5037
	5.4974	6.4927	6.7462	7.1847	7.4677	7.6127
Individu 4	6.4035	6.6589	6.9909	6.8849	7.4129	6.8044
	6.4565	6.3939	6.7326	5.8190	6.4897	5.8335
Individu 5	6.6424	6.5836	7.2928	6.4666	6.5817	6.3772
	5.9673	5.3728	6.0488	5.3251	6.1974	5.6117
Individu 15	5.4697	7.7614	5.7437	7.5840	7.5826	7.7234
	4.7524	5.6385	4.7020	6.4166	6.8364	6.6489
Individu 16	5.8303	6.1344	6.0981	6.8977	7.2588	6.9334
	6.9245	6.5320	6.7487	5.2968	5.2840	4.3565

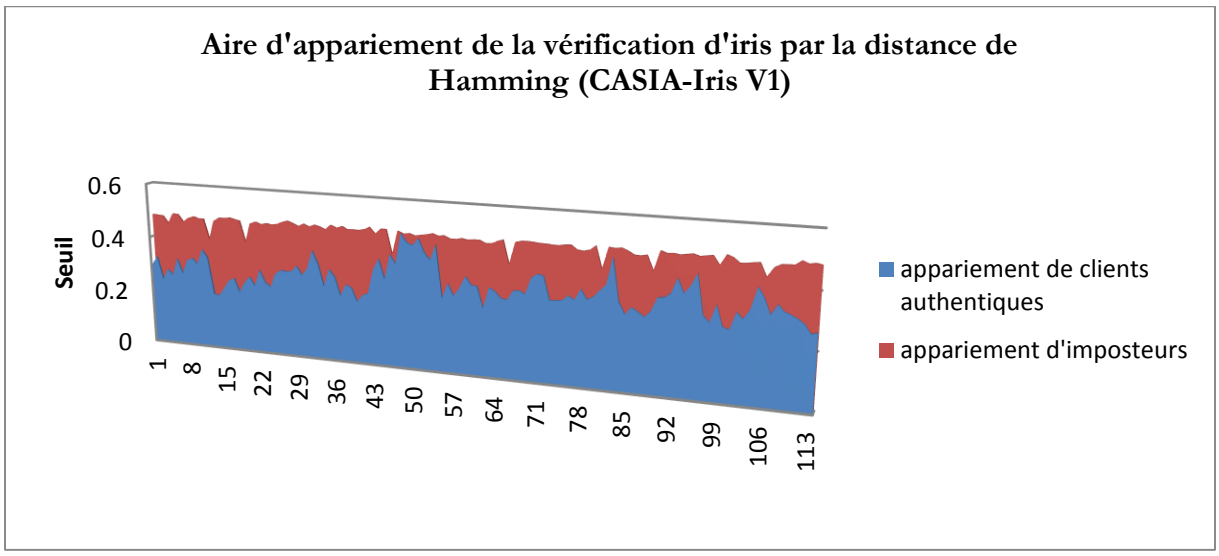
Seuil pour l'individu 17=5.5619 **Seuil pour l'individu 18 = 6.32245**

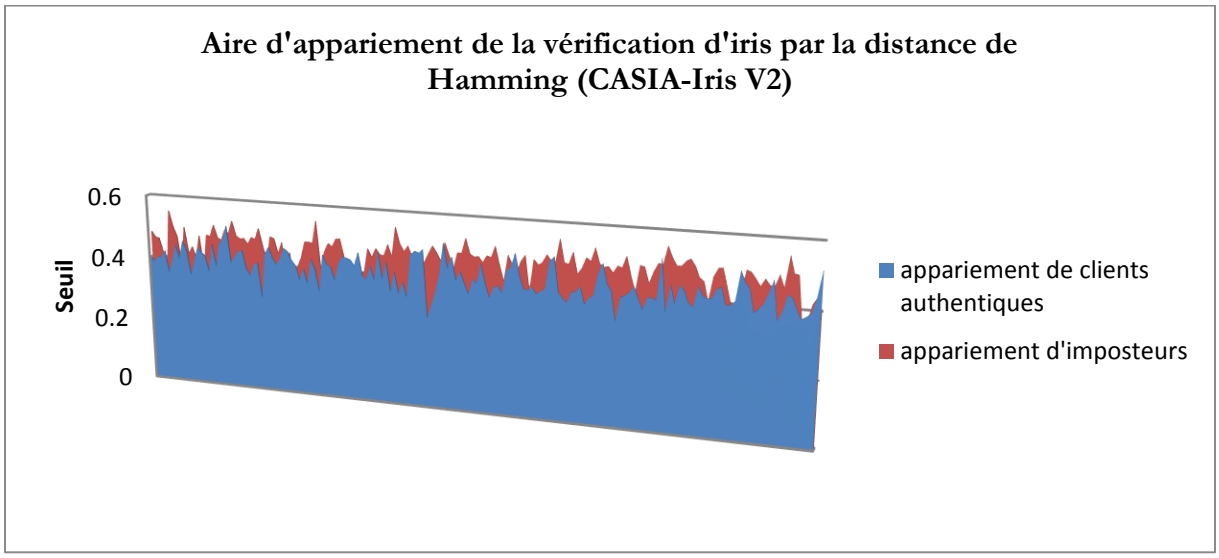
	Individu 17			Individu 18		
Individu 1	7.6247	6.7838	7.7661	6.3459	7.2288	7.4076
	7.3818	6.7575	7.3482	6.4239	7.2047	7.1470
Individu 2	8.1673	5.3451	6.8133	6.8035	6.7746	7.4001
	8.8663	6.8968	6.9852	7.4409	7.9148	7.4057
Individu 3	7.2106	6.5407	7.0506	5.9852	7.2349	6.5552
	7.6590	6.9752	7.1640	6.5780	7.6085	6.9599
Individu 4	7.5598	8.7705	7.5284	7.6575	8.2841	6.7292
	6.7112	7.8827	6.6961	6.7002	6.7969	5.5517
Individu 5	7.6210	8.4919	7.2601	7.4431	8.1985	6.8177
	6.3710	6.8286	6.3772	5.7819	6.5761	5.7379
Individu 17	3.3214	5.7787	5.0795	6.4025	7.3317	7.0606
	3.8734	4.8712	4.1674	6.0795	7.1338	6.3075
Individu 18	6.8736	7.3087	6.6169	5.2377	7.0932	6.6892
	6.7019	7.6045	7.1490	6.8756	6.4915	7.2047

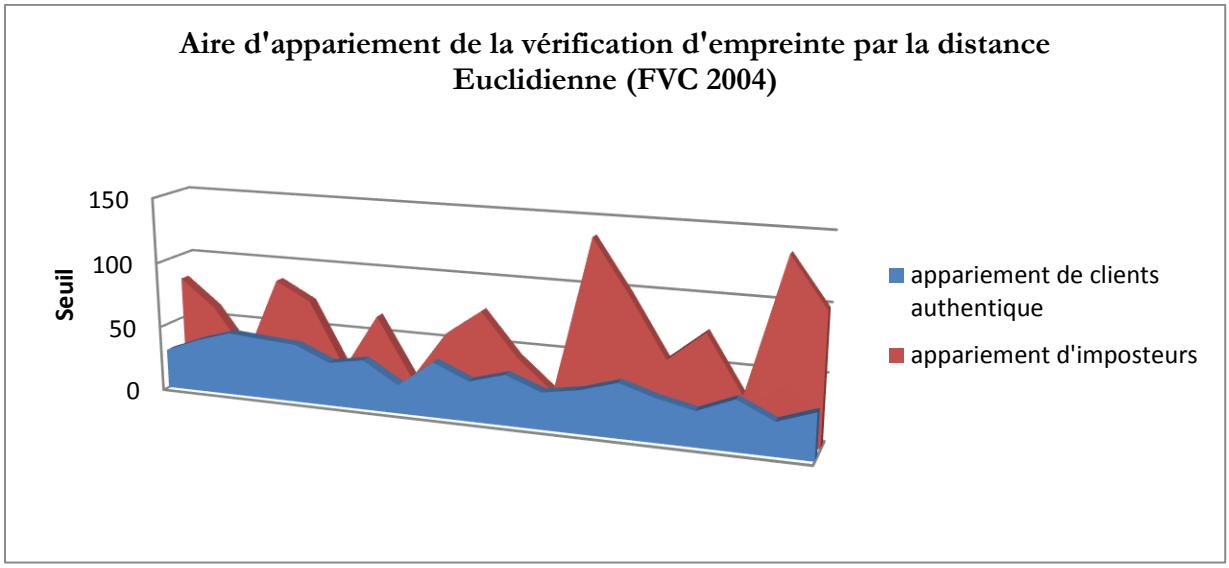
Seuil pour l'individu 19=6.2431 **Seuil pour l'individu 20 = 5.6942**

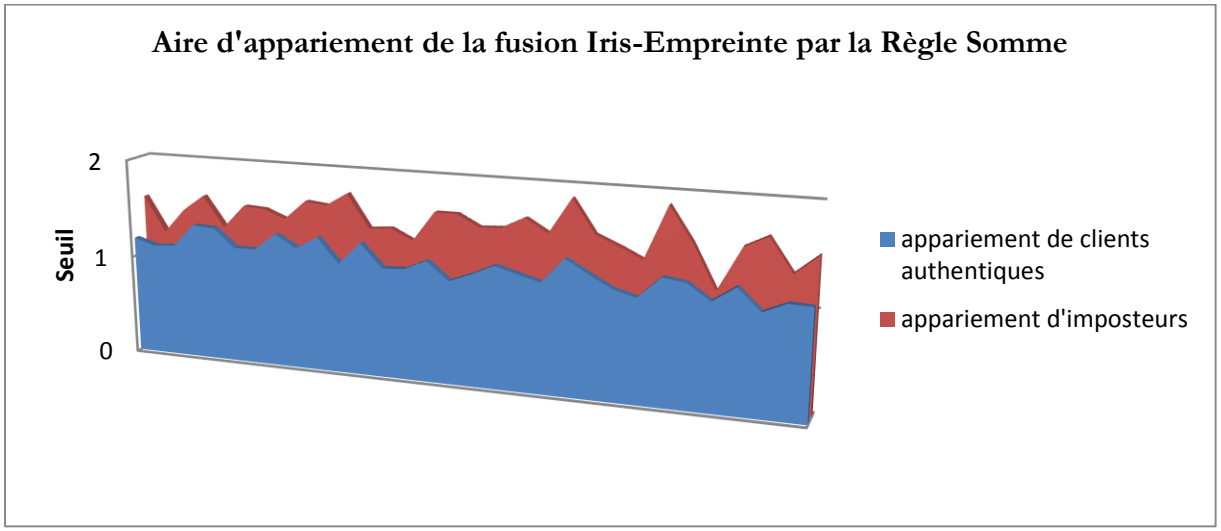
	Individu 19			Individu 20		
Individu 1	7.5326	7.3090	7.4708	6.9452	6.6311	7.1032
	6.8308	6.4158	6.7970	6.5134	5.5827	6.0255
Individu 2	5.9993	7.7707	7.1201	7.4564	6.9892	6.7559
	5.1154	6.6116	7.1523	7.1103	5.9105	5.3238
Individu 3	6.5645	5.5762	6.3812	6.4615	5.7990	6.3225
	6.7199	5.5013	6.6703	6.9830	5.8870	5.8266
Individu 4	8.2030	6.6516	6.9013	6.4617	6.5487	8.0173
	7.7091	7.0696	5.9507	5.9042	6.5067	7.7918
Individu 5	7.8324	6.1532	6.7687	6.2283	6.5797	7.9647
	6.6293	5.6603	5.6458	5.0587	5.4784	6.7692
Individu 19	6.2873	7.3708	6.9331	7.6541	7.4304	7.7796
	5.4781	5.8089	5.1278	5.4620	5.7577	6.0053
Individu 20	6.3229	6.5476	6.6163	5.8573	4.4466	4.7599
	5.2740	5.2409	6.3075	6.0646	3.8222	3.9627

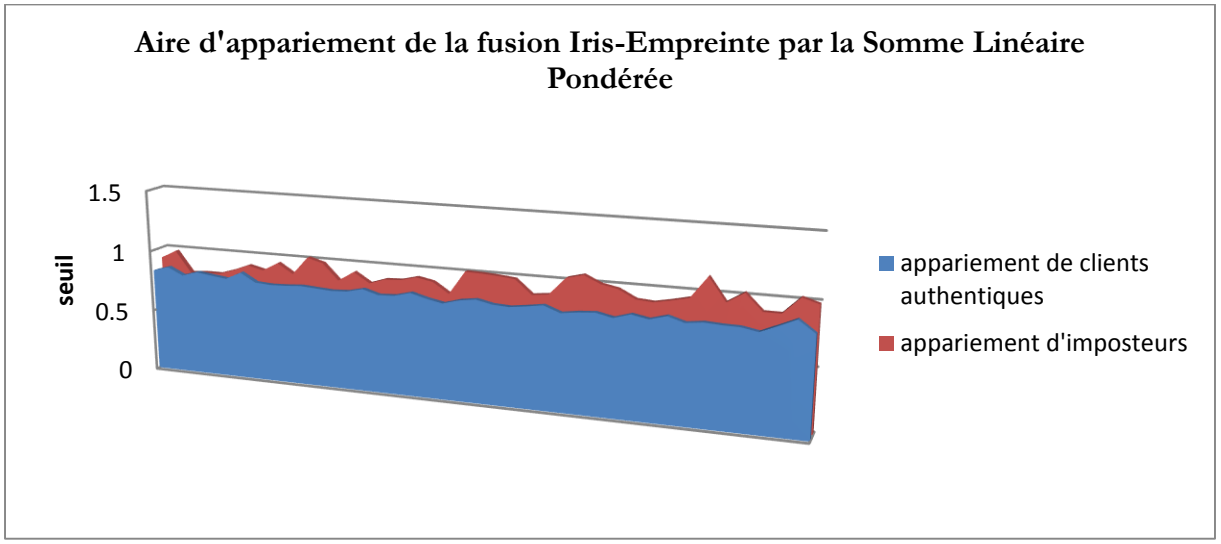

Aire d'appariement pour la vérification d'iris par la distance Euclidienne (CASIA-Iris V1)
Seuil
15
10
5
0
appariement de clients authentiques
appariement d'imposteurs


Aire d'appariement de la vérification d'iris par la distance de Hamming (CASIA-Iris V1)
Seuil
0.6
0.4
0.2
0
1
8
15
22
29
36
43
50
57
64
71
78
85
92
99
106
113
appariement de clients authentiques
appariement d'imposteurs


Aire d'appariement de la vérification d'iris par la distance de Hamming (CASIA-Iris V2)
Seuil
0.6
0.4
0.2
0
appariement de clients authentiques
appariement d'imposteurs


Aire d'appariement de la vérification d'empreinte par la distance Euclidienne (FVC 2004)
150
100
50
0
Seuil
appariement de clients authentique
appariement d'imposteurs


Aire d'appariement de la fusion Iris-Empreinte par la Règle Somme
2
1
0
Seuil
appariement de clients authentiques
appariement d'imposteurs


Aire d'appariement de la fusion Iris-Empreinte par la Somme Linéaire Pondérée
1.5
1
0.5
0
seuil
appariement de clients authentiques
appariement d'imposteurs

Distribution d'appariements de la fusion Iris-Empreinte par la Logique Floue

	Individu 2			Individu 5		
Individu 1	mauvais	mauvais	moyen	mauvais	très mauvais	mauvais
	Très mauvais	mauvais	Très mauvais	moyen	mauvais	très mauvais
Individu 2	bon	moyen	très bon	mauvais	mauvais	mauvais
	moyen	bon	moyen	moyen	moyen	mauvais
Individu 3	moyen	mauvais	mauvais	Très mauvais	mauvais	Très mauvais
	Mauvais	Très mauvais	mauvais	Très mauvais	mauvais	Très mauvais
Individu 4	Mauvais	Mauvais	très mauvais	Très mauvais	Moyen	Moyen
	mauvais	mauvais	mauvais	Mauvais	Mauvais	mauvais
Individu 5	très mauvais	Moyen	Mauvais	Très bon	Très bon	Très bon
	Mauvais	Mauvais	très mauvais	Excellent	Très bon	Très bon

	Individu 1			Individu 6		
Individu 1	bon	bon	moyen	mauvais	très mauvais	mauvais
	Très bon	bon	moyen	moyen	mauvais	très mauvais
Individu 2	très mauvais	moyen	très mauvais	mauvais	mauvais	mauvais
	moyen	mauvais	mauvais	très mauvais	moyen	mauvais
Individu 3	moyen	mauvais	mauvais	mauvais	mauvais	mauvais
	Mauvais	Très mauvais	mauvais	Très mauvais	mauvais	Très mauvais
Individu 4	Mauvais	Mauvais	très mauvais	Très mauvais	Moyen	Moyen
	mauvais	mauvais	mauvais	Mauvais	Mauvais	mauvais
Individu 5	très mauvais	Moyen	Mauvais	Très mauvais	Mauvais	Mauvais
	Mauvais	Mauvais	très mauvais	Mauvais	Très Mauvais	Très Mauvais

	Individu 4			Individu 8		
Individu 1	bonne	bonne	moyen	mauvais	très mauvais	mauvais
	Très bonne	bonne	moyen	moyen	mauvais	très mauvais
Individu 2	très mauvais	moyen	très mauvais	mauvais	mauvais	mauvais
	moyen	mauvais	moyen	moyen	moyen	mauvais
Individu 3	moyen	mauvais	mauvais	bonne	bonne	bonne
	Mauvais	Très mauvais	mauvais	Très bonne	Moyen	Très bonne
Individu 4	bon	bon	très bon	Très mauvais	Moyen	Moyen
	excellent	Très bon	Très bon	Mauvais	Mauvais	mauvais
Individu 8	très mauvais	Moyen	Mauvais	Très bon	Très bon	bon
	Mauvais	Mauvais	très mauvais	excellent	Très bon	Très bon

	Individu 6			Individu 7		
Individu 1	Très mauvais	mauvais	mauvais	mauvais	très mauvais	mauvais
	Très mauvais	mauvais	mauvais	moyen	mauvais	très mauvais
Individu 2	très mauvais	moyen	très mauvais	mauvais	mauvais	mauvais
	moyen	mauvais	moyen	mauvais	mauvais	mauvais
Individu 3	moyen	mauvais	mauvais	mauvais	mauvais	mauvais
	Mauvais	Très mauvais	mauvais	Très bonne	Moyen	Très bonne
Individu 6	bon	bon	très bon	Très mauvais	Moyen	Moyen
	bon	bon	bon	Mauvais	Mauvais	mauvais
Individu 7	très mauvais	Moyen	Mauvais	Très bon	bon	bon
	Mauvais	Mauvais	très mauvais	bon	bon	bon

	Individu 8			Individu 9		
Individu 8	Très bon	bon	bon	mauvais	très mauvais	mauvais
	Très bon	bon	bon	moyen	mauvais	très mauvais
Individu 9	très mauvais	moyen	très mauvais	bon	bon	bon
	moyen	mauvais	moyen	bon	bon	bon
Individu 10	moyen	mauvais	mauvais	mauvais	mauvais	mauvais
	Mauvais	Très mauvais	mauvais	Très bonne	Moyen	Très bonne
Individu 11	mauvais	mauvais	très mauvais	Très mauvais	Moyen	Moyen
	mauvais	mauvais	mauvais	Mauvais	Mauvais	mauvais
Individu 12	très mauvais	Moyen	Mauvais	Très mauvais	mauvais	mauvais
	Mauvais	Mauvais	très mauvais	mauvais	mauvais	mauvais

	Individu 1			Individu 12		
Individu 8	Très mauvais	mauvais	Très mauvais	mauvais	très mauvais	mauvais
	Très mauvais	Très mauvais	Très mauvais	moyen	mauvais	très mauvais
Individu 12	très mauvais	moyen	très mauvais	bon	bon	bon
	moyen	mauvais	moyen	bon	bon	bon
Individu 13	moyen	mauvais	mauvais	mauvais	mauvais	mauvais
	Mauvais	Très mauvais	mauvais	Très bonne	Moyen	Très bonne
Individu 14	mauvais	mauvais	très mauvais	Très mauvais	Moyen	Moyen
	mauvais	mauvais	mauvais	Mauvais	Mauvais	mauvais
Individu 15	très mauvais	Moyen	Mauvais	Très mauvais	mauvais	mauvais
	Mauvais	Mauvais	très mauvais	mauvais	mauvais	mauvais

	Individu 2			Individu 9		
Individu 7	Très mauvais	mauvais	Très mauvais	mauvais	très mauvais	mauvais
	Très mauvais	Très mauvais	Très mauvais	moyen	mauvais	très mauvais
Individu 8	très mauvais	moyen	très mauvais	mauvais	mauvais	mauvais
	moyen	mauvais	moyen	mauvais	mauvais	mauvais
Individu 9	moyen	mauvais	mauvais	bon	bon	bon
	Mauvais	Très mauvais	mauvais	Très bon	Moyen	Très bon
Individu 11	mauvais	mauvais	très mauvais	Très mauvais	Moyen	Moyen
	mauvais	mauvais	mauvais	Mauvais	Mauvais	mauvais
Individu 12	très mauvais	Moyen	Mauvais	Très mauvais	mauvais	mauvais
	Mauvais	Mauvais	très mauvais	mauvais	mauvais	mauvais

	Individu 2			Individu 10		
Individu 8	Très mauvais	mauvais	Très mauvais	mauvais	très mauvais	mauvais
	Très mauvais	Très mauvais	Très mauvais	moyen	mauvais	très mauvais
Individu 9	très mauvais	mauvais	très mauvais	mauvais	mauvais	mauvais
	mauvais	mauvais	Très mauvais	mauvais	mauvais	mauvais
Individu 10	moyen	mauvais	mauvais	bon	bon	bon
	Mauvais	Très mauvais	mauvais	Très bon	Moyen	Très bon
Individu 11	mauvais	mauvais	très mauvais	Très mauvais	Moyen	Moyen
	mauvais	mauvais	mauvais	Mauvais	Mauvais	mauvais
Individu 12	très mauvais	mauvais	Mauvais	Très mauvais	mauvais	mauvais
	Mauvais	Mauvais	très mauvais	mauvais	mauvais	mauvais