République Algérienne Démocratique et Populaire
Ministère de l'enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE KASDI MERBAH OUARGLA

Faculté des Nouvelles technologies de l'information et de la communication
Département de l'électronique et de télécommunication

MEMOIRE MASTER ACADEMIQUE

Domaine : Électronique
Spécialité : Automatique

Présenté par :

DJILI Abdellah **MAHDADI Djamel Eddine**

Thème

Reconnaissance de personnes utilisant la multi-représentation de l'iris

Soutenu publiquement
le : 31/05/2016

Devant le jury :

Mme	Cherif. F	MCB	Président	UKM Ouargla
Mr	Saigaa.M	MAA	Encadreur	UKM Ouargla
Mr	Meraoumia.A	MCB	Co-Encadreur	UKM Ouargla
Mr	Chenina.H	MAB	Examinateur	UKM Ouargla
Mme	Louazen. H	MAB	Examinatrice	UKM Ouargla

Année Universitaire : 2015 /2016

Dédicaces

Je dédie ce mémoire:

À mes très chers parents pour leur soutient durant toute

ma vie d'étudient et sans eux je ne serai jamais devenu

Et mes frère et mes sœurs. Et a toute ma famille.

À mes amis d'Enfance. À mes amis d'étude

A mes amis pour leurs soutiens et leurs

encouragements.

À tous les professeurs et enseignants qui m'ont suivi

durant tout mon cursus scolaire et qui m'ont permis

de réussir Dans mes études.

À toute personne ayant contribué à ce

travail de près ou de loin.

DJILI Abdellah - MAHDADI Djameleddine

Remerciement

Louange à notre Seigneur "ALLAH" qui nous a dotées de la merveilleuse faculté de raisonnement. Louange à notre Créateur qui nous a incitées à acquérir le savoir. C'est à lui que nous adressons toute notre gratitude en premier lieu.

Nous ne saurons suffisamment remercier la personne qui m'a aidé à réaliser ce travail dans les meilleures conditions mon encadreur monsieur MOHAMMED SAIGAA. Sa disponibilité, sa patience tout au long de ce travail nous a été bénéfique. Nous tenons à remercier Dr.Abdallah MERAOUMIA et Dr.Djamel SAMAI
, les doctorants Mr Ben sid et Mr Kourichi pour l' aide, et Mr Ghilani pour la disponibilité d'utilisation d'un labo dans Center de recherche laboratoire de génie électrique "LAGE".
Nous remercions
également le Président et les membres du Jury qui nous
font l'honneur d'accepter de juger notre travail. Sans
oublier bien entendu tous les enseignants qui ont
contribués par leur savoir et leurs encouragements le long
de nos parcours.

Nous avons eu la chance de travailler ou que j'ai eu l'honneur de côtoyer avant et pendant mon mémoire, et à tous mes professeurs de l'Université de KASDI MERBAH OUARGLA.

ملخص

النظام البيومتري - القياسات الحيوية - من التكنولوجيات الجديدة المعتمدة في العالم ، استعمالها مبني أساسا على تحقيق مستوى عالي من الأمن أو حفظ المعلومات المخزنة ، حيث تقوم تقنية البيومتري بمعرفة الأشخاص بشكل آلي استنادا على مميزاتهم أو خصائصهم الفيزيائية أو سلوكياتهم ، في مذكرتنا هذه تم دراسة السمة البيومترية للقزحية لكونها مستقرة ومميزاتها عالية ، وهي كذالك من السمات البيومترية الأقوى لأنظمة تحديد الهوية .

يعتمد نظام التعرف على القزحية على أربعة مراحل: تجزئة القزحية، تسوية القزحية، استخراج الخصائص مع المقارنة مع نسخ القزحية ، و استخدام طريقة القالب للمساعدة في تطبيق القوانين ، في هذه المذكرة سنحاول معرفة الأشخاص باستعمال التقديم المتعدد للقزحية .

اعتمدنا في نظام النموذج الأحادي على طريقتين و استخرجنا النتائج، وكانت مقبولة، ثم قمنا بعمل المطابقة بين الطريقتين السابقين - و هو ما يعرف بنظام النموذج المتعدد - و تحسنت النتائج أكثر .

في دراستنا هذه نفذنا الخوارزمية التعريفية و البرنامج النهائي على برنامج مطلب 2014، و استنادا على قاعدة البيانات كازيا .

كلمات مفتاحية : قزحية ، التعرف على القزحية ، قالب ،المطابقة ، نظام النموذج الأحادي، نظام النموذج المتعدد

RESUME

Les systèmes biométriques est nouvelles technologies biométriques dans le monde, un bâtiment principalement utilisé pour atteindre un niveau élevé de sécurité ou d'enregistrer des informations stockées

Lorsque la technologie biométrique de connaître les personnes automatiquement sur les caractéristiques physiques ou les comportements, Dans notre étude de ces IRIS biométrique est l'attribut d'être stables et élevés caractéristiques, qui sont des plus puissants systèmes d'identification biométrique .

Les systèmes de reconnaissance de personnes utilisant la multi-représentation l'iris comportent quatre étapes principales : la segmentation de l'iris, la normalisation de l'iris, l'extraction des caractéristiques et la comparaison des exemplaires de l'iris. Ce mémoire présente un système d'identification d'iris,

En système unimodale nous utilisons deux méthodes et extrait des résultats, était acceptables, alors nous faisons entre les méthodes anciennes et est ce qu'on appelle système multimodales et extrait de meilleurs résultats.

Les tests ont été achevés sur la base de données CASIA-Iris. Nous avons implémenté cet algorithme d'identification avec le logiciel MATLAB 2014.

Mots clés : IRIS, reconnaissance de l'iris, appariement, modèle, système unimodale, système multimodal.

Abstract

The biometrics system is new biometric technologies in the world, a building used primarily to achieve a high level of security or save stored information.

When biometric technology, know the people automatically on physical characteristics or behavior, in our study of these IRIS biometric is the attribute to be stable and high features, which are more powerful biometric identification systems.

Systems of recognition of persons using the iris multi-representations consist of four main stages: iris segmentation, normalization of the iris, the feature extraction and comparison of copies of the iris. This thesis presents a system for iris identification,

System unimodale we use two methods and extracted results, was acceptable, so we do between old methods is the so called system multimodal and provide best results.

Keywords: IRIS, iris recognition, matching, template, unimodale system,multimodal system.

Abréviation

CASIA	Chinese Academy of Sciences, Institut of Automation
CHT	Circulaire de Hough transformée (Circular Hough transform)
CL	Client
ERR	Taux d'erreurs égales ("Equal Error Rate")
FAR	Taux de Fausses Acceptations ("False Acceptance Rate")
FRR	Taux de Faux Rejets ("False Reject Rate")
GAR	Jute accepte des taux("Gunnies Accept Rate")
HD	distance de Hamming (Hamming Distance)
IM	Imposture
MACE	l'énergie de corrélation moyenne minimale (Minimize the Average Correlation Energy)
MAX	Maximum
MIN	Minimum
M-P	Mace PEAK
M-PSR	Mace PSR
MUL	Multiplication
ROC	Courbe représentant les taux d'erreur ("Receiver Operating Curve")
SOM_P	Somme Pondéré
SOM	Somme

Table des matières

Liste des Figures

Chapitre 03

Liste des tableaux

Introduction général

Dans un court laps de temps, la biométrie est devenue l'une des technologies les plus pertinentes utilisées dans les technologies de sécurité de l'information (TI). Cette technologie offre non seulement un mécanisme pour la protection des biens, mais garantit également que la personne qui veut avoir accès à eux est la vraie personne autorisée. Cela est dû au fait que la biométrie consiste en la reconnaissance automatique des individus en analysant les caractéristiques de l'être humain intrinsèques qui ne peuvent être facilement oubliées, perdues, échangé ou volé, car il peut se produire avec des mots de passe ou des cartes. Merci à cette propriété, au cours de la dernière décennie, la reconnaissance biométrique a été considérée comme la solution la plus appropriée pour des applications qui implique une authentification de sécurité telles que le contrôle d'accès, le contrôle des frontières, les services bancaires, etc.

Néanmoins, bien que la technologie de la biométrie est plus fiable pour les personnes de reconnaissance que d'autres technologies d'identification informatiques tels que la possession ou des mots de passe, cette technologie a deux vulnérabilités inhérentes. De nombreuses modalités sont aujourd'hui inventées pour des applications biométriques. On peut citer des modalités physiologiques comme : le visage, l'iris, la rétine, la forme de la main et d'autres comportementales comme : la voix, la frappe de clavier. Toute cette variété de modalités biométriques a donné naissance à divers produits commerciaux intégrant des systèmes biométriques. Ce sont des systèmes, dans la plus part des cas, monomodaux s'appuyant sur le témoignage d'une seule source d'information issue d'une seule modalité biométrique.

Les systèmes biométriques utilisant une seule biométrie (appelés systèmes monomodaux) possède trois limitations principales : une limitation en termes de performances, une limitation en termes d'universalité d'utilisation et une limitation en termes de détection des fraudes. Ce qui a donné naissance à la biométrie multimodale qui se base sur la combinaison de diverses informations de différentes sources biométriques.

Ces sources peuvent êtres différentes instances de la même modalité, des modalités biométriques différentes, plusieurs prototypes d'une modalité issues de plusieurs capteurs ou plusieurs informations issues de plusieurs algorithmes d'extractions de caractéristiques d'une seule modalité. Ainsi, des études ont démontrés que ces systèmes biométriques multimodaux

peuvent obtenir de meilleures performances par rapport aux systèmes monomodaux [14]. Pour cette raison, les systèmes biométriques multimodaux sont adaptés à de nombreux domaines d'applications.

Dans ce travail nous intéressons à la modalité de L'iris, L'iris est une modalité biométrique jugée parmi les plus fiables modalités. Pour ce avons choisi l'iris l'utiliser par notre système biométrique. L'iris est la zone colorée située entre le blanc de l'œil et la pupille, c'est le seul organe interne humain visible de l'extérieur, il est stable durant la vie d'une personne. La texture de l'iris est unique pour chaque œil d'une personne, c'est une combinaison de plusieurs éléments qui font d'elle l'une des textures distinctives les plus riches du corps humain. L'iris présente donc une caractéristique unique qui est d'être à la fois un organe protégé de l'environnement extérieur en même temps qu'il est relativement facile à acquérir comparé aux autres organes internes du corps humain comme par exemple la rétine.

La reconnaissance par l'iris a fait l'objectif de notre système multi-représentation proposé, ce système est composé de deux algorithmes, le 1er algorithme on a utilisé le filtre MACE pour le calcul de premier score et le filtre de Gabor 1D pour le deuxième score, la combinaison de ces scores au niveau scores.

Ce manuscrite est composé de trois chapitres :

- Dans le 1er chapitre nous présenterons les notions de base de la biométrie et nous présentons aussi un système biométrique en général, les mesures de performance adaptée pour la biométrie.
- Dans le chapitre nous présenterons les systèmes unimodale et leur limitation en termes de robustesse et éclairons les avantages des systèmes multimodal, puis on présenterons notre système multi-représentation proposé.
- Le chapitre 3 est réservé aux résultats expérimentaux, l'évaluation de performance de système proposé est faite sur une base de données de CASIA.

Chapitre 01

Introduction à la biométrie

1.1.Introduction

La croissance rapide de l'utilisation des applications Internet et la grande préoccupation de la sécurité nécessitent une identification personnelle fiable et automatique.

Les systèmes traditionnelles d'identification personnelle automatiques peuvent être divisés en deux catégories: la connaissance, comme un mot de passe et à base de puce, comme une clé physique, une carte d'identité et un passeport. Cependant, ces approches ont des limitations. Dans l'approche basée sur la connaissance, dans une certaine mesure, la «connaissance» peut être deviné, oublié ou partagé. Dans l'approche basée sur les puces, le "puce" peut être facilement volé ou perdu.

D'autre part, ce chapitre introduit la technologie biométrique à partir d'un point de vue technique considérant à la fois les systèmes biométriques et sa fonctionnalité. A cet effet, un modèle général des systèmes biométriques, y compris ses différents composants et leurs interactions sont expliquées. En outre, les fonctions biométriques pour compléter le processus de reconnaissance sont fournies pour la phase de l'enrôlement et la phase de reconnaissance (vérification et identification).

1.2.Biométrie

Depuis son existence, l'homme a toujours essayé de trouver les différences existantes entre lui-même et son entourage et les exploiter dans ses besoins quotidiens.

Les chinois ont été les premiers à utiliser, il y a 1000 ans, les empreintes digitales à des fins de signature de documents. Après, c'était le tour de l'anatomiste Marcello Malpighi (1628–1694) qui les a étudiées avec un nouvel instrument nommé microscope.

Puis le physiologiste tchèque Jan Evangelista Purkinge (1787–1869) a essayé de les catégoriser selon certaines caractéristiques.Vers la fin du XIXè siècle, le Dr Henry Faulds (1843–1930), chirurgien à Tokyo, a marqué le premier pas vers l'élaboration d'un système d'identification d'individus en se basant sur des méthodes statistiques pour la classification des empreintes. [1].

En ce moment, un de ses contemporains, le français Alphonse Bertillon (1853- 1914), était en train de tester une méthode d'identification des prisonniers nommée anthropométrie judiciaire. Bertillon procédait à la prise de photographies de sujets humains, mesurait certaines parties de leurs corps (tête, membres, etc.) et on notait les dimensions sur les photos et sur des fiches à des fins d'identification ultérieure. C'était la naissance de la première base de données contenant des informations des individus. [1].

Et depuis, ces systèmes de reconnaissance ne cessent de se développer et de devenir plus performants.

La biométrie est un terme dérivé du mot grec «bio» (la vie) et «métrie» (mesure) et il se réfère à l'analyse statistique des observations et des phénomènes biologiques [1]. Néanmoins, au cours des dernières décennies, ce terme a également été utilisé comme une abréviation de "reconnaissance biométrique" dans certains domaines tels que la sécurité de l'information et l'authentification physique [2]. Actuellement la biométrie a une définition plus spécifique, comme la reconnaissance automatique des individus en fonction de leurs caractéristiques comportementales et biologiques.

La biométrie consiste en l'analyse mathématique des caractéristiques biologiques d'une personne et a pour objectif de déterminer son identité de manière irréfutable. Contrairement à ce que l'on sait ou ce que l'on possède la biométrie est basée sur ce que l'on est et permet ainsi d'éviter la duplication, le vol, l'oubli ou la perte.

La biométrie offre une solution naturelle est fiable pour certains aspects de la gestion d'identité en utilisant des systèmes entièrement automatisés ou semi-automatisés de reconnaissance des individus [3]. Un système biométrique typique utilise les sondes convenablement conçues pour capturer le trait biométrique d'une personne et le compare à l'information stockée dans une base de données pour établir l'identité[4].

1.3.Propriétés d'une modalité biométrique

Les systèmes biométriques automatiques doivent identifier un individu ou vérifier son identité en utilisant des mesures des caractéristiques du corps humain .Chaque trait biométrique a ses avantages et ses inconvénients, c'est pourquoi, le choix de la technique pour une application particulière dépend d'une variété de questions en plus de sa performance [5] ont identifié sept facteurs déterminant la convenance des traits physiques ou comportementaux pour être utilisés dans une application biométrique [6].

- Universalité : toute personne ayant accès à l'application doit posséder le trait.
- Unicité : le trait doit être suffisamment différent d'une personne à une autre.
- La permanence: ceci signifie que le trait biométrique ne change pas dans le temps.
- Mesurabilité : il devrait être possible d'acquérir et de numériser les données biométriques à l'aide d'un dispositif approprié.

- La performance: ceci spécifie non seulement la réalisation d'une vérification exacte, mais également les conditions de ressource de réaliser avec exactitude une vérification acceptable.
- La robustesse: ceci se rapporte à l'influence du fonctionnement ou des facteurs environnementaux (canal, bruit, déformations...) qui affectent l'exactitude de la vérification [7].
- Acceptabilité : les individus qui vont utiliser cette application doivent être disposés à présenter leurs traits biométriques au système.

Depuis que la biométrie se présente comme une nouvelle technologie de reconnaissance, plusieurs caractéristiques qui correspondent aux propriétés ci-dessus, dans une mesure plus ou moins ont été découvertes. À son tour, chacune de ces caractéristiques a provoqué l'émergence de différentes modalités biométriques. Un aperçu de ces modalités sont décrites dans la section suivante.

1.4.Différentes modalités biométriques

En fonction de la caractéristique biométrique utilisée dans le processus de reconnaissance, un large éventail de techniques de reconnaissance des individus existe. Formellement, chacune de ces techniques nommé modalité biométrique (*Figure 1.1*) Considérant une classification préliminaire, ces modalités peuvent être divisées en deux groupes principaux [8]:

1.4.1. ***Les modalités physiques*** (également nommés statique ou passive). Ces modalités sont basées sur les caractéristiques anatomiques ou physiologiques. Ces caractéristiques sont obtenues sans qu'il soit nécessaire que les utilisateurs effectuent une action spécifique. Les modalités les plus communes qui appartiennent à ce groupe sont: empreintes digitales, le visage, l'iris, la rétine, la main / géométrie de doigt, la paume, la reconnaissance des formes vasculaires et de l'ADN. Il y a aussi de nouvelles modalités telles que la forme de l'oreille ou l'odeur corporelle.

Empreinte digitale : L'identification à l'aide des empreintes digitales est la technique biométrique que la plupart de gens connaissent. Il s'agit de la plus vieille technique biométrique [9], les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Ces éléments sont appelés minuties [10].

L'utilisation est facile, il suffit de poser le doigt au dessus du lecteur, mais certaines personnes peuvent créer de "faux doigts" [09]

Visage : Le visage est sujet à une variabilité tant naturelle (vieillissement, par exemple) que volontaire (des produits de beauté, chirurgie esthétique, grimaces...etc.). Cette réalité demeurera un défi pour des systèmes d'identification de visage.

La reconnaissance du visage est utilisée comme système de surveillance ou d'identification par les autorités ou les corps policiers principalement dans les lieux publics. Elle est parmi les techniques les plus acceptables, mais elle nécessite un arrière plan simple et fixe pour que le résultat soit précis [9].

L'iris : L'iris est la partie colorée de l'œil qui entoure la pupille noire. L'acquisition de l'iris est effectuée au moyen d'une caméra pour pallier aux mouvements inévitables de la pupille. Son inspection attentive révèle de nombreuses structures détaillées uniques et indépendantes du code génétique de l'individu et pratiquement ne varient pas pendant la vie.

1.4.2. ***Les modalités comportementales*** (également nommées dynamique ou active): Ces modalités sont basées sur les caractéristiques biométriques qui impliquent l'exécution de certaines activités. Cette activité entraîne un comportement qui a été appris ou acquis au fil du temps. Ces modalités sont la signature dynamique, frappe, et l'une des plus récentes reconnaissances de la, démarche. reconnaissance vocale est également une autre modalité biométrique qui pourrait être classé dans ce groupe, même si elle implique vraiment les caractéristiques physiques et comportementales.

Écriture (signature) : La vérification par signature comme technique est parmi les premières utilisées dans le domaine de la biométrie. Elle se base généralement sur le fait que l'utilisateur signe avec un stylo électronique sur une palette graphique. Il ya plusieurs systèmes concurrents dans ce domaine analysant les caractéristiques spécifiques d'une signature comme précision géométrique, variations de vitesse, pression exercée sur le crayon, le mouvement, les points et les intervalles de temps où le crayon est levé….etc. Ces données sont enregistrées pour comparaison ultérieure. Certains systèmes ne font qu'enregistrer l'image statique de la signature pour comparaison [10].

Voix humaine : est une caractéristique biométrique intéressante, puisqu'elle dépond des facteurs comportementaux et physiologiques. Initialement une table de référence de la voix d'une personne doit être construite. Pour ce faire, celle-ci doit lire une série de phrases ou de

mots à plusieurs reprises. L'identification par la voie est basée sur la forme et la taille des appendices (bouche, cavités nasales et les lèvres) utilisées dans la synthèse du son.

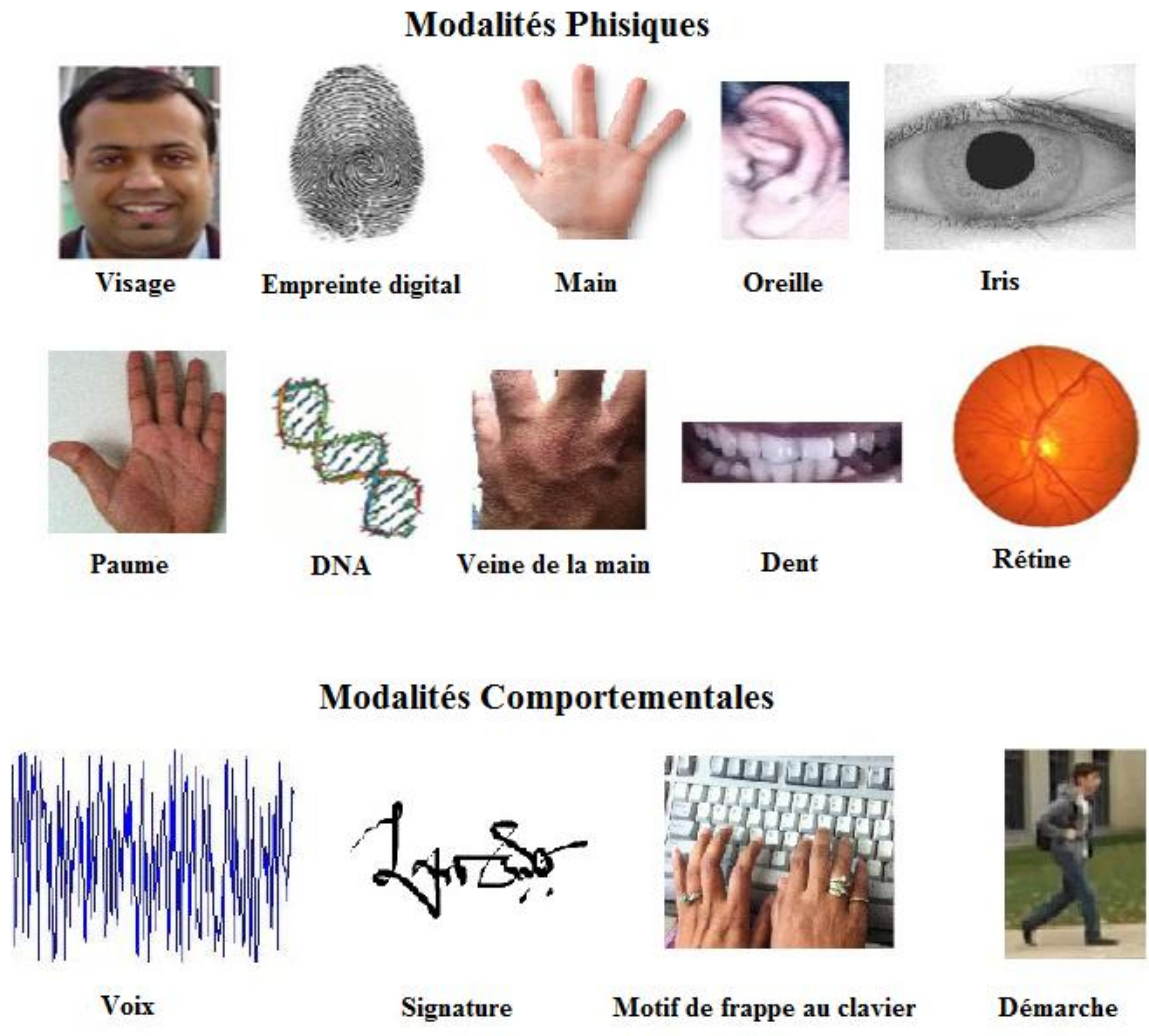


Figure 1.1 :-Différentes modalités biométriques physiques et comportementales

Démarche : Il s'agit de reconnaître un individu par sa façon de marcher et de bouger. En analysant les déformations des jambes et bras au niveau des articulations. La démarche serait en effet étroitement associée à la musculature naturelle donc elle est très personnelle [4], l'intérêt de cette technologie réside que l'identification de démarche se situe dans la capacité d'identifier un individu à distance.

Dynamique de frappe au clavier : Un tel système est peu coûteux, mais pas celui ci car il ne nécessite pas de matériel d'acquisition autre que le clavier de l'ordinateur. Il s'agit d'un dispositif logiciel qui calcule la durée entre frappes, fréquence des erreurs où son temps de relâchement « Software Only », cette mesure est capturée environ mille fois par seconde, elle est appliquée au mot de passe qui devient ainsi beaucoup plus difficile à «imiter », lors de la

mise en place de cette technique il est demandé à l'utilisateur de saisir son mot de passe une dizaine de fois de suite.

L'existence d'un grand nombre de modalités biométriques ainsi que leur éventuelle combinaisons provoquent qu'il existe plusieurs types de systèmes biométriques. Chacun d'eux est mis en œuvre avec dispositif de capture biométrique approprié et algorithmes pour acquérir et traiter les caractéristiques biométriques correspondant. La section suivante vous expliquera en détail ces systèmes.

1.5.Structure d'un système biométrique

La structure d'un système biométrique est toujours la même et comprend deux phases distinctes : l'enregistrement et l'authentification pour une application de vérification ou identification.

Un système biométrique comprend 4 modules (*Figure 1.2)* dont certains sont communs à la phase d'enregistrement et à celle d'authentification : l'acquisition, l'extraction des caractéristiques, la comparaison et la décision.

L'acquisition et l'extraction de caractéristiques ont lieu lors de l'enregistrement et lors de l'authentification. L'extraction de caractéristiques est une représentation de la donnée (par exemple image ou signal temporel acquis) sous la forme d'un vecteur que l'on cherche à être à la fois représentatif de la donnée et discriminant vis à vis des autres données (issues d'autres personnes). Lors de l'enregistrement, le vecteur des caractéristiques extrait de l'échantillon biométrique est appelé référence et est stocké sur le support personnel ou dans une base de données selon l'application. Lors de la phase d'authentification, les modules d'acquisition et d'extraction de caractéristiques permettent d'obtenir une représentation de la donnée biométrique à tester dans l'espace des caractéristiques.

Le module de comparaison est utilisé lors de la phase d'authentification pour comparer les vecteurs de caractéristiques de référence et de test.

Le module de décision sert ensuite à prendre une décision à partir de la sortie du module de comparaison qui correspond à un score de similarité entre les deux vecteurs de caractéristiques (souvent un nombre réel entre 0 et 1).

Pour les systèmes de vérification la comparaison n'est faite qu'une fois entre la référence stockée sur le support personnel et les données de test, et la décision est du type OUI/NON.

Pour les systèmes d'identification la comparaison est faite avec toutes les références stockées dans la base de données et la décision est la réponse à la question, est-ce que cette personne est dans la base de données, et si oui qui est-elle ?

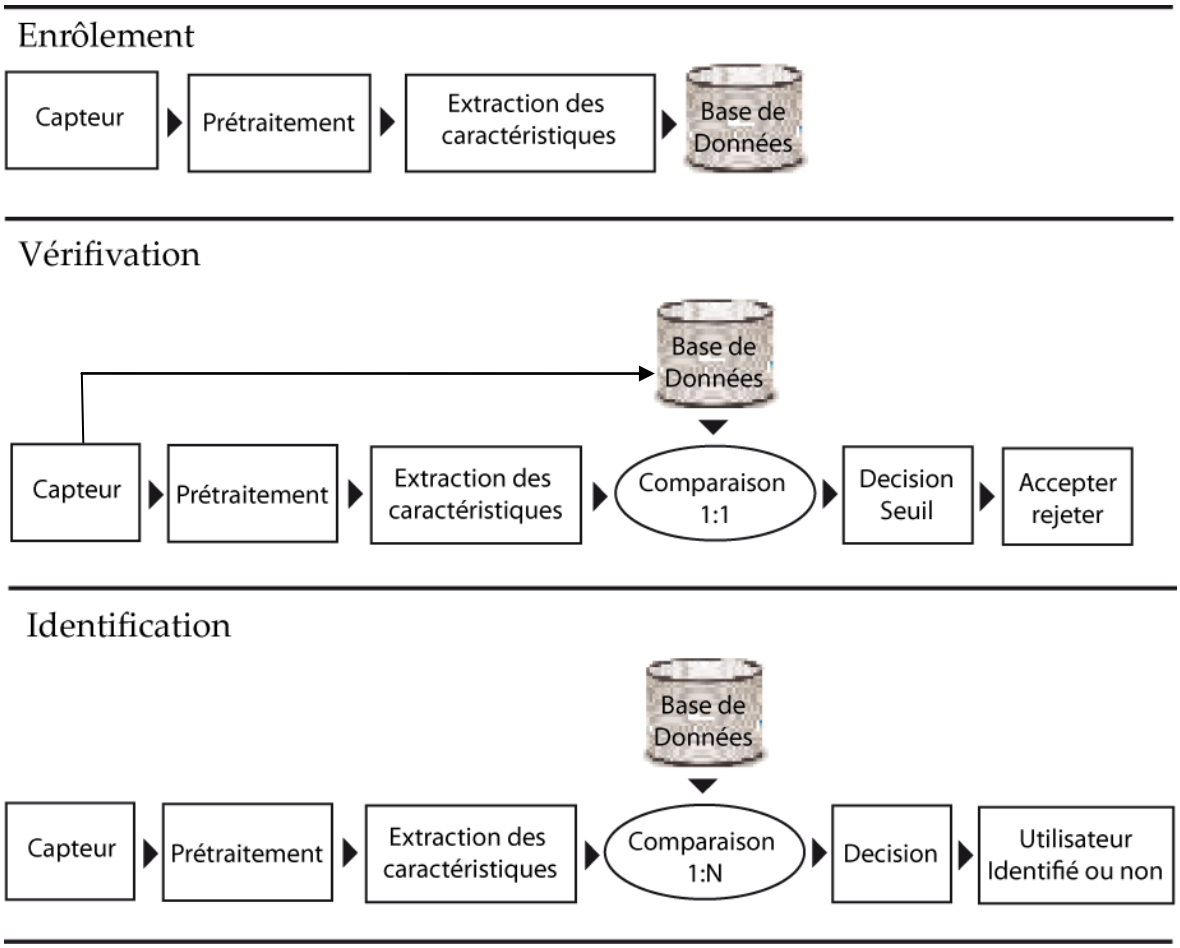


Figure 1.2 : Structure d'un système biométriques

1.6.Terminologie propre à la biométrie

Dans cette section, un ensemble de termes couramment utilisés dans la communauté biométrique est représenté.

- Un utilisateur client : est un utilisateur qui enregistre dans un système biométrique ;
- Un utilisateur Imposteur : est une personne qui n'enregistre pas dans le système, mais tente de l'utiliser.
- Gabarit : est une représentation de caractéristiques biométriques stockées dans une base de données du système.
- Le score Matching : est une valeur numérique qui représente la similitude ou de dissemblance entre deux signaux biométriques.

- Score de correspondance des clients : est un score de correspondance qui est générée en faisant comparaison deux signaux biométriques (par exemple des images du visage) de la même caractéristique biométrique (par exemple du visage).
- Score de correspondance des imposteurs : est un score de correspondance qui est générée en faisant correspondre deux signaux biométriques à partir de deux traits biométriques différents.
- La distribution des clients : est une distribution des scores correspondants clients.
- La distribution des Imposteurs est une distribution des scores correspondants imposteurs.
- Le système de vérification : est un système biométrique qui effectue une à une correspondance. Les utilisateurs sont tenus de fournir les identités des utilisateurs, les cartes à puce ou d'autres possessions pour récupérer leurs modèles dans la base de données. Selon le score de correspondance généré en comparant un signal biométrique d'entrée et le modèle récupéré, le système accepte ou rejette qu'ils sont de la même caractéristique biométrique
- Un système d'identification d'ensemble fermé : est un système biométrique qui effectue un à plusieurs matching. Un signal biométrique d'entrée est adaptée à tous les modèles dans la base de données. Le système classe les modèles en fonction de leurs scores correspondants.
- Un système d'identification d'ensemble ouverte : est une combinaison d'un système d'identification d'ensemble fermée et un système de vérification. Il récupère le premier rang du modèle, puis effectue une vérification.
- Taux d'acceptation client("Gunnies Accept Rate") (GAR) : est la probabilité ou le pourcentage d'un système de vérification de vérifier correctement un utilisateur client.
- Taux de fausse acceptation("False Acceptance Rate") (FAR) : est la probabilité ou le pourcentage d'un système de vérification en reconnaissant un utilisateur imposteur comme un utilisateur client.
- Taux de faux rejets("False Reject Rate") (FRR) : est la probabilité ou le pourcentage d'un système de vérification en reconnaissant un utilisateur client comme un utilisateur imposteur.

- Courbe ROC (Receiver operating characteristic curve) : cette courbe constitue l'une des méthodes les plus couramment utilisées afin d'évaluer la performance globale d'un système d'authentification biométrique. La courbe ROC représente la relation entre le taux de fausses acceptations (FAR) et le taux de faux rejets (FRR) pour les différentes valeurs du seuil de décision, respectivement en abscisses et en ordonnées.

1.7.Fonctionnent d'un système biométrie

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Selon le contexte de l'application, un système biométrique peut fonctionner en deux modes :

1.7.1. Enrôlement :

L'enrôlement est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier. Plusieurs campagnes d'acquisitions de données peuvent être réalisées afin d'assurer une certaine robustesse au système de reconnaissance aux variations temporelles des données.

Pendant cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis représentées sous forme numérique (signatures), et enfin stockées dans la base de données.

1.7.2. Reconnaissance (teste):

La reconnaissance est la fonction biométrique qui reconnaît les personnes au sens strict. Cependant, il existe deux méthodes possibles pour mener à bien cette fonction: la vérification et l'identification.

Vérification ou authentification : est une comparaison "un à un", dans lequel le système valide l'identité d'une personne en comparant les données biométriques saisie avec le modèle biométrique de cette personne stockée dans la base de données du système.

Identification: est une comparaison "un à N", dans lequel le système reconnaît un individu en l'appariant avec un des modèles de la base de données. La personne peut ne pas être dans la base de données. Ce mode consiste à associer une identité à une personne. Elle ajoute la possibilité de vérifier si l'utilisateur appartient réellement à la base de données « Qui suis-je ? » [09].

Le processus d'identification peut être de deux types: l'identification de l'ensemble ouvert, dans lequel toutes sortes de gens vont utiliser le système biométrique, et

l'identification-ensemble fermé, dans lequel seul un ensemble spécifique de gens vont l'utiliser.

1.8.Application de la biométrie

Les applications de la biométrie peuvent être très diverses; les limitations ne peuvent être que l'imagination d'un individu. Il est devenu alors que le collecteur des modèles différents sont utilisés dans différentes zones pour différents types de fonctionnalités. Quelques applications de la biométrie dans les différents secteurs sont présentées:

- Les propriétaires sont facilitées par la biométrie coffre-fort et serrures biométriques, qui permettent la plus grande sécurité et de fiabilité.
- Entrée de petits bureaux ou de grandes organisations, résidentielles, les institutions et le gouvernement peuvent être garantis grandement avec l'utilisation de systèmes de contrôle d'accès biométriques.
- La mise en œuvre de la biométrie dans les services financiers tels que les guichets automatiques, les kiosques, l'enregistrement de compte bancaire permet d'individualiser et de garder l'intimité privée.
- Dans des domaines tels que les services sociaux et les soins de santé, la biométrie peut éviter les droits frauduleuses et de renforcer la vie privée des dossiers médicaux.
- Dans les dispositifs électroniques, tels que les téléphones intelligents, les tablettes, les cartes téléphoniques, les ordinateurs personnels, l'accès au réseau, l'accès et la connexion à Internet peut être pris énormément privé et sécurisé.
- La biométrie est largement utilisée dans l'application de la loi, par exemple, la personnalisation de permis de conduire, l'identification contrôlée dans les établissements correctionnels et des prisons, des fusils intelligents, le confinement de la maison et des appartements, des enquêtes, l'identification et l'authentification des criminels avec une grande précision, une meilleure sécurité de l'aéroport. [12]

La variation des applications avancées ci-dessus, montre la polyvalence et la large gamme de facilité d'utilisation des systèmes biométriques qui ne se limite pas à un usage individuel, ni est-il uniquement aux buts juridiques; il est l'outil de chacun pour assurer Droit à la vie privée et la véritable pratique d'identification.

1.9.Evaluation des performances des systèmes biométriques

Une question qui se pose souvent dans ce domaine est la suivante :
« Quelle est la meilleure technique biométrique ? » La réponse naturellement est qu'il n'y a aucune meilleure technique biométrique en termes absolus, tout dépend de la nature précise de l'application et des raisons de son exécution. L'International Biométrique Group [IBG] à effectué une étude basée sur quatre critères d'évaluation :

Intrusivité : l'existence d'un contact direct entre le capteur utilisé et l'individu à Reconnaitre, comme la reconnaissance par l'iris qui est jugée comme étant intrusive

Fiabilité : Elle dépend de la qualité de l'environnement (éclairage par exemple) dans lequel se trouve l'utilisateur. Ce critère influe sur la reconnaissance de l'utilisateur par le système.

Coût : Il se doit d'être modéré, c'est-à-dire que la collecte de l'information ne doit pas être relativement coûteuse pour établir une base de données, exemple : pour une reconnaissance de l'iris un appareil photo numérique d'une certaine qualité est nécessaire.

Effort : Il est requis par l'utilisateur lors de la saisie de mesures biométrique, et il doit être réduit le le plus possible.

Au même temps, On représentant par définir les différentes mesures des taux d'erreur en vérification d'identité des systèmes biométriques et les courbe de performance. Ensuite, nous présenterons les points de fonctionnement et son déférent type et les points de fonctionnement.

Pour estimer les performances d'un système biométrique, Philips et al. ont définit trois types d'évaluation différenciés par le niveau de spécificité d'une application l'évaluation technologique, l'évaluation de scénario et l'évaluation opérationnelle.

1.9.1. Mesures des taux d'erreur

Nous allons nous concentrer sur l'évaluation "technologique" des systèmes biométriques, c'est-à-dire, une évaluation de leurs taux d'erreurs pour la vérification d'identité en utilisant une base de données biométriques, Il y a donc des "erreurs" des systèmes biométriques que nous ne traiterons pas car elles dépendent du module d'acquisition. Ces "erreurs" sont en réalité des impossibilités d'acquisition.

Lorsque l'on évalue la partie "algorithmique" des systèmes biométriques on encore détecter deux types d'erreur :

Impossibilités de comparaison : (dépend du module d'extraction ou du module de comparaison) : Ce type d'erreur est dû au module de traitement (extraction et comparaison) qui contient en général une partie contrôle qualité. Si le système est incapable de fournir un score associé à une comparaison on parle alors d'impossibilité de comparaison ("failure to match" en anglais).

Erreurs de classification : (dépend du module de décision et donc du seuil de décision) : Il existe 2 types d'erreurs de classification correspondant aux mauvaises décisions pour les 2 classes (Client et Imposteur) mesurées de manière différente. Ces erreurs de décision sont de deux types :

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.

Lors de l'évaluation d'un système de vérification sur une base de données, on mesure des taux d'erreur sur cette base.

Taux de Fausses Acceptations FAR (False Acceptance Rate). Ce taux représente le pourcentage d'individus reconnus par le système biométrique alors qu'ils n'auraient pas dû l'être. Le système classe alors deux caractéristiques provenant de deux personnes différentes comme appartient à la même personne (indique la probabilité qu'un utilisateur soit reconnu comme quelqu'un d'autre) [4], [09].

$$FAR = \frac{Nombre\ des\ imposteurs\ acceptés}{Nombre\ totale\ d'accès\ imposteurs}. \qquad (Eq.\ 1.1)$$

Taux de Faux Rejets FRR (False Rejection Rate). Ce taux représente le pourcentage d'individus censés être reconnus par le système mais qui sont rejetés. Le système classe alors deux caractéristiques biométriques provenant de la même personne comme provenant de deux personnes différentes (indique la probabilité qu'un utilisateur connu soit rejeté) [09], [11].

$$FRR = \frac{Nombre\ des\ client\ rejetés}{Nombre\ totale\ d'accès\ clients}. \qquad (Eq.\ 1.2)$$

1.9.2. Les points de fonctionnement

Pour les applications, on doit fixer un seuil avec lequel on prend les décisions d'acceptation ou de rejet de l'utilisateur. Cela correspond donc à choisir un point de fonctionnement du système.

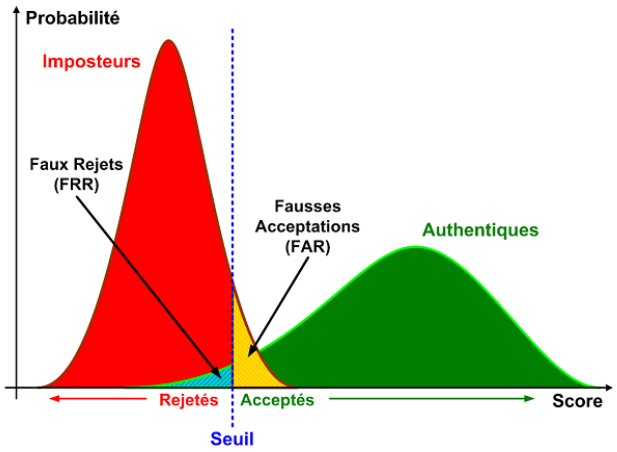


Figure 1.3 : Illustration du FRR et du FAR.

1.9.3. Les courbes de performance:

Les courbes de performances permettent de représenter les performances pour toutes les valeurs du seuil sans fixer un seuil a priori. Par exemple on peut représenter l'évolution des deux taux d'erreurs (FAR et FRR) lorsque le seuil varie pour les distributions de scores Client et Imposteur représentés sur la(*Figure 1.3)* :

Comme les taux d'erreurs FAR et FRR dépendent tous les deux du même seuil de décision, on peut également représenter sur une courbe la variation du FRR en fonction de FAR lorsque le seuil varie.

.

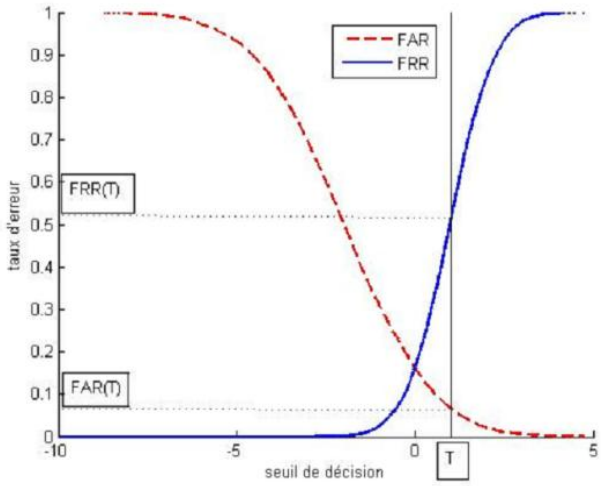


Figure 1.4 : Variation des taux de Faux Rejets (FRR) et taux de Fausses Acceptations (FAR) en fonction du seuil de décision varie

Ces courbes s'appellent des courbes ROC (Receiver Operating Characteristic) représentées sur la (*Figure 1.5).*

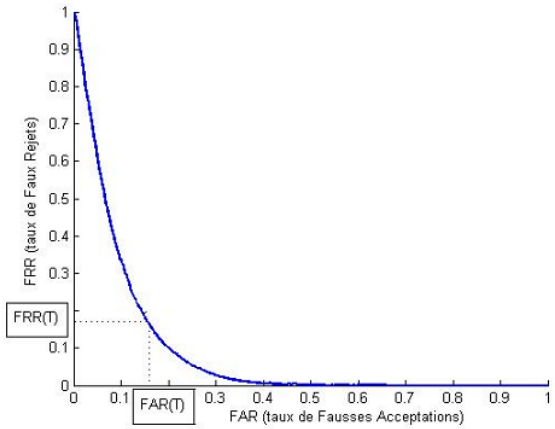


Figure 1.5 : La courbe ROC

Ou des courbes DET (Detection Error Tradeoff) représentées sur la (*Figure 1.6)* lorsque les échelles pour les deux taux d'erreurs sont logarithmiques.

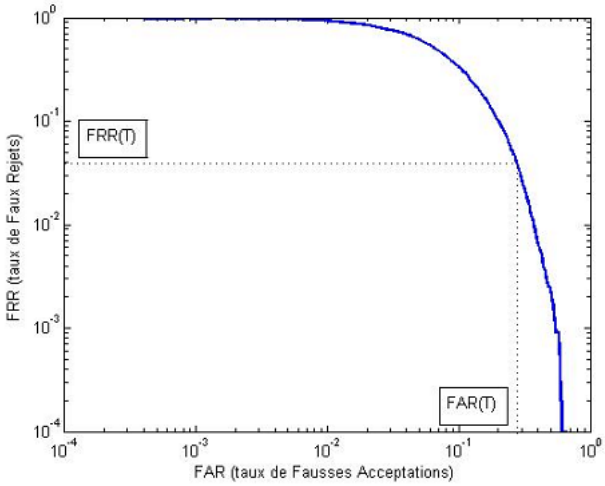


Figure 1.6 : Les courbes DET

1.9.4. Les différents types de point de fonctionnement :

Les 4 types de points de fonctionnement les plus utilisés sont :

EER : "Equal Error Rate" ou taux d'erreurs égales. Ce point de fonctionnement correspond au seuil qui donne des taux FAR et FRR égaux.

WER :"Weighted Error Rate" ou taux d'erreur pondéré. Ce point de fonctionnement correspond au seuil tel que le FRR est proportionnel au FAR avec un coefficient qui dépend de l'application. Le seuil du WER est égal au seuil de l'EER lorsque ce coefficient est égal à 1.

FAR fixé : Ce point de fonctionnement correspond au seuil tel que le taux FAR est égal à un taux fixé par l'application (par exemple 1% ou 0.1%).

La performance du système est donnée par le taux FRR pour cette valeur de FAR fixée.

FRR fixé : Ce point de fonctionnement correspond au seuil tel que le taux FRR est égal à un taux fixé par l'application (par exemple 1% ou 0.1%). La performance du système est donnée par le taux FAR pour le FRR fixé.

1.9.5. Les points de fonctionnement sur les courbes de performance

Sur la Figure suivante sont représentés des exemples des quatre types de points de fonctionnement présentés ci-dessus. La (*Figure 1.7)* représente ces mêmes points de fonctionnement sur une courbe ROC.

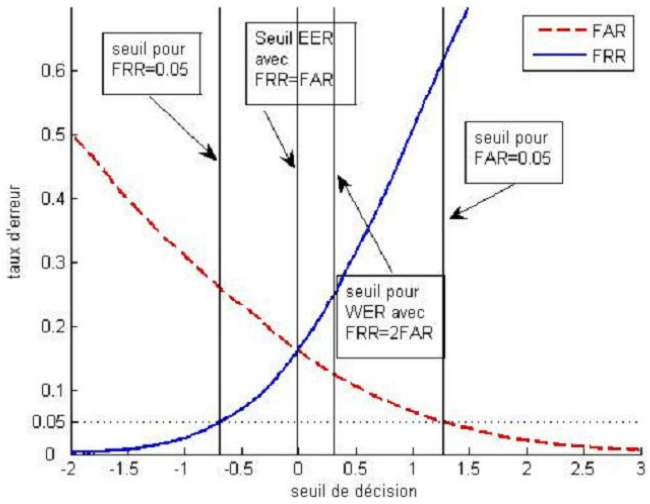


Figure 1.7 : Les points de fonctionnement représentés sur une courbe des taux d'erreurs en fonction du seuil de décision.

Le seuil du point EER (Equal Error Rate) correspond au seuil pour lequel les deux taux d'erreurs, FAR et FRR, sont égaux, il correspondant donc à l'intersection des deux courbes sur la(*Figure 1.6).* Il correspond à l'intersection de la courbe avec la première bissectrice pour les courbes ROC ou DET comme représenté sur la(*Figure 1.6).*

Sur les(*Figures 1.7)* et (*1.6),* sont représentés le point WER tel que FRR = 2FAR et les points FAR = 0.05 et FRR = 0.05.

Sur la (*Figure 1.7*)(courbe ROC), le terme de point de fonctionnement prend tout son sens car il s'agit bien d'un point localisé sur la courbe et pour lequel on peut estimer les valeurs des taux d'erreurs, FAR et FRR.

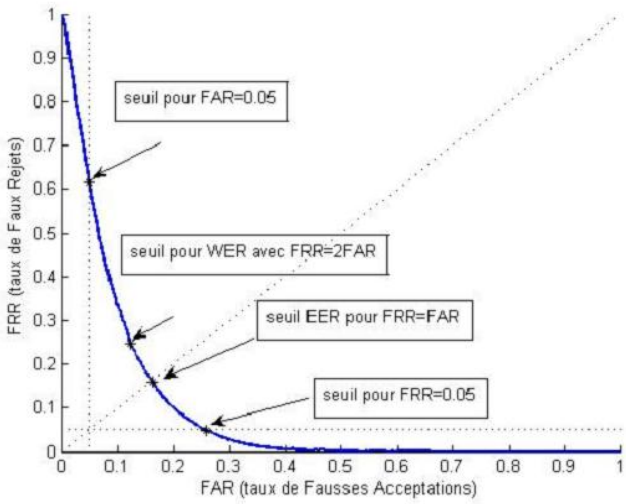


Figure 1.8 : *Les points de fonctionnement représentés sur une courbe des taux d'erreurs en fonction du seuil de décision.*

Pour chacun de ces points on peut ensuite estimer plusieurs valeurs à partir des FAR et FRR. La valeur la plus classique est l'erreur moyenne aussi appelé HTER (Half Total Error Rate) qui correspond à la moyenne entre le FAR et le FRR :

$$HTER = \frac{FAR + FRR}{2} \qquad \textit{(Eq. 1.3)}$$

Cette valeur de l'HTER est plutôt utilisée pour les points de fonctionnement associés à l'EER ou proches de l'EER où les deux taux d'erreurs sont du même.

Pour les points de fonctionnement associés au WER (Weighted Error Rate), il est logique d'utiliser une valeur globale d'erreur qui tienne compte de cette pondération.

On utilise alors le WTER (Weighted Total Error rate) tel que :

$$\text{WTER} = \alpha\text{FAR} + (1 - \alpha)\text{FRR} \qquad \textit{(Eq. 1.4)}$$

Dans notre exemple précédent où l'on cherche le point de fonctionnement qui correspond à FRR = 2FAR, c'est à dire 1 3FRR = 2 3FAR, la valeur de $\alpha = \frac{2}{3}$.

Pour les deux autres points de fonctionnement qui correspondent à des valeurs fixées pour le FAR ou pour le FRR, dans ces deux cas on n'utilise pas de valeur globale du taux d'erreur mais la valeur du taux d'erreur non fixé. Par exemple pour le point correspondant à FAR = 0.05 on lit sur la(*Figure 1.7)* que FRR = 0.61.

1.9.6. Quel point de fonctionnement pour quelle application

Le point de fonctionnement qui définit le choix du seuil dans le module de décision dépend de l'application visée. En général lorsqu'il n'y a pas d'application dénie mais qu'il s'agit

d'un test de performance sur une base de données préenregistrée, on utilise le plus souvent l'EER (c'est-à-dire les deux taux d'erreurs égaux) car c'est un point de fonctionnement assez neutre qui ne favorise aucun des deux types d'erreurs.

En revanche lorsqu'une application est dénie ou lorsque l'on connaît les 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.

Le compromis à faire pour le réglage du seuil de décision est le compromis entre confort et sécurité. Le confort correspond à un taux de Faux Rejets bas et la sécurité à un taux de Fausses Acceptations bas.

En général pour un besoin de sécurité on fixe FAR = 1% ou FAR = 0.1% selon le niveau de sécurité souhaité. Pour un besoin de confort on fixe FRR = 1% ou FRR = 0.1% en fonction du degré de confort souhaité.

Cependant, il est important de noter que le seuil de décision associé au point de fonctionnement choisi va être estimé sur une base de données, dite de développement, avec laquelle on règle les paramètres qui seront ensuite utilisés pour l'application en condition réelle. Le choix de cette base de données est primordial pour le bon réglage d'un système biométrique. Tout d'abord la base de données doit être représentative de l'application visée mas surtout elle doit être de taille su sante. En particulier, pour estimer des seuils de décision pour des taux de FAR ou de FRR fixés et faibles (par exemple FAR = 0.1%), cela nécessite un grand nombre de données pour avoir de la précision dans des zones où il y a peu d'erreurs.

1.10. Conclusion

Dans ce chapitre, On a présenté un système biométrique de façon général. Nous avons cité les différentes modalités puis on a détaillé pour le fonctionnement d'un système biométrique que ce soit pour la vérification et l'identification, dans notre travail on s'intéresse que pour l'identification, Nous avons aussi présenté les différents méthodes d'évaluation de performances d'un système biométrique, pour nous on doit utiliser les mesures FAR, FRR, EER, et GAR.

Chapitre 02

Système biométrie multimodales

2.1.Introduction

Les applications de Securities basé sur le système biométrique sont les plus utilisés dans tous les domaines. Aujourd'hui, avec les traitements informatiques, les systèmes biométriques sont automatisés. Dans ce chapitre, nous présentons l'utilisation de la biométrie ainsi que la structure, les avantages et les inconvénients des systèmes biométriques uni-modale en utilisant comme modalité l'ris. Ensuite, nous présenterons la biométrie multimodale qui est l'intérêt d'étude de cette mémoire. La biométrie multimodale est la combinaison de plusieurs modalités différentes, ce qui implique l'utilisation d'informations complémentaires pour une personne donnée.

2.2.Type des systèmes biométrie

Tous les systèmes biométriques ont généralement quatre étapes à franchir; l'enregistrement, l'acquisition, le stockage et de comparaison pour la vérification. Bien que, les quatre étapes sont nécessaires pour une réussite des phases biométriques complètes, ces quatre phases de travail en six étapes détaillées [13]. Elles sont:

- **Acquisition d'un échantillon:** les échantillons biométriques doivent être recueillis, par exemple, l'image d'empreinte digitale, échantillon d'ADN, une image pour l'orientation de l'oreille.
- **Extraction des caractéristique**: Cette étape consiste à convertir l'échantillon en données numériques, ces données numériques est le modèle. Cependant, dans certains cas, les images complètes sont utilisées qui éliminent la conversion des échantillons de données numériques.
- **Confirmation de la qualité:** La confirmation de la qualité comprend les deux premières étapes que pour que le système a meilleur modèle ou échantillon pour une utilisation ultérieure.
- **Stockage:** Selon l'application, le stockage du modèle est nécessaire si l'on veut utiliser plus tard.
- **Comparaison:** Dans cette étape, la comparaison est effectuée entre les modèles d'entrée en temps réel avec le modèle (s) stocké.
- **Résultat:** Cette dernière étape est directement proportionnelle au résultat de la comparaison. Cela dépend aussi souvent sur le seuil de décision utilisé par le système,

ce qui pourrait conduire à la suggestion de vérification supplémentaire si nécessaire en conformité avec les critères d'application dépendant.

Le système biométrique est divisé en deux catégories, système biométrique uni-modal et système biométrique multimodale

Les systèmes biométriques unimodaux : permettent de reconnaître une personne en utilisant une seule modalité biométrique, mais ne peuvent pas garantir avec certitude une bonne identification.

2.3.Limitation des systèmes biométrie

Bien que les techniques de reconnaissance biométrique promettent d'être très performantes, on ne peut garantir actuellement un excellent taux de reconnaissance avec des systèmes biométriques uni modaux, basés sur une signature biométrique unique. De plus, ces systèmes sont souvent affectés par les problèmes suivants [13] :

Bruit introduit par le capteur : le 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 [14].
Non-universalité : si chaque individu d'une population ciblée est capable de présenter une modalité biométrique pour un système donné, alors cette modalité est dite universelle. Ce 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. L'Institute National des Standards et Technologies (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.) [15].

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.

Manque d'individualité : les caractéristiques extraites à partir de données biomé- triques 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.

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), à l'utilisation de capteurs différents lors de l'enrôlement et de la vérification, à des changements de conditions de l'environnement ambiant (par exemple, changements en éclairement pour un système de reconnaissance faciale) ou encore à 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.

Sensibilité aux attaques : bien qu'il semble très difficile de voler les modalités biométriques d'une personne, il est toujours possible de contourner un système biométrique en utilisant des modalités biométriques usurpées. Des études ont montré qu'il était possible de fabriquer de fausses empreintes digitales en gomme et de les utiliser pour contrer un système biométrique [16]. Les modalités biométriques comportementales telles que la signature et la voix sont plus sensibles à ce genre d'attaque que les modalités biométriques physiologiques.

Ainsi, à cause de tous ces problèmes pratiques, les taux d'erreur associés à des systèmes biométriques unimodaux sont relativement élevés, ce qui les rend inacceptables pour un déploiement d'applications critiques de sécurité. Pour pallier ces inconvénients,

une solution est l'utilisation de plusieurs modalités biométriques au sein d'un même système, on parle alors de système biométrique multimodal.

Nous pouvons résumés les Principales limitations des systèmes unimodales sont:

- Les données bruitées :
  - Bruit ou distorsions dans les données acquises
  - Capteurs défectueux ou incorrectement maintenus
  - Conditions ambiantes/physiologiques défavorables
- La variabilité intra-individu : Les traits acquis de l'individu divergent du modèle stocké dans la base biométrique (modification des caractéristiques du capteur).
- La distinction entre individus : Grande similarité entre individus (selon les caractéristiques utilisées pour représenter les traits)
- Le manque d'universalité : FTE/A – 'Failure to Enroll/Acquire'(un échec dans l'échantillonnage biométrique

2.4.Systèmes multimodales

La multimodalité est l'utilisation de plusieurs systèmes biométriques. La combinaison de plusieurs systèmes a pour objectif de diminuer les limitations vues au système monomodal. En effet, l'utilisation de plusieurs systèmes a pour but premier d'améliorer les performances de reconnaissance. En augmentant la quantité d'informations discriminante de chaque personne, on souhaite augmenter le pouvoir de reconnaissance du système.

De plus, le fait d'utiliser plusieurs modalités biométriques réduit le risque d'impossibilité d'enregistrement ainsi que la robustesse aux fraudes.

Alors, les Systèmes biométriques multimodaux sont ceux qui utilisent ou qui sont fonction de l'utilisation, plusieurs caractéristiques physiologiques ou comportementales pour inscription, vérification ou l'identification.

2.4.1. Source d'information

Les systèmes biométriques multimodaux diminuent les contraintes des systèmes biométriques monomodaux en combinant plusieurs systèmes. On peut différencier 5 types de systèmes multimodaux selon les systèmes qu'ils combinent (*Figure 2.1).*

Multi-capteurs: lorsqu'ils associent plusieurs capteurs pour acquérir la même modalité, par exemple un capteur optique et un capteur capacitif pour l'acquisition de l'empreinte digitale. **Multi-instances :**lorsqu'ils associent plusieurs instances de la même biométrie, par exemple

l'acquisition de plusieurs images de visage avec des changements de pose, d'expression ou d'illumination.

Multi-algorithmes: lorsque plusieurs algorithmes traitent la même image acquise, cette multiplicité des algorithmes peut intervenir dans le module d'extraction en considérant plusieurs ensembles de caractéristiques et/ou dans le module de comparaison en utilisant plusieurs algorithmes de comparaison.

Multi-échantillons: lorsqu'ils associent plusieurs échantillons différents de la même modalité, par exemple deux empreintes digitales de doigts différents ou les deux iris (droite + gauche). Dans ce cas les données sont traitées par le même algorithme mais nécessitent des références différentes à l'enregistrement contrairement aux systèmes multi-instances qui ne nécessitent qu'une seule référence.

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

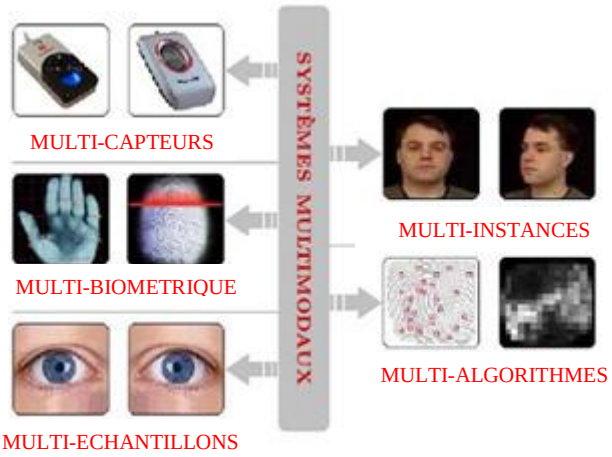


Figure 2.1 : les différents systèmes biométriques multimodales

Tous ces types de systèmes peuvent pallier à des problèmes différents et ont chacun leurs avantages et inconvénients. Les quatre premiers systèmes combinent des informations issues d'une seule et même modalité ce qui ne permet pas de traiter le problème de la non-universalité de certaines biométries ainsi que la résistance aux fraudes, contrairement aux systèmes "multi-biométries"

Les systèmes biométriques multimodales présentent des avantage vis-à-vis les systèmes uni-modales que l'on peut cité dans les points suivants.

- Bonne précision : augmente la précision et la robustesse car on intègre plusieurs sources d'informations biométriques indépendantes.

– L'universalité est présente

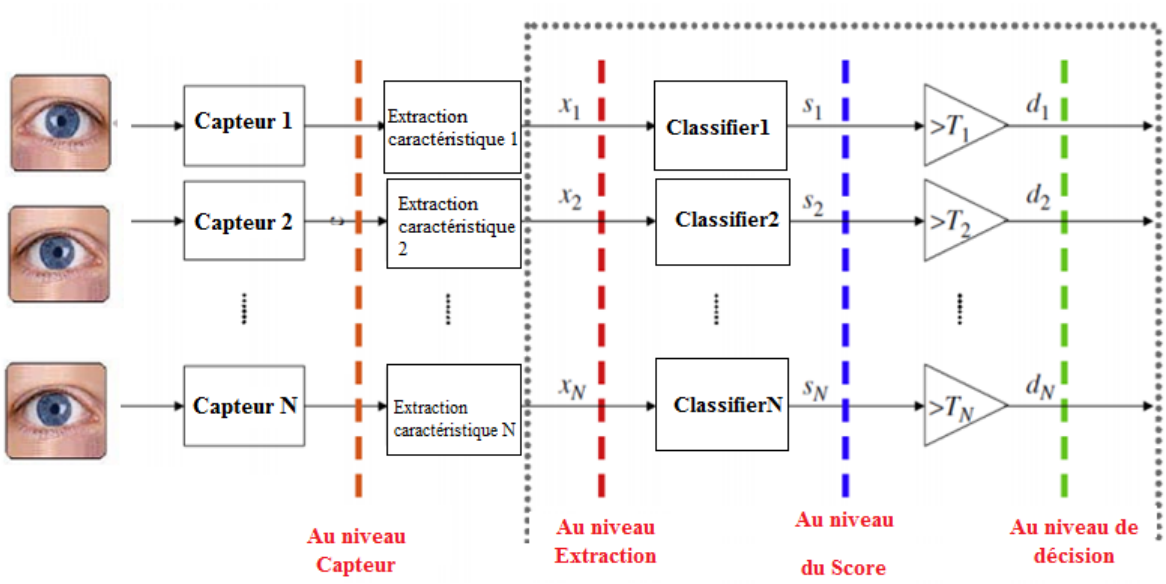
– Trouver une solution au problème de vulnérabilité aux imposteurs: il est plus difficile d'imiter plusieurs sources biométriques simultanément

Dans notre travail on s'intéresse que pour les systèmes multimodales (Multi-algorithmique) dont on combinat deux algorithme que nous allons détailler dans les sections suivantes.

2.4.2. Fusion de l'Information dans les Systems Biométriques Multimodaux

La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents : au niveau des données, au niveau des caractéristiques extraites, au niveau des scores issus du module de comparaison ou au niveau des décisions du module de décision (*Figure 2.2).*

Ces quatre niveaux de fusion peuvent être classés en deux sous-ensembles : la fusion pré-classification (avant comparaison) et la fusion post-classification (après la comparaison).



Figur 2.2 : Les niveaux de fusion [17]

Fusion au niveau capteur : fusion des informations issues de plusieurs données biométriques au niveau du capteur (images brutes), ce type de fusion relativement peu utilisée car elle nécessite une homogénéité entre les données. Par exemple il est possible de combiner plusieurs images de visages dans des canaux de couleurs différents ou en visible et en infrarouge s'ils correspondent à la même scène.

Fusion au niveau des caractéristiques : est moins limitée par la nature des données biométriques. Cependant une certaine homogénéité est nécessaire pour la plupart des

méthodes de fusion au niveau des caractéristiques comme par exemple la moyenne de plusieurs "templates" d'empreintes ou de visage. Un exemple de fusion au niveau des caractéristiques qui ne nécessitent pas vraiment d'homogénéité est la concaténation de plusieurs vecteurs de caractéristiques avant le traitement par l'algorithme de comparaison.

Fusion au niveau des décisions : est souvent utilisée pour sa simplicité. En effet, chaque système fournit une décision binaire sous la forme OUI ou NON que l'on peut représenter par 0 et 1, et le système de fusion de décisions consiste à prendre une décision finale en fonction de cette série de 0 et de 1. Les méthodes les plus utilisées sont des méthodes à base de votes telles que le OR (si un système a décidé 1 alors OUI), le AND (si tous les systèmes ont décidé 1 alors OUI) ou le vote à la majorité (si la majorité des systèmes ont décidé 1 alors OUI). On peut également utiliser des méthodes plus complexes qui pondèrent les décisions de chaque sous-système ou qui utilisent des classiffeurs dans l'espace de décisions telles que BKS (Behaviour Knowledge Space) [18].

Fusion au niveau des scores : est le type de fusion le plus utilisé car elle peut être appliquée à tous les types de systèmes (contrairement à la fusion pré-classification), dans un espace de dimension limité (un vecteur de scores dont la dimension est égale au nombre de sous-systèmes), avec des méthodes relativement simples et efficaces mais traitant plus d'information que la fusion de décisions. La fusion de scores consiste donc à la classification : OUI ou NON pour la décision finale, d'un vecteur de nombres réels dont la dimension est égale au nombre de sous-systèmes.

2.5.Fusion au niveau scores

Le niveau de fusion utilisé dans notre travail est celle de la fusion au niveau score, dans lequel les règles de fusion sont présentés.

Un système de fusion est constitué de deux modules, un module de fusion et un module de décision (*Figure 2.3).* Le problème devient donc un problème de classification à 2 classes (OUI ou NON, Client ou Imposteur) à partir d'un vecteur de nombre réels dont la dimension est égale au nombre de sous-systèmes du système multimodal.

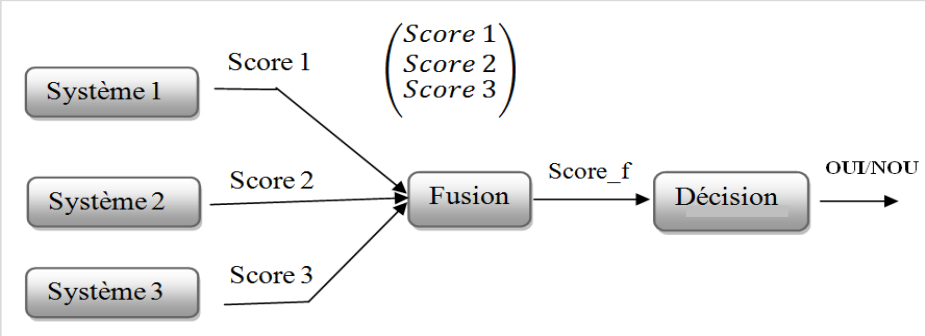


Figure2.3 : fusion au niveau score

Il existe de nombreuses méthodes pour classifier ces vecteurs de scores. On les distinguera ici en deux sous-ensembles : les méthodes de combinaison simple des scores et les méthodes de modélisation.

2.5.1. Règles de fusions

Les méthodes de combinaisons de scores sont des méthodes très simples dont l'objectif est d'obtenir un score final s à partir des N scores disponibles si pour $i = 1$ à N issus de N systèmes.

Les méthodes les plus utilisées sont le minimum, maximum, la somme, la somme pondéré et le produit [19].

– Combiner les scores par le minimum consiste à calculer s tel que

$$s = \min(s_i) \qquad \textit{(Eq. 2.1)}$$

– Combiner les scores par le maximum consiste à calculer s tel que

$$s = \max(s_i) \qquad \textit{(Eq. 2.2)}$$

– Combiner les scores par la somme consiste à calculer s tel que

$$s = \sum_{i=1}^{N} s_i \qquad \textit{(Eq. 2.3)}$$

– Combiner les scores par la somme pondéré consiste à calculer s tel que

$$s = \sum_{i=1}^{N} w_i s_i \qquad \textit{(Eq. 2.4)}$$

– Combiner les scores par le produit consiste à calculer s tel que

$$s = \prod_{i=1}^{N} s_i \qquad \textit{(Eq. 2.5)}$$

Toutes ces méthodes sont des méthodes simples qui ne nécessitent aucune adaptation. Il existe également des méthodes un peu plus évoluées de combinaison qui nécessitent le réglage de paramètres comme la somme pondérée, La somme pondérée permet de donner des poids différents w_i à chacun des sous-systèmes en fonction de leur performance individuelle ou de leur intérêt dans le système multimodal.

Cependant toutes ces méthodes de combinaison ne peuvent être utilisées que si tous les scores issus des sous-systèmes sont homogènes. Pour cela les méthodes de combinaison de scores nécessitent une étape préalable de normalisation des scores.

2.5.2. Normalisation de scores

Les méthodes de normalisation de scores ont pour objectif de transformer individuellement chacun des scores issus des sous-systèmes pour les rendre homogènes avant de les combiner. En effet, les scores issus de chaque sous-système peuvent être de nature différente. Certains systèmes produisent des scores de similarité (plus le score est grand, plus la référence ressemble au test, donc l'utilisateur est un client), d'autres produisent des distances (plus la distance est faible, plus la référence et le test sont proches, plus l'utilisateur est un client).

De plus chaque sous-système peut avoir des intervalles de variations des scores différents, par exemple pour un système les scores varient entre 0 et 1 et pour un autre les scores varient entre 0 et 1000.

L'étape pour rendre les scores homogènes peut être de deux natures différentes :

- remise à l'échelle des scores
- l'interprétation des scores dans un domaine commun

La normalisation de scores par remise à l'échelle ont pour objectif de transformer chaque score dans un intervalle commun. Chaque score issu de chaque sous-système est traité séparément par des translations et/ou changements d'échelle pour le transformer dans un intervalle défini et identique pour chaque sous-système.

Les méthodes de normalisation de scores par remise à l'échelle les plus utilisées sont : La méthode du *Minmax*, La méthode "Znorm" et La méthode *tangente* hyperbolique "Tanh", la méthode du *Minmax* est celle exploité dans notre travail.

$$n_i = \frac{s_i - min_i}{max_i - min_i} \qquad \textit{(Eq. 2.6)}$$

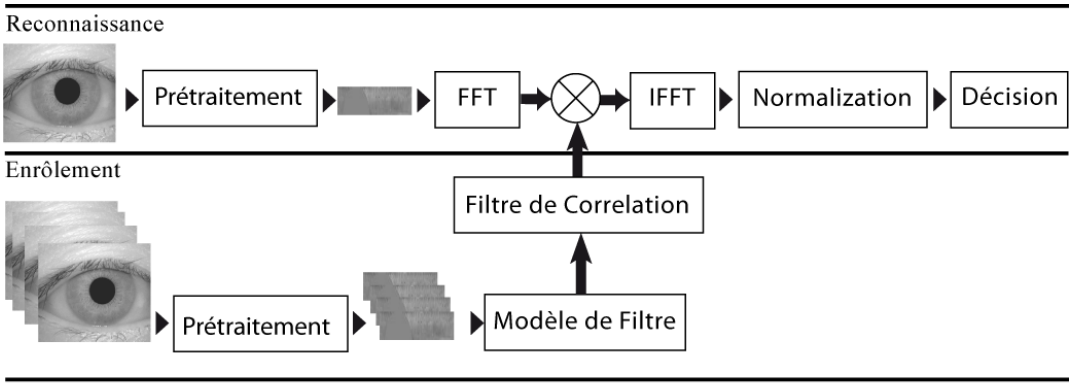
Les paramètres min_i et max_i sont déterminés pour chaque sous-système sur une base de développement. La méthode du Minmax met chaque score normalisé n_i dans l'intervalle [0; 1] sous forme de score de similarité, c'est-à-dire, avec les clients proches de la borne supérieure (1) et les imposteurs proches de la borne inférieure (0).

2.6. Système proposé

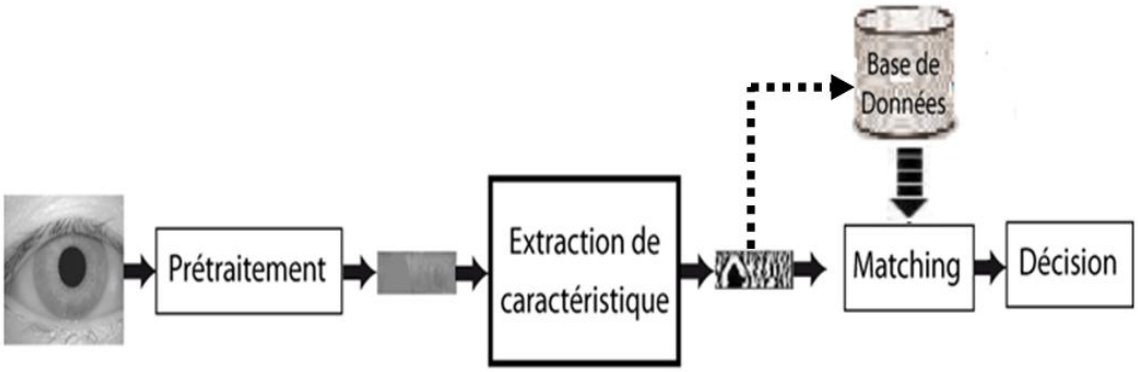
Le système proposé est composé de deux algorithmes différents l'échange d'informations correspondant à niveau de score. Chaque algorithme exploite la modalité iris.

La (*Figue 2.4)* présente (le premier algorithme) un système unimodal biométrique d'identification basé sur la modalité d'Iris, se constitue de prétraitement, matching (processus de corrélation), la normalisation et le processus de décision. la première identification de l'algorithme avec des filtres de corrélation est effectuée par corrélation d'une image de test transformé dans le domaine fréquentiel par une transformation discrète de Fourier rapide (FFT) avec le filtre conçu (d'enrôlement) également dans le domaine des fréquences. La sortie de corrélation est soumis à une transformée de Fourier rapide inverse (IFFT) et réorganisés dans les dimensions de l'image d'origine, avant d'être déphasés. Le plan de corrélation résultante est quantifiés en utilisant mesures de performance (peak-to sidelobe (PSR) "crête à lobe latéraux) rapport ou max pic, sur la base de cette mesure unique, une correspondance finale de score est faite.

La (*Figure 2.5)* présente (le second algorithme) un système uni-modale biométrique d'identification basée sur modalité d'iris, constitué de prétraitement, extraction de caractéristiques et de processus de matching, le vecteur de caractéristique est créer par le filtre de log-Gabor 1D et on a utilisé le métrique de la distance de hamming pour la comparaison.



Figue 2.4 : diagramme bloc d'un système d'identification uni-modale proposé basée sur l'énergie de corrélation moyenne minimale MACE.



Figue 2.5 : diagramme bloc d'un système d'identification uni-modale basée sur Filtre Gabor 1D.

Les deux scores des deux sous systèmes sont combiné et on utilisant les cinq règles de fusion au niveau scores, sur la base de ce score de fusion, une décision finale est prise (l'utilisateur est identifié ou rejeté). Cette structure améliorée prend un avantage de l'aptitude de chaque individu biométriques et de peuvent être utilisées pour surmonter certaines limites d'une seule modalité de représentation.

2.6.1. Processus de prétraitement

L'iris est la région annulaire de l'oeil borné par la pupille et la sclérotique (blanc de l'oeil) de chaque côté. Le motif d'iris est une caractéristique biométrique prometteuse car elle est considérée comme propre à chaque oeil, avec un degré élevé de capacité de discrimination [20]. Par conséquent, le motif de l'iris est le plus important candidat de la caractéristique biométrique, qui peut être utilisé pour différencier les individus. Par rapport à une autre technique biométrique, la reconnaissance de l'iris a beaucoup de mérites.

2.6.1.1. Prétraitement

L'œil contenait des images doivent être traitées de telle sorte que les caractéristiques de l'iris caractéristiques peuvent être extraites à des objectifs de comparaison. Au cours des étapes de pré-traitement [24], la région d'iris effective dans une image numérique de l'oeil consiste à isoler. La région de l'iris, peut être approchée par deux cercles, l'un pour frontière de l'iris / sclérotique et l'autre, l'intérieur de la première, pour frontière de l'iris / pupille. Les paupières et les cils obstruent normalement les parties supérieure et inférieure de la région d'iris.

Segmentation: Une fois que les frontières des deux cercles extérieurs et intérieurs sont définis, la région d'iris est localisé (*Figure 2.6).* La Transformée circulaire de Hough est adoptée pour rechercher les frontières. Les paupières sont détectées en interposant les deux

lignes en utilisant la transformée de Hough linéaire et cil est isolé par une technique de seuillage simple, [22].

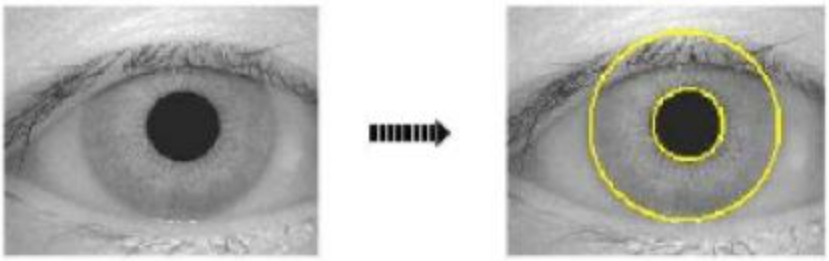
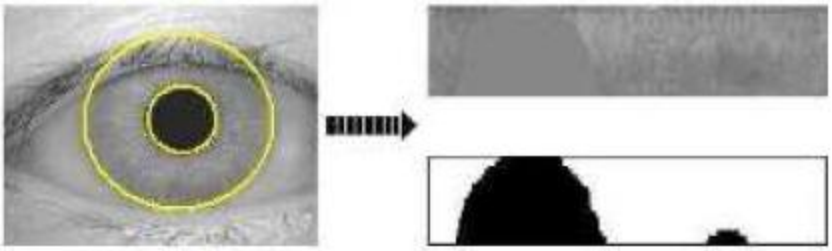


Figure 2.6 :Image de l'œil et segmentation de l'iris

Normalisation: Afin d'effectuer une comparaison entre les iris, la région de l'iris segmenté doit être aligné sur une taille fixe. La normalisation est effectuée en utilisant Daugmans modèle de feuille de caoutchouc [23], où la région circulaire est transformée à une forme rectangulaire. Au cours de la normalisation, le centre de la pupille est considéré comme le point de référence, tandis que le cercle de vecteurs radial à travers la région d'iris. Le processus de codage produit un modèle binaire contenant un certain nombre de bits d'information, et un masque de bruit correspondant qui correspond à des zones de corruption au sein du motif de l'iris, et les bits de masque dans le modèle comme corrompu. La (*Figure2.7)* montre un iris avec des frontières, la normalisation de l'iris, et son masque.



Figue 2.7 : Image avec des frontières (à gauche), la normalisation de l'iris (en haut à Droite) et son masque (en bas à Droite).

2.6.2. Système d'identification à base d'un filtre MACE

Pour chaque classe un filtre MACE unique est synthétisé. Une fois que le filtre de MACE $H\ (u,v)$ a été déterminé, l'image d'entrée de test f est en corrélation croisée avec elle de la manière suivante:

$$c(x,y) = IFFT\{FFT(f(x,y)) * H^{*}(u,v)\} \qquad \textit{(Eq. 2.7)}$$

Lorsque l'image de test est d'abord transformé en domaine fréquentiel puis reformé pour être sous la forme d'un vecteur. Le résultat du processus précédent est convolée avec le

conjugué du filtre de MACE. Cette opération est équivalente à une corrélation croisée avec le filtre de MACE. La sortie se transforme à nouveau dans le domaine spatial. Essentiellement le filtre MACE est la solution d'un problème d'optimisation sous contrainte, qui cherche à minimiser l'énergie de corrélation moyenne, et même temps satisfaire les contraintes le pic de corrélation. En conséquence, la sortie des plans de corrélation sera proche de zéro partout sauf aux emplacements des objets formés qui sont définis pour être correct où un pic sera produit.

Le filtre MACE, H, est trouvé en utilisant des multiplicateurs de Lagrange dans le domaine fréquentiel et donnée par convolution [24]:

$$H = D^{-1}X(X^{*}D^{-1}X)^{-1}u \qquad \textit{(Eq. 2.8)}$$

D est une matrice diagonale de taille $d \times d$ (d est le nombre de pixels dans l'image) contenant les énergies de corrélation moyenne des images d'apprentissage à travers ses diagonales. X est une matrice de taille $N \times D$ où N est le nombre d'images d'entraînement et * est le conjugué complexe. Les colonnes de la matrice X représentent les coefficients de Fourier discrète pour une image d'apprentissage particulièreXn. Le vecteur de colonne (u) de taille N contient les valeurs de contrainte de pic de corrélation pour une série d'images d'apprentissage. Ces valeurs sont normalement fixées à 1,0 pour des images de la même classe.

Mesure de Similarité

Typiquement, le haut pic peut être utilisé comme une bonne mesure de similarité pour l'image correspondante (*Figure 2.8)(a)*. Un autre paramètre, PSR, peut être utilisé pour mesurer la similarité entre deux échantillons. PSR est une métrique qui mesure la finesse du pic du plan de corrélation. Pour l'estimation du PSR, le pic est localisé en premier. Ensuite, la moyenne et l'écart-type de la région de lobe latéral 40 * 40 (à l'exclusion d'un masque central 5 * 5) centrée sur le pic sont calculées. PSR est ensuite calculé comme suit [25]:

$$PSR = \frac{peak - moyenne(région\ des\ lobes\ latéral\ )}{\sigma(région\ des\ lobes\ latéral)} \qquad \textit{(Eq. 2.9)}$$

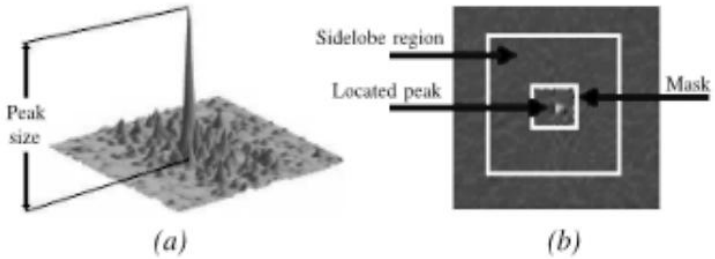


Figure 2.8 : Similarité correspondant. (a) pic max. (b) Max des lobes latéral

2.6.3. Système d'identification à base d'un filtre 1D Gabor

Les informations les plus discriminantes présentés dans un motif d'iris doit être extrait. Seules les caractéristiques significatives de l'iris doivent être codées de telle sorte que les comparaisons entre les modèles peuvent être faites. Le filtre 1D Log- Gabor est capable de fournir une représentation conjointe optimale d'un signal dans l'espace et la fréquence spatiale [26]. La fonction est générée à partir de l'iris normalisé par filtrage de l'image avec filtre 1D Log-Gabor.

Log-Gabor Filtre: l'extraction des caractéristiques par le filtre de Gabor est un choix commun pour l'analyse de texture. Ils offrent une meilleure localisation simultanée de l'information spatiale et fréquentielle. L'inconvénient du filtre de Gabor est qu'aura composante continu lorsque la largeur de bande est supérieure à une octave [27]. Pour remédier à cet inconvénient, un type de filtre Gabor connu comme filtre Log-Gabor, qui est gaussien sur une échelle logarithmique, peut être utilisé pour produire des composantes nulles à courant continu pour toute la bande passante. La réponse en fréquence d'un filtre delog-Gabor est donnée comme suit:

$$G(f) = exp\left[\frac{-(log(f/f_0))^2}{2(log(\sigma/f_0))^2}\right] \qquad \textit{(Eq. 2.10)}$$

où f_0 représente la fréquence centrale, et σ donne la bande passante du filtre. Les paramètres du filtre Log-Gabor ont été empiriquement sélectionnés comme f_0 = 1/2 et σ = 0: 0556. sont utilisés dans tous les calculs.

Les lignes de la ROI sont cancatés pour générer vecteur 1D pour l'extraction de caractéristiques. Ces signaux ont été convolution avec filtre 1D Log-Gabor. La forme du signal de convolution résultante est complexe a évalué. Nous appliquons ensuite les inégalités suivantes pour extraire les modèles de réponse binaire pour les deux, partie réelle et imaginaire.

$$\begin{array}{llll} b_r = 1 & if\ \ Re[\blacksquare] \geq 0\ \ ; & b_r = 0 & if\ \ Re[\blacksquare] < 0 \\ b_i = 1 & if\ \ Im[\blacksquare] \geq 0\ \ ; & b_i = 0 & if\ \ Re[\blacksquare] < 0 \end{array} \qquad \textit{(Eq. 2.11)}$$

$$\blacksquare : pixel$$

La méthode d'extraction de caractéristiques stocke la partie réelle et imaginaire dans un vecteur de caractéristique.

Extraction de caractéristiques dans ce système est basé sur un modèle binaire dérivé par l'application de filtre log-Gabor pour binarise le résultat. La comparaison est basée sur la

Distance de Hamming normalisée entre les deux représentations. L'algorithme de distance de Hamming employé intègre également le bruit de masquage, de sorte que seuls les bits significatifs sont utilisés dans le calcul de la distance de Hamming entre deux modèles d'iris. Maintenant, en prenant la distance de Hamming, seuls les bits dans le motif de l'iris qui correspondent aux bits 1 dans les masques de bruit des deux modèles d'iris seront utilisés dans le calcul [28].

Hamming Distance: Soit $T_1\,[i,j]$ et $T_2\,[i,j]$ deux images de taille $N_1 \times N_2$ et soit M_1; M_2 leur masque. Ensuite, la distance de Hamming (HD), entre T_1 et T_2 peut être défini comme [29]:

$$HD = \frac{\sum_{i=0}^{N1}\sum_{j=0}^{N2} M_1(i,j) \cap M_2(i,j) \cap \{T_1(i,j) \oplus T_2(i,j)\}}{\sum_{i=0}^{N1}\sum_{j=0}^{N2} M_1(i,j) \cap M_2(i,j)} \qquad \textit{(Eq. 2.12)}$$

Il est à noter que la HD est compris entre 1 et 0. pour le matching parfait, le score correspondant est égal à zéro. Lorsque la distance de Hamming de deux modèles est calculée, un gabarit est décalé à gauche et à droite du bit et un certain nombre de valeurs de distance de Hamming sont calculées à partir des changements successifs.

2.7.Conclusion

Dans ce chapitre, nous avons illustré l'endiccape d'utilisé un système unimodale vis-à-vis un système multi-algorithmique, puis on a présenté le système multi algorithmique proposé dans lequel on a détaillé chaque bloc de ce système.

La fusion utilisé dans ce système est celle de la fusion au niveau score, les deux distance combinés sont calculé a partir de système basé sur un filtre MACE et un système basé sur un filtre 1D Gabor, où ces distance son normalisé avas et après la fusion. On a utiles les cinq règles de fusion (Min, Max, Somme, Somme pondéré et Produit).

Chapitre 03

Résultats expérimentaux

3.1.Introduction

Ce chapitre présente les procédures de mise en œuvre, la base de données utilisée pour les tests et les résultats des systèmes uni-modales et le système Multi-Représentation proposé. La base de données CASIA a été utilisée pour évaluer les performances du système. L'identification de personne par un système biométrique utilisant l'Iris comme modalité biométrique. La raison la plus impérieuse de combiner deux algorithmes est d'améliorer les taux de performance de ces systèmes biométriques.

Le processus du système biométrique multi-représentation proposé comporte deux grandes phases : la phase de pré-fusion, la phase de sélection des scores en utilisant deux algorithmes, le 1er algorithme on a utilisé le filtre MACE pour le calcul de premier score et le filtre de Gabor 1D pour le deuxième score, et la phase de fusion. La phase de pré-fusion, consiste à suivre les processus des deux systèmes biométriques monomodaux (basé sur l'iris) allant de l'étape de prétraitement de ce système jusqu'à l'extraction des caractéristiques. Dans la deuxième phase, on combine ces scores par les cinq règles de fusion.

Nous avons utilisé MATLAB 2014b pour l'implémentation de notre système et son environnement une grande puissance de calcul. Il dispose de plusieurs boites à outils en particulier celle du traitement de l'image « Image Processing ToolBox » qui propose un ensemble d'algorithmes et d'outils graphiques de référence pour le traitement d'image, l'analyse, la visualisation et le développement de traitement d'image.

Dans la suite de ce chapitre, nous présentons le système biométrique multi-représentation que nous avons proposé. Puis, nous exposons les résultats expérimentaux de l'évaluation des différentes méthodes proposées.

3.2.Bases de données

Pour évaluer la performance du système d'identification multi-biométrique proposée, une base de données contenant des images de l'iris a été nécessaire. Dans ce travail, nous construisons une base de données multi-représentation pour nos expériences sur la base de la base de données CASIA Iris [30] de L'Académie chinoise des sciences - Institut d'Automation (CASIA) base de données d'image de l'œil contient 756 images de l'œil avec 108 niveaux de gris yeux ou des classes uniques et 7 images différentes de chaque œil unique. Images de chaque classe sont prises à partir de deux sessions avec un mois d'intervalle entre les sessions. Les images ont été capturées en

particulier pour la recherche de reconnaissance de l'iris en utilisant l'optique numérique spécialisée développés par le Laboratoire national de reconnaissance de formes, la Chine. La base de données multi-représentation se compose de six images d'iris images par personne avec un total de 100 personnes. 3 échantillons, de chaque iris, sont choisis au hasard pour construire un ensemble d'apprentissage et le reste des échantillons sont pris comme l'ensemble de test.

3.3.Evaluation des performances

Les systèmes biométriques, qu'ils soient monomodaux (une seule modalité biométrique) ou multimodaux (la combinaison de plusieurs modalités biométriques) ont vocation à être utilisés dans un grand nombre d'applications. Pour pouvoir envisager le déploiement de ces systèmes dans la vie courante, les systèmes ont besoin d'être évalués pour pouvoir estimer leurs performances en utilisation réelle. L'évaluation des performances comprend de nombreux aspects qui peuvent être plus ou moins importants à tester selon les applications.

Les systèmes d'identification peuvent fonctionner en 2 modes : mode d'identification dans un ensemble ouverte ou fermé, dans notre travail on s'intéresse que pour le mode de fonctionnement d'ensemble ouverte et on utilise les mesures des taux d'erreurs suivantes : FAR, FRR, EER, GAR et les courbes ROC définit dans le 2ème chapitre.

Le but de cette travail est d'évaluer la performance du système lorsqu'on utilisant des informations provenant de deux algorithme proposé (filtre MACE et filtre 1D Gabor) et leurs fusion au niveau score avec les cinq régler de fusions. Il y a un total de 300 images d'apprentissage et 300 images de test pour chaque modalité, respectivement. Par conséquent, il y a au total 300 comparaisons authentiques et 29700 comparaisons imposteurs sont générées.

3.3.1. Résultat de test Uni-modal

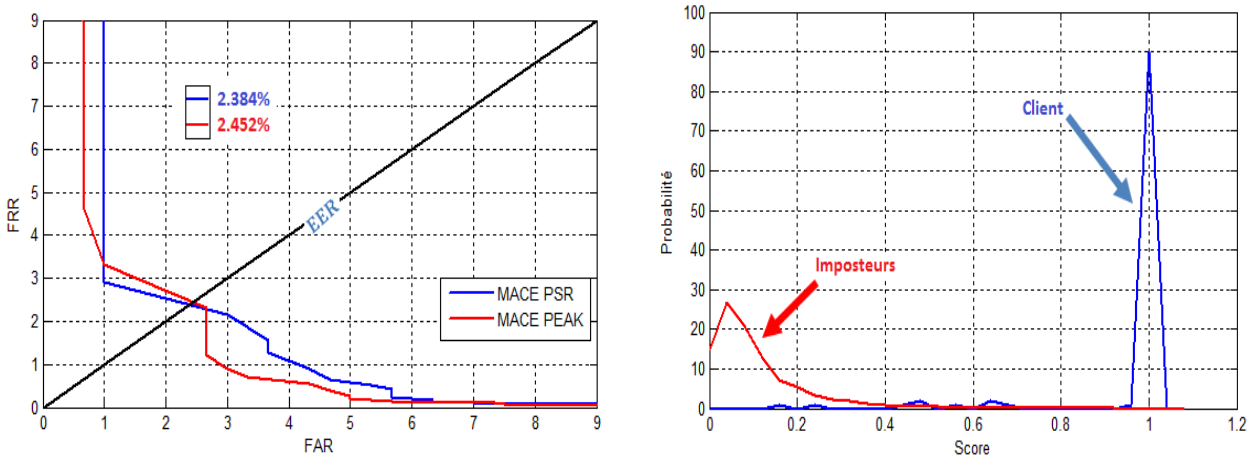
Dans le 1er algorithme le filtre MACE est appliqués pour évaluer la performance d'identification et on utilisé le PEAK (pic) et PSR comme métrique de similarité, pour le 2ème algorithme le filtre 1D Log-Gabor est appliqué pour extraire les caractéristiques et on a utilisé la distance de Hamming pour évaluer la performance d'identification pour le deuxième algorithme.

Résultat de test du 1er algorithme : L'objectif du 1er algorithme est de comparer les deux métrique PEAK et le PSR en utilisant le filtre MACE. La *Figure 3.1* montre que le métrique PSR donne un meilleur résultat que le PEAK en termes de taux d'erreur Égal (EER). Par exemple, si le filtre MACE avec un PEAK est utilisé, nous avons un EER = 2.452 % au seuil To = 0,474 et

avec le PSR l'EER = 2.384 % au seuil To = 0.467. Le système a été testé avec des seuils différents comme le montre le tableau 3.1. Pour le reset de travail on utilise le PSR comme métrique de similarité.

MACE					
PEAK			PSR		
FAR	FRR	GAR	FAR	FRR	GAR
0.666	4.606	95.394	1.087	2.882	97.118
2.452	2.452	97.548	**2.384**	**2.384**	**97.616**
4.661	0.400	99.600	4.560	0.722	99.278

Tableau 3.1 : Performance de Système d'identification uni-modale (Filtre MACE)



(a) *(b)*

Figure 3.1 : Résultats des tests du système d'identification Uni-modale : (a) comparaison de performance entre les métriques PEAK et PSR, (b) distribution des clients et les imposteurs (MACE PSR)

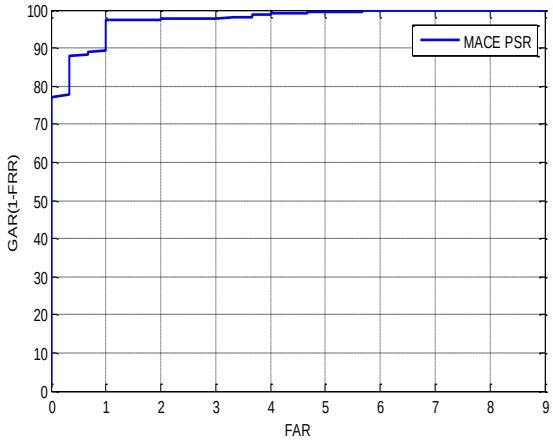
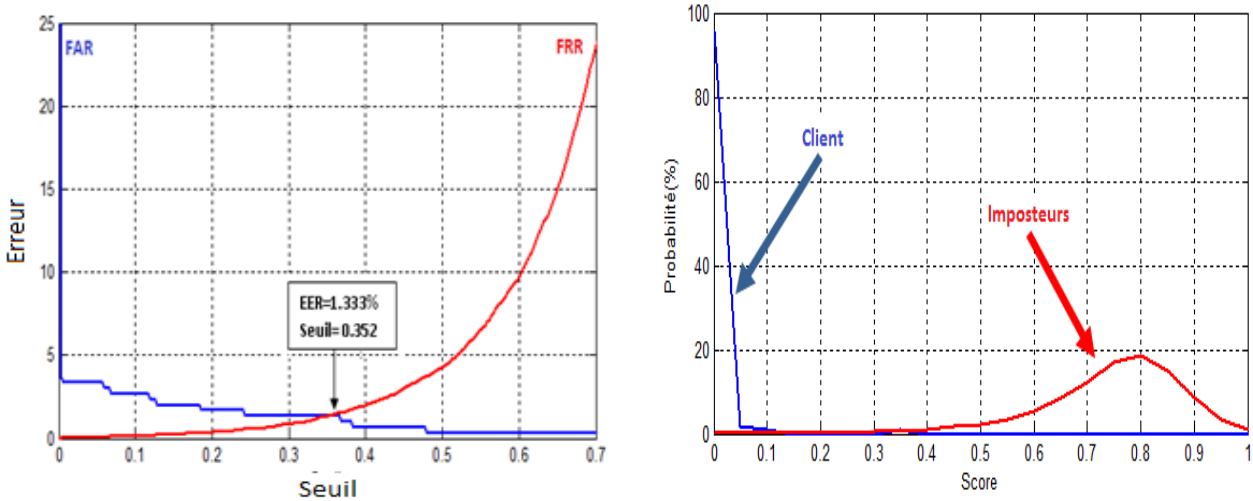


Figure 3.2 : Courbes ROC de filtre MACE PSR Matching.

Résultat de test du 2ème algorithme : *(Figure. 3.3)* représente la performance du système d'identification d'iris en utilisant le filtre de Gabor 1D. L'EER de cette expérience est d'environ 1.333 % , alors que le seuil correspondant est To = 0,352.



(a) *(b)*

Figure 3.3 : Résultats des tests du système d'identification Uni-modale : (a) c Courbes ROC de filtre Gabor 1D, (b) distribution des clients et les imposteurs.

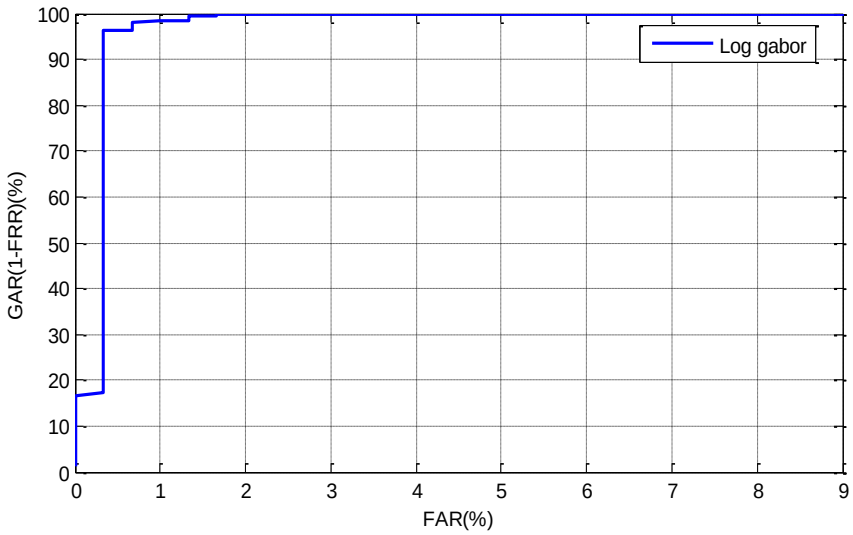


Figure 3.4 : Courbes ROC de filtre Gabor 1D.

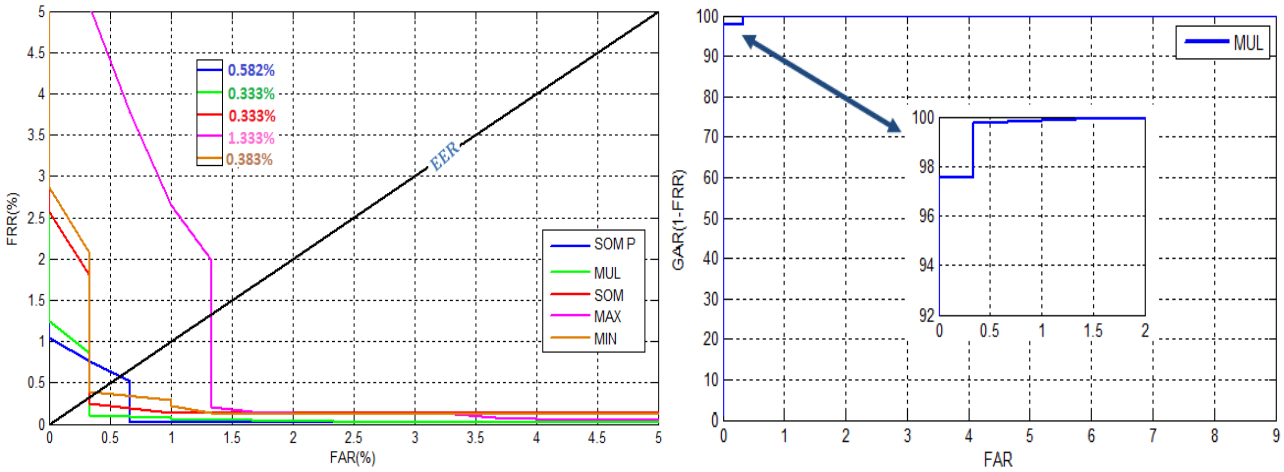
3.3.2. Résultat de test Multimodal

Le but de cette expérience était d'étudier la performance de système lorsque nous fusionnons information issue de deux algorithmes de la modalité iris. Par conséquent, les informations présentées par différents multi-représentation est fusionnée à rendre le système efficace.

La fusion au niveau score est préféré dans le domaine de la reconnaissance biométrique, car il est contenu de l'information suffisante et il est facile d'accès et de combiner les scores correspondants [24]. Dans notre système, nous avons adopté l'approche combinée, où les scores correspondants individuels sont combinés pour générer un score unique scalaire, qui est ensuite utilisé pour prendre la décision finale. Au cours de la conception du système, nous utilisons les cinq de fusions suivants: Som-score, Min-score, Max-notes et, Mul-score, Som-pondéré-score [25]. Supposons que la quantité D_{0i} représente le score de la matcher i^{ème} (i = 1; 2) pour les deux algorithmes et D_F représente le score de fusion. Par consequent, DF est donnée par:

- Som-score (SOM) : $D_F = \sum_{i=1}^{N} D_{0i}$
- Min-score (MIN) : $D_F = min\{D_{0i}\}$
- Max-score (MAX) : $D_F = max\{D_{0i}\}$
- Mul-score (MUL) : $D_F = \prod_{i=1}^{N} D_{0i}$
- Som-pondéré-score (SOM_P) : $D_F = \sum_{i=1}^{N} w_i \cdot D_{0i}$

Fusion au niveau du score : Les informations présentées par les deux algorithmes est fusionné au niveau du score pour rendre le système efficace. Pour cela, une série d'expériences ont été réalisées à la sélection de la meilleure règle de fusion qui minimisent l'EER en utilisant le meilleur résultat unimodale (MACE filtre avec PSR correspondant) pour le premier algorithme et combiné avec la mise en correspondance de score obtenu par le second algorithme. Ainsi, pour déterminer la meilleure règle de fusion, une relation graphique (ROC) peut être établie (voir *Figure 3.5*. (a)). Nous pouvons observer que la fusion à base de règles MUL a la meilleure performance. Ainsi, le meilleur résultat en termes d'EER est donné à 0.333%. La performance du système d'identification est considérablement améliorée par l'utilisation de la fusion. Enfin, la performance du système d'identification sous différentes règles de fusion avec base de données égale à 100 est représentée dans le (tableau 3.2).



(a) *(b)*

Figure 3.5: Résultats multi-représentation : (a) Les courbes ROC pour la fusion au niveau des scores, (b) Les courbes ROC pour le meilleur système multimodal

SOM		MIN		MAX		MUL		SOM_P	
To	**EER**	**To**	**EER**	**To**	**EER**	**To**	**EER**	**To**	**EER**
0.346	0.333	0.157	0.383	0.511	1.333	0.103	0.333	0.370	0.582

Tableau 3.2 : Performance de Système d'identification multi-modale

3.4.Conclusion

Dans ce chapitre, nous avons présenté notre système biométrique multi-représentation, dans ce système, nous avons implanté deux algorithmes pour la multi-représentation, le 1er algorithme on a utilisé le filtre MACE pour le calcul de premier score et le filtre de Gabor 1D pour le deuxième score, la combinaison de ces scores au niveau scores a donné un système biométrique performant pouvant identifier une personne d'une manière fiable ce qui a été prouvé par une évaluation sur la base de données utilisées.

Conclusion général

Ce mémoire a présenté un système de reconnaissance de l'iris, qui a été testé en utilisant une base de données d'images en niveaux de gris de l'œil afin de vérifier les performances selon la technologie de reconnaissance de l'iris.

Dans ce travail nous nous sommes intéressés à étudier profondément la biométrie d'une manière générale et la biométrie multimodale d'une manière plus particulière afin de créer un produit biométrique. Puis nous avons présenté la biométrie monomodale, la biométrie multimodale, leurs caractéristiques, leurs limitations, ainsi que des généralités sur la biométrie. Nous nous sommes ensuite focalisés sur le système multi-représentation proposés.

Le système multi-représentation proposé est composé de deux algorithmes, le 1er algorithme on a utilisé le filtre MACE pour le calcul de premier score et le filtre de Gabor 1D pour le deuxième score, la combinaison de ces scores au niveau scores, La performance du système d'identification est considérablement améliorée par l'utilisation de cette fusion.

REFERENCES BIBLIOGHRAPHIES

[1] National Science and Technology Council (NSTC), Biometrics History, 2006c.

[2] James L. Wayman, Technical Testing and Evaluation of Biometric Identification, National Biometric Test Center Collected Works 1997-2000, 2000.

[3] Aiello L, Gardner T, King G, Blankenship G, Cavallerano J, Ferris F, Klein R. « Diabetic Retinopathy «. Diabetes Care 1(21):143–156, 1998.

[4] Anil K. Jain, Stan Z. Li, « Encyclopedia Of Biometrics », Springer 2009.

[5] Anil. K. Jain, R. Bolle, And S. Pankanti, « Biometrics: Personal Identification In Networked Society «, Kluwer Academic Publishers, 1999.

[6] Anil. K. Jain, P. Flynn, A. Ross, « Handbook Of Biometrics », Springer, 2007.

[7] Djamel SAIGAA, " Contribution à l'authentification d'individus par reconnaissance de visages", THESE Présentée pour obtenir le Diplôme de Doctorat d"Etat en Automatique, Faculté des Sciences et Sciences de l"ingénieur, Université Mohamed Kheider, Biskra, 2006.

[8] National Science and Technology Council (NSTC), Biometrics Glossary, 2006b.

[9] K. Jain, Ruud Bolle,Sharath Pankanti (BIOMETRICS Persona1 .Identification in Networked Society.

[10] Biometric_User_Authentication_for_IT_SECURITY

[11] EURODAC "Information and communication" unit, Directorate-General Justice, Freedom and Security, B-1049 Brussels – August 2004. Retrieved October 22 2013

[12] These-Pierre-Buyssens (Fusion de differents modes de capture pour la ´ reconnaissance du visage appliquee aux transactions) , 2011.

[13] Y. Chen, S. Dass, and A. Jain. "Fingerprint Quality Indices for Predicting Authentication Performance". In : Proceedings of Fifth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), pp. 160–170, New York, NY, USA, July 2005.

[14] A. Ross, K. Nandakumar, and A. Jain. Handbook of Multibiometrics. SpringerVerlag New York, Inc., 2006.

[15] C. Sanderson and K. Paliwal. “Information fusion and person verification using speech and face information”. Tech. Rep. IDIAP-RR 02-33, IDAIP, September 2002.

[16] Nicolas MORIZET, “ Reconnaissance Biométrique par Fusion Multimodale du Visage et de l’Iris”, Thèse présentée pour obtenir le grade de Docteur, Ecole Nationale Supérieure des Télécommunications, Paris, 18 Mars 2009.

[17] Tao, R. Veldhuis, Threshold-optimized decision-level fusion and its application to biometrics, Pattern Recognition, 42 (2009) 823 – 836.

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

[19] Wei Jia, Bin Ling, Kwok-Wing Chau, Laurent Heutte, Palmprint identification using restricted fusion, Applied Mathematics and Computation, 2008 Elsevier.

[20] C. R. Prashanth, Shashikumar D.R., K. B. Raja, K. R. Venugopal, L. M. Patnaik,High Security Human Recognition System using Iris Images, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009, pp. 647-652.

[21] Kaushik Roy and Prabir Bhattacharya, Optimal Features Subset Selection and Classification for Iris Recognition, Journal on Image and Video Processing, March 2008.

[22] XIE Mei, Iris Recognition Technique , Journal of Electronic Science and Technology of China, Vol.4 No.3, Sep. 2006, pp. 219-224.

[23] J. G. Daugman, BThe importance of being random: Statistical principles of iris recognition,[Pattern Recognition, vol. 36, pp. 279291, 2003.

[24] Aini Hussain, Rosniwati Ghafar, Salina Abdul Samad and Nooritawati Md Tahir, Anomaly Detection in Electroencephalogram Signals Using Unconstrained Minimum Average Correlation Energy Filter, Journal of Computer Science 5 (7): 501-506, 2009.

[25] Rosniwati Ghafar, Aini Hussain, Salina Abdul Samad and Nooritawati Md Tahir, Umace Filter for Detection of Abnormal Changes In Eeg: A Report of 6 Cases, World Applied Sciences Journal 5 (3): 295-301, 2008.

[26] Nooritawati Md Tahir, Aini Hussain, Salina Abdul Samad and Hafizah Husain, Posture Recognition Using Correlation Filter Classifier, Journal of Theoretical and Applied Information Technology, 4(9), 2008, 767-773.

[27] Suman Senapati, Goutam Saha, Speaker Identification by Joint Statistical Characterization in the Log-Gabor Wavelet Domain, International Journal of Intelligent Systems and Technologies, Winter 2007.

[28] F. Wang, J. Han. Iris recognition method using Log-Gabor filtering and feature fusion, Journal of Xian Jiaotong University, Vol.41, 2007.

[29] John Daugman, New Methods in Iris Recognition, Ieee transactions onsystems, man, and cybernetics-part b: cybernetics, vol. 37, no. 5, october 2007, pp. 1167- 1175.

[30] CASIA Iris Image Database, avaible from : http://www.sinobiometrics.com.