UNIVERSITE KASDI MERBAH
OUARGLA

FACULTÉ DES NOUVELLES
TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION
DEPARTEMENT DE L'ÉLECTRONIQUE ET DE TELECOMUNICATIONS

FILIERE : GÉNIE ÉLECTRIQUE
SPECIALITÉ: AUTOMATIQUE

MÉMOIRE
MASTER ACADEMIQUE

PRÉSENTÉ PAR:

MOULAY BRAHIM OUSSAMA **ARBAOUI MOHAMED IBRAHIM**

Thème

Identification des personnes par les articulations des doigts

Date de soutenance :
Le : 08 / 06 / 2015
Devant le jury :

M. MRAOUMIA Abdallah	**M.C.B**	**Président**	**UKM Ouargla**
M. SAMAI Djamel	**M.C.B**	**Encadreur**	**UKM Ouargla**
M. CHAA Mourad	**M.A.A**	**Examinateur**	**UKM Ouargla**
M. MANSEUR Abdelghani	**M.A.A**	**Examinateur**	**UKM Ouargla**

Ce travail a été réalisé au niveau du laboratoire de génie électrique UKM Ouargla

Année Universitaire : 2014 /2015

Dédicaces Oussama

Je dédie ce mémoire:

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

A Ma grand-mère

Et mon frère et mes sœurs.

À mes amis d'enfance: Mohammed, AbdelHack, AbdelRahim, Houdifa.

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

À mes amis d'étude : Mohammed, Brahim, Rabeh, Boubakeur

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

Dédicaces Ibrahim

Je dédie ce travail, A ma ***mère*** *avec toute mon affection,*

A mon ***père*** *et grand frère* ***Mohamed*** *avec toute ma reconnaissance,*

A mon petit frère ***Hamza*** *et mes* ***sœurs****, A tous mes* ***oncles*** *et* ***tantes****,*

A tous mes ***amis*** *pour leurs soutiens et leurs encouragements.*

Et a toute ma ***famille****.*

Remerciements

En tout premier lieu, nous remercions du plus profond de nos cœurs ALLAH de nous avoir éclairés vers le bon chemin. Je tiens à remercier ma famille pour son apport affectif et ses sacrifices. Nous ne saurons suffisamment remercier la personne qui m'a aidé à réaliser ce travail dans les meilleures conditions mon encadreur monsieur Samai Djamel. Sa disponibilité, sa patience tout au long de ce travail nous a été bénéfique. Nous tenons à remercier Mr Ben sid et Mr Kourichi pour leur aide. 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.

Abstract

Authentication and verification of FKP have several advantages over other biometric technologies: it is natural, non-intrusive and easy to use. The uni-modal biometric systems allow to recognize a person using a single biometric modality, but cannot guarantee with certainty proper authentication. So, the solution is the establishment of multimodal biometric systems obtained by merging several FKP recognition systems. In this present work, we discuss several important issues concerning multimodal biometrics. First, after drawing up a state of the art of FKP recognition and studied several methods to select the best authentication systems FKP based. Then we present the multi-samples of FKP (left and right index and left and right middle) and muti-algorithm using score fusion by melting PCA and Gabor. Finally, we will compare the different score combination of methods to choose the best among them.

Keywords: authentication, biometric, uni-modal, multimodal, fusion, multi-samples, PCA, Gabor.

Résumé

L'authentification et l'identification des FKP possèdent plusieurs avantages par rapport aux autres technologies biométriques : elle est naturelle, non intrusive et facile à utiliser. Les systèmes biométriques unimodals permettent de reconnaître une personne en utilisant une seule modalité biométrique, mais ne peuvent pas garantir avec certitude une bonne authentification. Alors la solution est la mise en place des systèmes biométriques multimodals obtenus en fusionnant plusieurs systèmes de reconnaissance de FKP. Dans ce présent travail, nous abordons plusieurs points importants concernant la biométrie multimodale. Tout d'abord, après avoir dressé un état de l'art de la reconnaissance de FKP et étudié plusieurs méthodes pour sélectionner les meilleurs systèmes d'authentification de FKP. Ensuite, nous présentons les multi-échantillons des FKP (l'index gauche et droite et milieu gauche et droite) et la muti-algorithme par la fusion de score pour l'analyse en composantes principales (ACP ou PCA en anglais) et Gabor. Enfin, on va comparer les différentes méthodes de combinaison de score pour choisir la meilleur parmi elles.

Mots clés : authentification, biométrie, unimodale, multimodale, fusion, multi-échantillons, PCA, Gabor.

Chapitre3 Résultats et discussions

Abréviation

ADN : Acide D´esoxyriboNucléique

EER : Equal Error Rate

FAR : False Acceptance Rate

FKP : Finger Knuckle Print

FRR : False Rejection Rate

GAR : Genuine Acceptance Rate

PCA : Principal Component Analysis

ROC : Receiver Operating Curve

ROI : Region Of Interest

PIN : personal identification number

Introduction générale

Le développement internationale des communications, tant en volume qu'en diversité (déplacements des individus, transactions financières, accès aux services...), d'autre part l'augmentation du taux de criminalité, le piratage…etc. Ce qui nécessite le besoin de s'assurer de l'identité des individus, les systèmes traditionnels de sécurité sont basés sur une connaissance à priori "knowledgebased" (code PIN, mot de passe…)[1] ou sur une possession d'un objet "token-based" (clef ,pièce d'identité, badge…)[1], mais ces systèmes sont moins fiables pour beaucoup d'environnements, à cause de leur inhabilité commune à distinguer un individu réellement autorisé d'un fraudeur[2] (personnes ayant acquis ses privilèges d'accès frauduleusement), l'identification de l'individu est devenue essentielle pour assurer la sécurité des systèmes et organisations face à cette sollicitation grandissante, plusieurs méthodes de reconnaissance biométriques ont été proposées, reconnaissance faciale, reconnaissance du locuteur, empreinte digitale, reconnaissance de l'iris, de la forme de la main , de la rétine. c'est ce qui a permis a la biométrie de s'étendre vite à de nombreuses applications destinées a gérer l'accès a des ressources **physiques** (aéroports, casinos…etc.) et **logiques** (ordinateurs, comptes bancaires… etc.).

Dans cette perspective, un de ces systèmes a été choisi d'être étudié dans ce mémoire, c'est le système de reconnaissance par images FKP, ou plus exactement, un système qui utilise l'empreinte des doigts comme caractéristique biométrique d'identification des individus. Une image FKP d'une personne demeure stable durant toute sa vie, et son modèle est unique pour chaque individu aussi elle ne représente pas une gène pour l'utilisateur. Tout cela, fait de cette méthode d'authentification un bon candidat pour des environnements sécurisés.

Dans ce travail, nous allons nous focaliser sur une réalisation d'un système complet d'authentification par FKP comme trait biométrique. Le but est de développer une extraction robuste du modèle (template) biométrique par l'utilisation de deux méthodes PCA et GABOR et une méthodologie de comparaison de ces modèles. On va, aussi, utiliser la fusion des échantillons FKP et on compare les différentes méthodes de combinaison de scores pour

choisir la meilleur. En outre, le modèle ou le pattern biométrique doit être aussi compact que possible pour assurer une rapidité de calcul.

Nous présentons un système de reconnaissance FKP nous préconisons d'implémenter une technique pour l'extraction de caractéristiques pour l'analyse biométrique du FKP. Pour cela nous adoptons deux méthodes statistiques bien connues **PCA** et **Gabor** Cela réduit grandement les tailles des images, maintient un temps de calcul raisonnable et une discrimination efficace.

Notre mémoire se présente sous **trois chapitres** comme suit : Dans le **premier chapitre** nous définissons la biométrie et les différentes techniques utilisées. Le **deuxième chapitre** est consacré à l'étude des systèmes multimodals et les différents niveaux de fusion et les méthodes PCA et Gabor L'implémentation réalisée et les résultats obtenus se trouvent dans **.le troisième chapitre**. Il se présente en quatre expérimentations dans la première expérimentation nous avons mis en œuvre un Système de reconnaissance multi algorithmes sur la modalité FKP. Nous avons étudié les résultats obtenues issues par les algorithmes **PCA** et du filtre de **GABOR**. Puis la deuxième expérimentation ou on va faire la fusion au niveau des scores des algorithmes PCA et GABOR de chaque doigt parmi les quatre.

La troisième expérimentation fait la fusion des scores de L'Index gauche avec le Milieu gauche et L'Index droit avec Milieu droit conçus par les fusions obtenus dans l'étape précédente, finalement la quatrième expérimentation ou nous allons fusionnés les résultats obtenu dans l'expérimentation numéro trois Aussi dans cette étape on va tester trois méthodes de combinaison de scores (somme, min et max) pour choisir la meilleur entre elle. En fin, nous terminons notre mémoire par une conclusion.

Chapitre 1

Biométrie pour l'identification

1.1. Introduction

De plus en plus, notre société éprouve le besoin de se contrôler. Que ce soit pour garantir la sécurité des gens dans les lieux publics ou pour éviter le détournement ou le vol d'informations sensibles ce qui pose un grand problème pour les personnes, les entreprises et les gouvernements dans leur quête de protection de données contre le vol.

L'apparition de l'ordinateur et sa capacité à stocker les données et traiter les caractéristiques biométriques par certain ordre de processus automatisés à l'aide des dispositifs comme des modules de balayage, ont permis la création des systèmes biométriques informatisés qui envahit notre quotidien depuis quelques années. L'utilisation de la biométrie qui permet de vérifier que l'usager est bien la personne qu'il prétend être, s'est répandue énormément dans la vie quotidienne et trouve de nombreuses applications.

De nombreux travaux de recherche ont été menés et en cherche toujours de nouvelles méthodes, devant cette déferlante, il était nécessaire de faire le point sur ce qu'est exactement la biométrie, quelles techniques existent vraiment et leur degré de fiabilité pour ensuite détailler les plus utilisées dans ce chapitre.

1.2. Définition de la biométrie

On peut la définir comme suit :

-Le terme de **biométrie** est originaire d'une contraction des deux anciens termes grecs :
« bios » qui signifie : la vie et « metron » qui se traduit par : mesure **[3]**.

-La **biométrie** est la science d'établir l'identité d'une personne par l'analyse mathématique basée sur les attributs **morphologiques** (empreinte digitale, visage…etc.) ou **comportementales** (la démarche, la dynamique de frappe au clavier, la voix…etc.) ou **biologiques** (salive, ADN…etc.) liés à un individu. Ces caractéristiques sont appelées modalités biométriques qui doivent être **fiables**, **infalsifiables**, **universelles**, **uniques** pour chaque individu, **permanentes**, **enregistrables** et finalement **mesurables**.

1.3. Etat de l'art des techniques biométriques

Dans les mesures de la biométrie ils existent trois types principaux (morphologiques, comportementales et biologiques) et cela pour obtenir des informations concernant les traits personnels [4].

La diversité de modalité biométrique comme la figure 1.1 illustre apparaît continûment de nouvelle, dans ce qui suit nous ne décrivons que les modalités les plus communes à savoir le visage, la parole…etc.

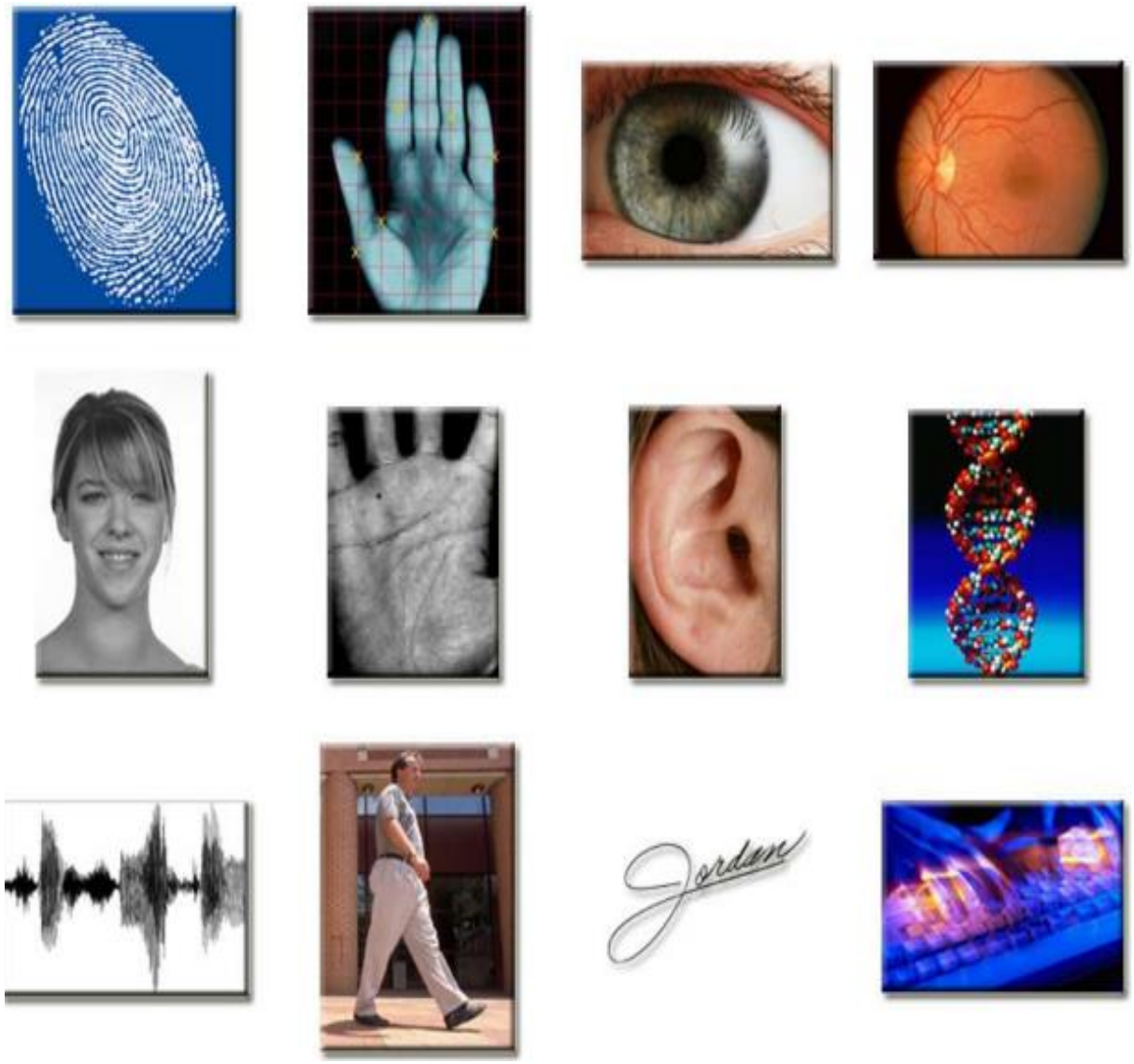


Figure 1.1 – illustration de la diversité des techniques biométriques.

1.3.1 Biométrie morphologique (physique)

1. Empreinte digitale : L'identification à l'aide des empreintes digitales est la technique biométrique que la plupart des gens connaissent. Il s'agit de la plus vieille technique biométrique **[4],** les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Ces éléments sont appelés **minuties** **[2]**. Les **minuties** sont des changements de continuité de l'empreinte digitale. Il existe plusieurs types de minuties : lac, bifurcation, delta ou impasse...etc. généralement une quarantaine sont extraites de la zone scannée. Statistiquement il est impossible de trouver douze points identiques chez deux individus.

Ce type de système est utilisé par les institutions financières pour leurs employés et leurs clients. Il se retrouve également dans les hôpitaux, les écoles, les aéroports, les cartes d'identité, les passeports, les permis de conduire et de nombreuses autres applications.

Son prix est faible, la taille du lecteur biométrique d'empreinte digital n'est pas volumineuse et le système reste très simple à mettre en place.

2. 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. L'individu doit être positionné devant la caméra ou peut être en mouvement à une certaine distance, le système retire certaines caractéristiques essentielles, uniques, et invariables comme (yeux, nez, le haut des joues, les coins de la bouche…etc.) selon le système utilisé.

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 [4].

3. 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.

Environ 250 caractéristiques sont capturées, l'identification par l'iris est presque infalsifiable s'accroit en popularité ces dernières années dans le secteur financier pour les employés et les clients, dans les institutions carcérales, dans les aéroports et c'est une technique qui continuera sans doute à être employée couramment, mais elle est relativement désagréable pour l'utilisateur car l'œil doit rester grand ouvert et il est éclairé par une source lumineuse pour assurer un contraste correct toutefois la fraude étant néanmoins possible en utilisant des lentilles.

4. Empreintes des articulations des doigts –FKP-: Chaque doigt possède trois articulations et trois os qui sont appelés la phalange proximale, la phalange médiane et la phalange distale.

La première articulation est l'endroit où le doigt se joint à la main appelé la phalange proximale. Le deuxième joint est l'articulation interphalangienne proximale, ou conjointe PIP : l'articulation du Doigt et la surface arrière du doigt, il est également connu sous le nom dos de la main. Les modèles de peau inhérents à la surface extérieure autour de l'articulation de la phalange de doigt de l'individu, à une grande capacité à discriminer des individus différents. Tel motif d'image du doigt est unique et peut être l'obtention ligne, hors ligne pour l'authentification. L'extraction d'éléments de jointure pour l'identification dépend de l'utilisateur. Certains chercheurs extraient les caractéristiques pour l'authentification qui sont représentés sur la figure **1.2** Les caractéristiques sont centre de phalangienne, ligne en forme de U autour de la phalange. Le nombre de lignes, la longueur et l'espacement entre les lignes. **'**Knuckle' motifs pliage et les bavures comme moyen d'identification photographique. Ces caractéristiques sont uniques et peuvent être utilisé pour l'identification.

Figure 1.2 – lignes principales et secondaires (texture) crête ridules.

1.3.2. Biométrie comportementale

1. 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 y-a 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 [2].

L'acceptation de cette technique est très bonne car la signature est un geste commun pour tout le monde, ces systèmes sont utilisés dans les compagnies pharmaceutiques, les prisons, les services postaux et les banques, mais cette technique n'est pas très précise car la signature peut être affectée par des facteurs physiques et émotionnels au même temps il y-a des incohérences de certaines personnes en signant leur nom dynamiquement et graphiquement aussi la falsification est possible en passant par une phase d'apprentissage.

2. Voix : La 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.

Les caractéristiques physiologiques de la voix d'un individu comme le débit, la force (pitch), la dynamique et la forme des ondes produites sont uniques et invariantes mais les caractéristiques comportementales changent avec le temps, selon les conditions sanitaires (mal de gorge) et des états émotionnels…etc. Ce qui diminue l'exactitude du taux d'identification. Ces systèmes sont utilisés par les corps policiers, les agences d'espionnage et en téléphonie. La capture de la voix est relativement facile à effectuer à l'aide d'un microphone. Mais ce moyen est sensible à un grand nombre de facteurs tels que le bruit, la fatigue, le stress ou la maladie peuvent altérer la voix. Aussi la fraude est possible par enregistrement [2]. Ce qu'il ne rend pas un système complètement fiable.

3. 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 [2], l'intérêt de cette technologie réside que l'identification de démarche se situe dans la capacité d'identifier un individu à distance [4].

Elle peut, aussi, détecter les comportements suspects (par vidéo-surveillance), on l'utilise pour le contrôle d'accès aux bâtiments ou aux zones réglementées mais elle est facilement modifiable par l'individu.

4. 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.

Ce dispositif biométrique est utilisé comme méthode de vérification pour le commerce électronique et comme mécanisme de contrôle d'accès à des bases de données.

Il est facilement accepté par l'utilisateur, le but principal de cette technique est de renforcer la sécurité à des coûts moins élevés.

1.3.3. Biométrie biologique

1. La rétine : cette mesure biométrique se base sur le fait que les vaisseaux sanguins d'une rétine sont différents d'une personne à une autre et stables durant la vie [4].

L'utilisateur doit placer son œil à quelques centimètres d'un orifice de capture situé sur le lecteur de rétine. Un faisceau lumineux traverse l'œil jusqu'aux vaisseaux sanguins capillaires de la rétine. Le système localise et capture ainsi environ 400 points de référence. Cette technique demande la collaboration étroite de la part de l'utilisateur, car il doit placer son œil devant la caméra.

Cette technologie est la plus complexe à falsifier, mais probablement à cause de son coût élevé elle n'est pas utilisée que dans les cas où la sécurité est primordiale, notamment dans le domaine militaire [2], le secteur spatial (NASA) et par des agences d'espionnage comme la CIA. L'analyse biométrique de la rétine est la technologie la plus difficile à mettre en œuvre, aussi elle trouve peu de faveur au sein de la communauté parce qu'elle présente une gène pour les utilisateurs (rester sans cligner les yeux pendant quelque instants).

2. Structure des veines : On a longtemps considéré que le modèle des veines dans l'anatomie humaine peut être unique aux individus. En conséquence, il y a eu de diverses réalisations du balayage de veine au cours des années, du balayage de **main**, au balayage de **poignet** et, plus récemment, au balayage de **doigt**. Cette technique utilise un «scanner du réseau veineux palmaire», pour être identifié il faut placer la surface concernée au-dessus du lecteur. Il s'agit, ici, d'analyser le dessin formé par le réseau des veines pour en garder quelques points caractéristiques [4].

1.4. Phases de fonctionnement d'un système biométrique

Selon le contexte de l'application, un système biométrique peut fonctionner en mode d'enrôlement ou en mode de vérification ou bien en mode d'identification.

1. Phase d'enrôlement : Est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier. Pendant l'enrôlement, les modalités biométriques sont mesurée en utilisant un capteur biométrique, ses caractéristiques qui vont être traités sont, ensuite, insérées dans une base de données [4], [4] biométriques permettant de relier un vecteur de caractéristiques à une identité.

2. Phase de reconnaissance : Est une comparaison "un à un", consiste à contrôler si l'individu utilisant le système est bien la personne qu'il prétend être en comparant les données biométriques capturées (d'un nom d'utilisateur, d'une carte futée…etc.) à sa propre base de données, le système doit alors répondre à la question «Suis je bien la personne que je prétends être?» [2], [4].

Dans cette phase, les systèmes biométriques effectuent une mise à jour des patterns pour les types de traits biométriques qui changent légèrement à travers le temps (Reconnaissance faciale).

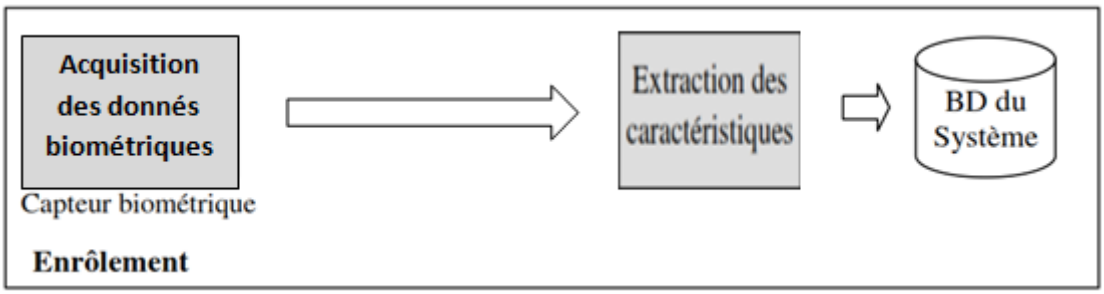
3. Le mode d'identification : Elle est plus connue sous le nom 1 parmi N [5], car elle permet de déterminer lequel des utilisateurs correspond le mieux à l'individu inconnu a partir des modèles de la base de données d'identités [4]. Elle ajoute la possibilité de vérifier si l'utilisateur appartient réellement à la base de données « Qui suis-je ? » [2].

1.5. Principaux modules du système biométrique

Un système biométrique est composé de quatre modules principaux :

Comment opère un système biométrique ?. Un système biométrique est essentiellement un système de reconnaissance qui nécessite les informations biométriques d'un individu,

On extrait les caractéristiques de ces informations, on compare ces caractéristiques avec celles qui sont stockées dans la base de données et on exécute une décision basée sur les résultats de cette comparaison c'est pour cela la structure générale d'un système biométrique se compose de quatre modules essentiels : chacun de ces modules est défini dans ce qui suit.



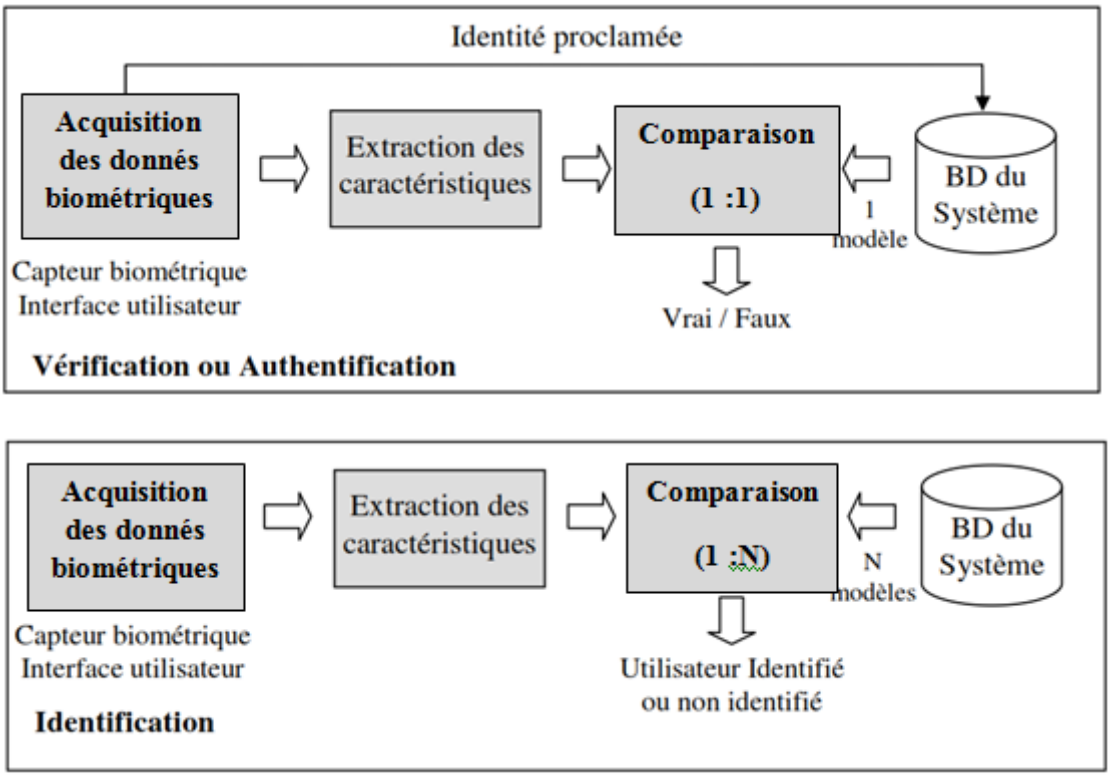


Figure 1.3 - Principaux modules d'un système biométrique ainsi que les différents modes.

1. **Module d'acquisition biométrique :** correspond à la lecture de certaines caractéristiques physiologiques, comportementales ou biologiques d'un individu [4] à l'aide d'un module de balayage, au moyen d'un capteur biométrique.

2. **Module d'évaluation de qualité et d'extraction de caractéristiques ou Module création d'une signature :** Les données biométriques acquises sont traitées d'une manière qui permet d'obtenir un modèle numérique de la personne ''signature biométrique'', Qui sera conservé sur un support portable (puce ou autre) ou dans une base de données [2].

3. **Module de comparaison (matching) et de prise de décision :** compare les caractéristiques biométriques d'une personne soumise à contrôle avec les « signatures » mémorisées. Le résultat de taux de correspondance de la signature va être utilisé pour prendre une décision pour la validation ou le rejet de l'identité de l'individu à reconnaitre.

4. **Module base de données :** stocke les modèles biométriques des utilisateurs enrôlés [4].

1.6. 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 Biometric Group [IBG]** – à effectuer une étude basée sur quatre critères d'évaluation :

1. **Intrusivité** : l'existence d'un contact direct entre le capteur utilisé et l'individu à reconnaitre.
2. **Fiabilité** : ce critère influe sur la reconnaissance de l'utilisateur par le système.
3. **Coût** : doit être raisonnable.
4. **Effort** : déployer par l'utilisateur lors de la saisie de mesures biométriques.

Au même temps, on peut mesurer la performance d'un système biométrique par deux indices : le FAR et le FRR.

- Le **FAR**: 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) [2], [6].

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

- Le **FRR**. 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) [2], [6].

$$\mathbf{FRR} = \frac{\text{Nombre des clients rejetés}}{\text{Nombre totale d'accès clients}} \qquad (1.2)$$

Ces deux indices sont liés : une diminution du **FAR** entraîne systématiquement une augmentation du **FRR** (et inversement). Il s'agit d'adapter le système en fonction du niveau de sécurité souhaitée.

La statistique la plus simple pour mesurer la performance d'un algorithme est de calculer le point d'équivalence des erreurs [2].

● **Le EER** Il est fréquemment utilisé pour donner un aperçu de la performance d'un système, Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations comme représente la figure **1.4**. Seuls des systèmes qui produisent des taux **EER** faibles sont capables d'être déployés en mode identification. Ainsi, les protocoles d'évaluation diffèrent dans le mode identification et le mode vérification.

$$\mathbf{EER = FAR = FRR} = \frac{\mathrm{FAR}\times X+\mathrm{FRR}\times Y}{X+Y} \qquad (1.3)$$

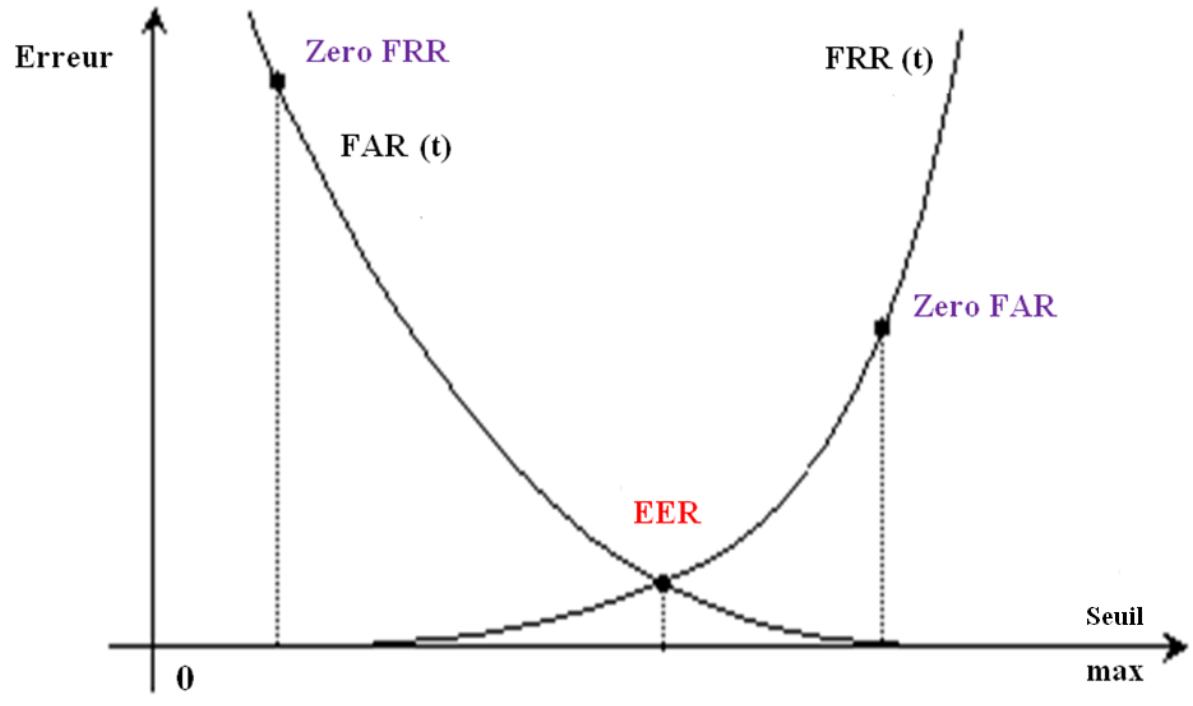


Figure1.4 - graphe démonstratif EER représente la marge d'erreur autorisée par un système.

Les performances d'un système biométrique (vérification et identification en ensemble ouvert) peuvent être présentées graphiquement à l'aide de la **courbe ROC** (Figure **1.5**). Sur laquelle les FRR sont données en fonction des FAR. Cette courbe est obtenue en calculant un couple (FAR, FRR) pour chaque valeur du seuil de décision, ce dernier varie de la plus petite valeur des taux obtenus en phase de test a la plus grande valeur. Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé. La performance globale d'un système de vérification d'identité est mieux caractérisée par sa courbe caractéristique de fonctionnement **ROC**, qui représente le **FAR** en fonction du **FRR.**

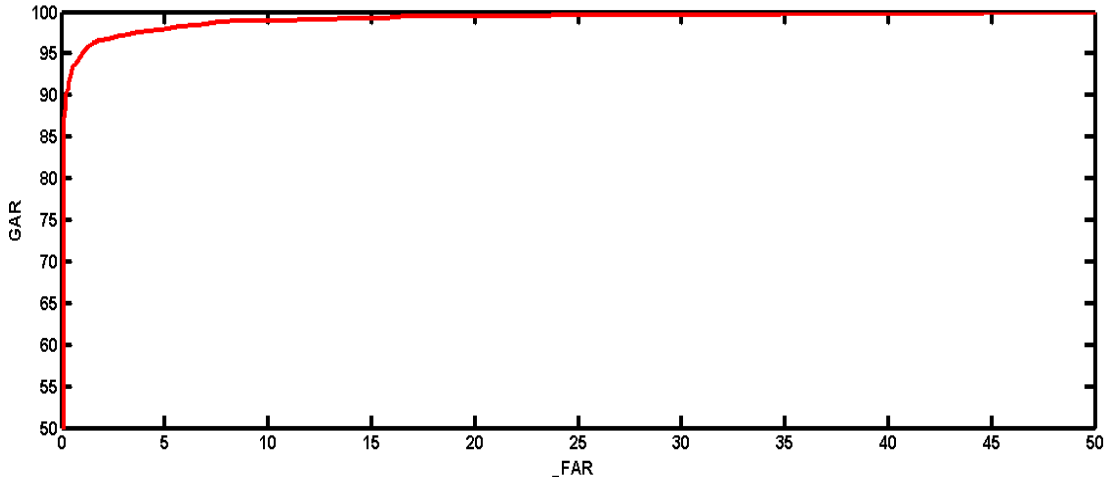


Figure 1.5 - Courbe ROC.

Le taux d'égale erreur **EER** est représenté graphiquement par l'intersection de la courbe ROC avec la première bissectrice... [10].

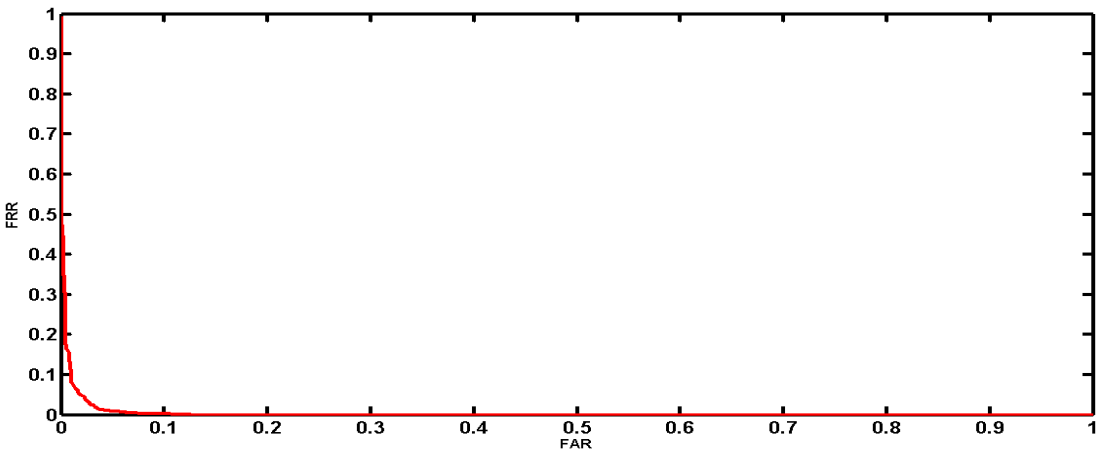


Figure 1.6 - Courbe DET.

Dans le cas des systèmes biométriques, la courbe DET est souvent préférée à la courbe ROC. En effet, la courbe DET trace les taux d'erreur sur les deux axes (FAR sur l'axe des abscisses contre FRR sur l'axe des ordonnées) en utilisant une normalisation de l'échelle (Figure**1.6**). Elle distribue les valeurs d'une manière homogène et permet de comparer les performances de plusieurs systèmes de façon très claire.

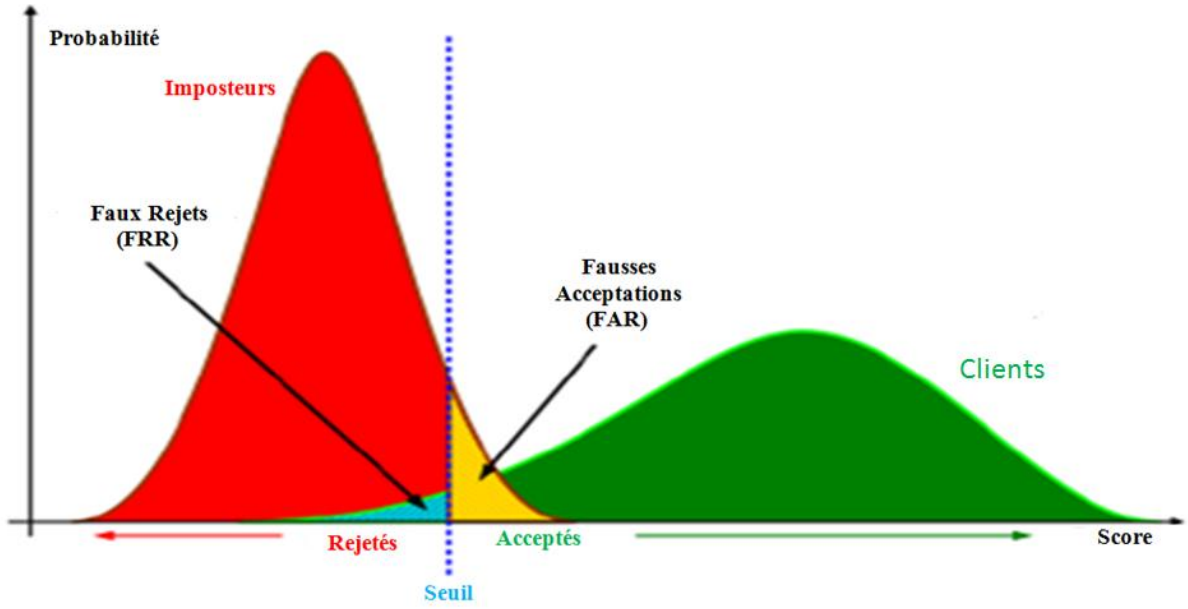


Figure1.7 - courbes de distribution des imposteurs et des clients.

Comme la Figure **1.7** illustre, on a toujours une zone de recouvrement. On aimerait évidemment avoir les deux distributions parfaitement disjointes, ce qui permettrait idéalement de séparer les clients des imposteurs, mais ce n'est jamais le cas dans la réalité.

1.7. Applications des systèmes biométriques

De nos jours, les systèmes biométriques sont de plus en plus utilisés dans des applications civiles, les applications de la biométrie peuvent être divisées en trois groupes principaux:

1.7.1. Applications commerciales : telles que l'ouverture de réseau informatique, la sécurité de données électroniques, le commerce, l'accès Internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance…etc.

1.7.2. Applications gouvernementales : telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports…etc.

1.7.3. Applications légales : telles que l'identification de corps, la recherche criminelle, l'identification de terroriste…etc.

1.8. Conclusion

Dans ce premier chapitre, nous avons présenté le cadre de ce mémoire, aussi, nous avons mis en relief quelques notions et définitions de base liées à la biométrie et sa diversité technologique, les différents modes et modules des systèmes biométriques. Nous avons, aussi, donné un aperçu sur les techniques de mesure et leurs performances, ainsi, que les domaines d'applications.

Chapitre 2

La multimodalité et la fusion des données

2.1 Introduction

Comme il a été annoncé dans le premier chapitre concernant les systèmes uni-modaux (c'est à dire utilisant une seule modalité), nombreuses limitations imposées par l'utilisation des systèmes biométriques unimodaux inclus les taux d'erreurs associés à ces systèmes biométriques qui sont restés relativement élevés. Ce qui les rend inacceptables pour un déploiement d'applications critiques de sécurité. Donc, chaque système en soi ne peut pas, toujours, être utilisé de manière fiable pour effectuer la reconnaissance. Cependant, la consolidation d'informations présentées par les différentes modalités peut permettre une authentification précise de l'identité. Ces dernières années, ont a vu l'émergence d'une approche innovante qui est l'utilisation de plusieurs modalités biométriques au sein d'un même système. On parle alors de système biométrique multimodal qui est étudié dans le reste de notre mémoire. La biométrie multimodale s'impose de manière indéniable comme une alternative d'avenir dans le domaine de la sécurité des personnes et leurs biens.

2.2. Définition de La biométrie multimodale

La biométrie multimodale est la combinaison de plusieurs modalités biométriques différentes, par exemple la biométrie de l'empreinte digitale + la biométrie du visage ou la biométrie de la voix + la biométrie de démarche. Elle permet de réduire certaines limitations des systèmes basés sur une seule modalité tout en améliorant, de manière significative, leurs performances de reconnaissance en augmentant la quantité d'informations discriminante de chaque personne et l'utilisation d'informations complémentaires pour une personne donnée [5].

De plus, le fait d'utiliser plusieurs modalités biométriques augmente la robustesse aux fraudes.

Cette technique permet :

- soit d'augmenter la sécurité en augmentant la certitude de l'identité de la personne.
- soit d'identifier une personne par l'une ou l'autre de ces données biométriques en cas de problème de lecture d'une des données [10].

2.3. L'architecture des systèmes multimodals

Les systèmes multimodaux associent plusieurs systèmes biométriques et nécessitent, donc, l'acquisition et le traitement de plusieurs données. L'acquisition et le traitement peuvent se faire successivement, on parle, alors, d'architecture en série, ou simultanément, on parle alors d'architecture en parallèle.

En effet, la différence entre un système multimodal en série et un système multimodal en parallèle réside dans le fait d'obtenir un score de similarité à l'issue de chaque acquisition (fusion en série) ou de procéder à l'ensemble des acquisitions avant de prendre une décision (fusion en parallèle) [17] .

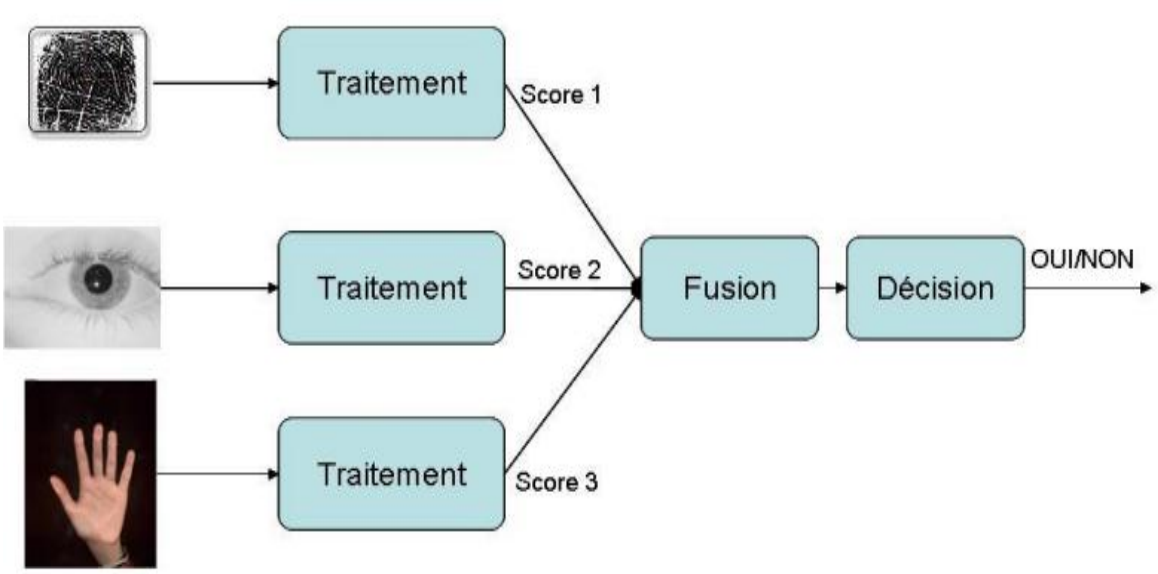


Figure 2.1 - Architecture de fusion en parallèle.

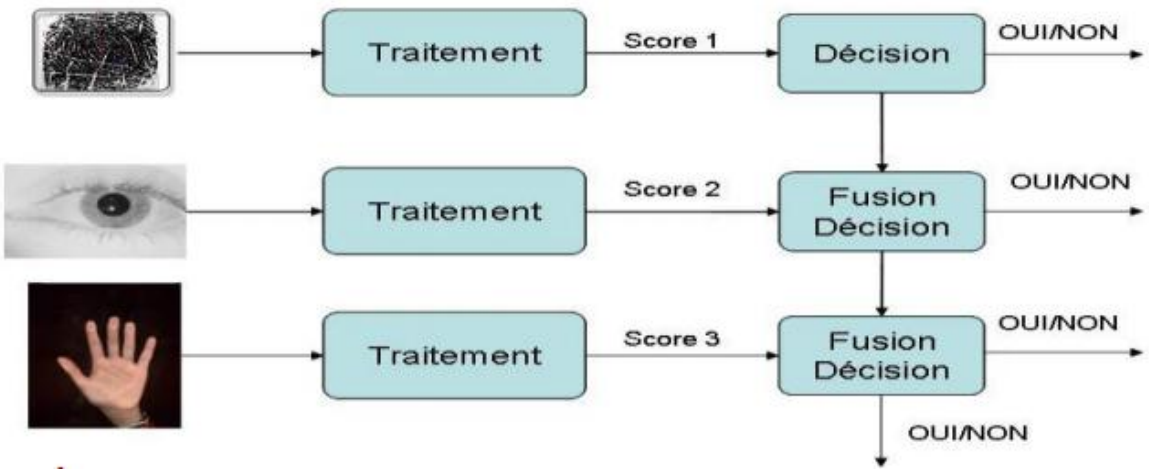


Figure 2.2 - Architecture de fusion en série.

L'architecture en **parallèle** (figure **2.1**) est la plus utilisée car elle permet d'utiliser toutes les informations disponibles et donc d'améliorer les performances du système. En revanche, l'acquisition et le traitement d'un grand nombre de données biométriques est coûteux en temps et en matériel, et réduit le confort d'utilisation. C'est pour cela que l'architecture en **série** (figure **2.2**) peut être privilégiée dans certaines applications par exemple si la multimodalité est utilisée pour donner une alternative pour les personnes ne pouvant pas utiliser l'empreinte digitale. Pour la majorité des individus seule l'empreinte est acquise et traitée mais pour ceux qui ne peuvent pas être ainsi authentifiés on utilise un système à base d'iris alternativement [17].

2.4. Les différents multi- possibles (les types de fusion)

La fusion d'éléments biométriques peut se référer à de nombreux scénarios différents.

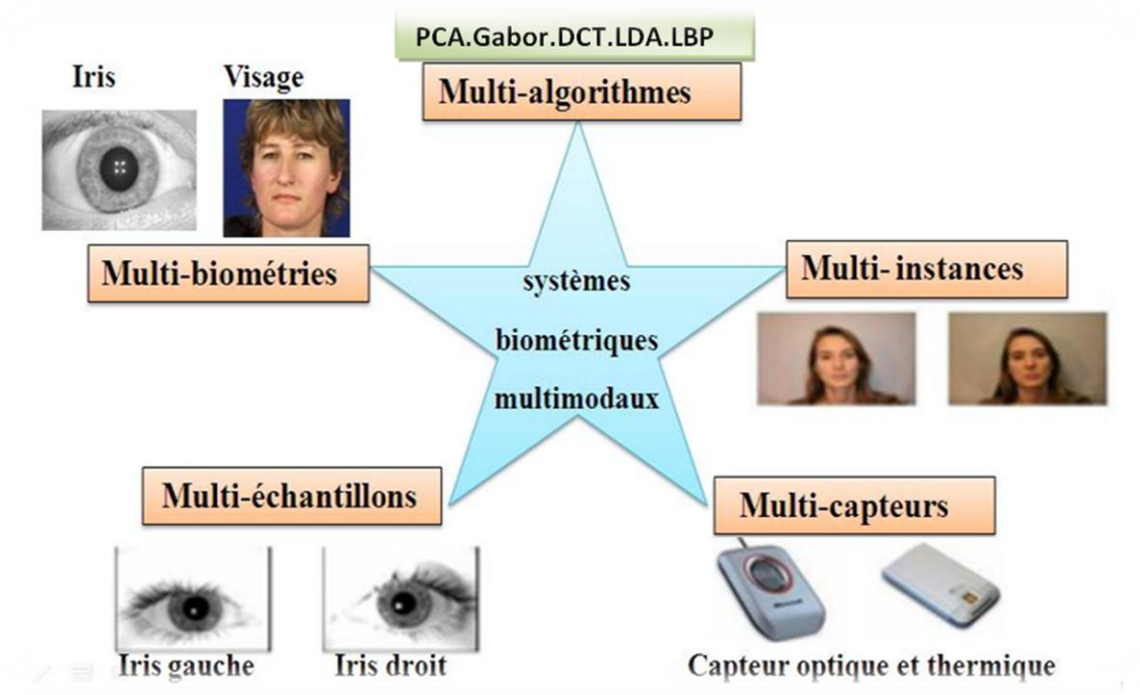


Figure 2.3 - Les différents systèmes multimodaux

2.4.1. Systèmes Multi-capteurs

Dans ces systèmes, la même modalité est obtenue à l'aide de plusieurs capteurs afin d'extraire diverses informations provenant de l'enregistrement des images par exemple un capteur optique et un capteur capacitif pour l'acquisition de l'empreinte digitale. Ce type de système permet notamment la fusion au niveau capteur, ce que ne permettent pas d'autres systèmes comme les systèmes multimodaux, aussi l'utilisation de plusieurs capteurs permet d'acquérir des informations complémentaires pour accroître les performances des systèmes unimodaux [10].

2.4.2. Systèmes Multi-biométries

Cette classe correspond aux systèmes impliquant plusieurs modalités biométriques. Ce type de système combine différents traits biométriques d'un individu. Les fusions visage iris, ou visage empreinte digitale font partie de ce type d'approche. On s'attend à ce que des traits biométriques décorrélés (comme les empreintes digitales et l'iris) fournissent une nette amélioration de la performance d'un système que des traits biométriques corrélés (comme la voix et les mouvements des lèvres).

Ces systèmes nécessitent différents capteurs ainsi que des algorithmes dédiés à chaque caractère biométrique. La précision en reconnaissance peut significativement être améliorée en utilisant un nombre croissant de traits biométriques. Puisque Cette classe correspond aux systèmes impliquant plusieurs modalités biométriques le coût de la réalisation de ces systèmes est généralement élevé, ceci est dû principalement à l'utilisation de plusieurs capteurs, et, par conséquent, la mise en place d'interfaces utilisateurs appropriées.

2.4.3. Systèmes Multi-instances

Ce type de système permet de capturer plusieurs instances du même caractère biométrique. Ces systèmes utilisent tout simplement plusieurs instances d'un même trait biométrique. L'acquisition de plusieurs empreintes digitales via le même capteur est l'exemple typique de ce type de système. Ces systèmes n'entraînent pas généralement de surcoût de capteurs, ni le développement de nouveaux algorithmes d'extraction de caractéristiques. À ne pas confondre avec les systèmes multi échantillons.

2.4.4. Systèmes multi-échantillons

Un unique capteur peut être utilisé pour acquérir plusieurs échantillons du même trait biométrique dans le but de prendre en compte les variations qui peuvent se produire au sein de ce trait, ou pour obtenir une représentation plus complète du caractère sous-jacent. Par exemple, un système de reconnaissance faciale peut capturer (et enregistrer) le profil frontal du visage d'une personne ainsi que les profils gauches et droits afin de tenir compte des variations de la pose faciale, 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.

2.4.5. Systèmes multi-algorithmes

Lorsque plusieurs algorithmes traitent la même image acquise, par exemple des algorithmes d'analyse de texture et de minuties peuvent être associés pour traiter la même image d'empreinte digitale afin d'extraire diverses caractéristiques qui peuvent améliorer la performance du système [13]. 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. Ainsi, ce genre de

système ne nécessite pas de capteurs supplémentaires et n'oblige pas l'utilisateur à interagir avec de multiples capteurs, d'où l'amélioration de la commodité d'utilisation [12].

2.4.6. Système hybride

Le terme hybride est utilisé pour désigner un système multibiométrique qui intègre un sous-ensemble de plusieurs scénarios parmi ceux présentés précédemment. Par exemple, un système qui comprend deux classifieurs pour la reconnaissance du locuteur et trois autres pour la reconnaissance du visage est à la fois multi-classifieurs car il intègre plusieurs classifieurs pour une même modalité et multimodal puisque plusieurs modalités biométriques sont impliquées. Les systèmes hybrides disposent donc de plus d'information que les systèmes précédents [13] [14].

2.5. Les niveaux de fusion

La fusion d'informations est un domaine de recherche spécifique qui étudie les différentes façons de fusionner des informations de nature différentes en exploitant au mieux les caractéristiques de chaque source. 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 **2.4**).

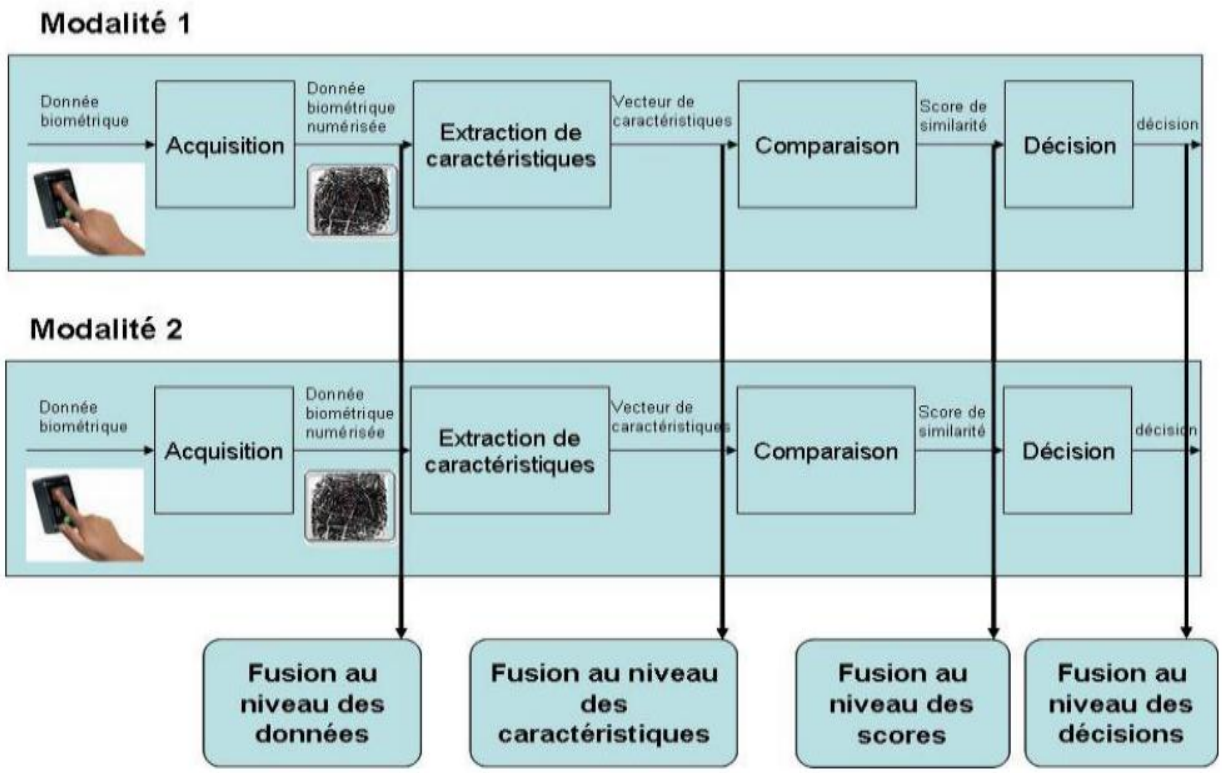


Figure 2.4 - illustration des différents niveaux de fusion.

Nous allons maintenant détailler ces niveaux de fusion que l'on peut répartir en deux grandes familles :

_ La fusion pré-classification (avant comparaison).

_ La fusion post-classification (après la comparaison).

2.5.1. La fusion pré-classification

La fusion pré-classification correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur (images brutes) ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques.

1. Niveau du capteur (Sensor Level)

A ce niveau, seuls les capteurs sont dédoublés et les données brutes ("raw data") issues de ces capteurs sont combinées, cette fusion de différentes sources permet de simplifier l'architecture des systèmes biométriques. Les sorties des capteurs sont regroupées pour ne former qu'un seul signal qui est alors utilisé comme entrée d'un système de reconnaissance

automatique[10], cette fusion n'est généralement pas possible si les instances des données sont incompatibles (par exemple, il est peut être difficile de fusionner des images de visages provenant de caméras ayant des résolutions différentes). De ce fait, les approches utilisant une fusion de données brutes peuvent améliorer les performances des systèmes, mais la fusion au niveau capteur est relativement peu utilisée [15].

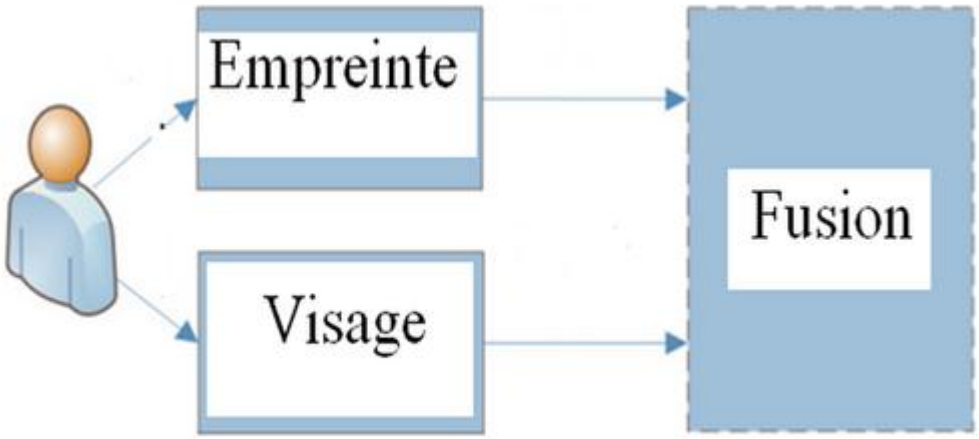


Figure 2.5 – système d'acquisition pour la fusion au niveau captures.

2. Niveau Caractéristiques (Feature Level)

La 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.

Elle consiste à combiner différents vecteurs de caractéristiques ("feature vectors") qui sont obtenus à partir d'une des sources suivantes: plusieurs capteurs du même trait biométrique, plusieurs instances du même trait biométrique, plusieurs unités du même trait biométrique ou encore plusieurs traits biométriques [17].

Lorsque les vecteurs de caractéristiques sont homogènes (plusieurs prises d'une empreinte d'un individu), il en résulte un seul vecteur de caractéristiques.

Les méthodes de fusion pré-classification sont assez peu utilisées car elles posent un certain nombre de contraintes qui ne peuvent être remplies que dans certaines

applications très spécifiques. En revanche, la fusion post-classification est très étudiée par les chercheurs [17].

2.5.2. La fusion post-classification

La fusion post-classification peut se faire au niveau des scores issus des modules de comparaison ou au niveau des décisions. Dans les deux cas, la fusion est en fait un problème bien connu de la littérature sous le nom de "Multiple Classifier systems".

1. Niveau Score (Score Level)

La fusion de scores est certainement l'approche la plus utilisée. Les différents sous-systèmes du système multimodal produisent des scores après l'étape de comparaison. Le mécanisme de fusion des scores permet de générer un nouveau score ou une classe finale à partir de ces scores. Ce type de fusion est 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.

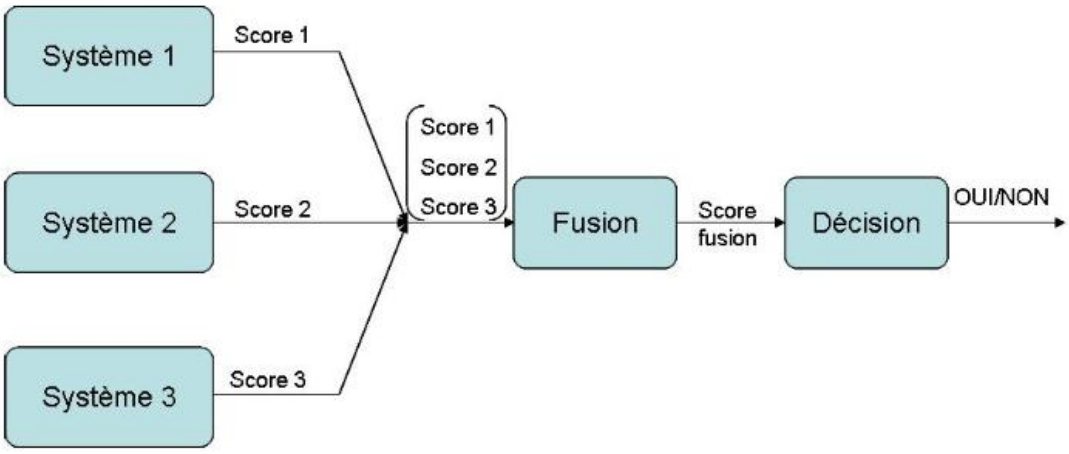


Figure 2.6 – Schéma de la fusion de scores.

1.2 Approche par combinaison de scores

Elle consiste à traiter le sujet comme un problème de **combinaison de scores** par des méthodes mathématiques de combinaison. Dans **l'approche par combinaison**, les scores individuels sont combinés de manière à former un unique score qui est ensuite utilisé pour prendre la décision finale. Afin de s'assurer que la combinaison de scores provenant de différents systèmes soit cohérente, les scores doivent d'abord être transformés dans un domaine commun : on parle alors de **normalisation de score** [17].

1.2.1. La normalisation des scores

Les méthodes de normalisation de scores ont pour objectif de transformer individuellement chacun des scores issus des systèmes pour les rendre **homogènes** avant de les combiner. En effet, les scores issus de chaque 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) [17]. De plus, chaque 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. On comprend bien la nécessité de normaliser les scores avant de les combiner. Les méthodes de normalisation présentées dans la suite, traitent des scores qui varient déjà tous dans le même sens (en général on considère tous les scores sous forme de similarité). Pour transformer des distances en similarité il existe deux solutions : l'inverse ou l'opposé. Dans toute la suite, nous considérerons que tous les scores à fusionner ont été transformés en scores de similarité (**scores Client > scores Imposteur**). Les différentes techniques de normalisation de scores sont :

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

1.2.2. Normalisation par la méthode Min-Max

La méthode du MinMax telle que

$$n(i)=\frac{s(i)-\min(i)}{\max(i)-\min(i)} \qquad (2.1)$$

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, aves les clients proches de la borne (1) et les imposteurs proches de la borne inférieure (0) [19].

Niveau des décisions

Ce type de fusion agit au niveau de l'espace de décision. Elle effectue l'association d'informations élaborées qui peuvent être considérées comme des propositions de décision

La fusion au niveau des décisions est souvent utilisée pour sa simplicité. Un utilisateur se présente au système multimodal, il donne son identifiant, le système effectue ensuite toutes les captures nécessaires à la vérification d'identité. En effet, chaque sous-système produit donc une décision binaire sous la forme OUI ou NON que l'on peut représenter par 0 et 1 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) [15].

2.6. Les différentes méthodes d'extraction des caractéristiques utilisées

2.6.1. Analyse en composantes principales (PCA)

L'algorithme ACP, PCA en anglais (Principal Component Analysis) est né des travaux de **MA. Turk** et **AP. Pentland** au **MIT Media Lab**, en **1991**. Il est aussi connu sous le nom de **Eigenfaces** car il utilise des vecteurs propres et des valeurs propres. Cet algorithme s'appuie sur des propriétés statistiques bien connues et utilise l'algèbre linéaire. Il est relativement rapide à mettre en œuvre mais il est sensibles aux problèmes d'éclairement, de pose et d'expression faciale. Il est à la base de nombreux algorithmes globaux actuels.

L'idée principale consiste à exprimer les M images d'apprentissage selon une base de vecteurs orthogonaux particuliers, contenant des informations indépendantes d'un vecteur à l'autre. Ces nouvelles données sont donc exprimées d'une manière plus appropriée à la reconnaissance du visage.

Nous voulons extraire l'information caractéristique d'une image de visage, pour l'encoder aussi efficacement que possible afin de la comparer à une base de données de modèles encodés de manière similaire. En termes mathématiques, cela revient à trouver les vecteurs propres de la matrice de covariance formée par les différentes images de notre base d'apprentissage.

Une image $I_i(m,n)$ est traitée comme un vecteur $\Gamma_i(m\times n,1)$ dans un espace vectoriel de grande dimension $(N=m\times n)$,par concaténation des colonnes .

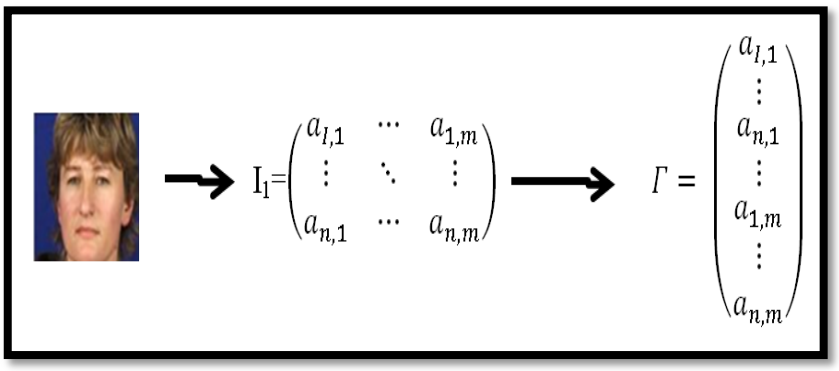


Figure2.7 - Passage d'une image vers un vecteur

Après avoir rassemblé nos M images dans une unique matrice, nous obtenons une

matrice d'images Γ, où chaque colonne représente une imageΓ_i :

$$\Gamma=\begin{pmatrix} a_{1,1} & b_{1,1} & \cdots & z_{1,1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,1} & b_{n,1} & \cdots & z_{n,1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{1,m} & b_{1,m} & \cdots & z_{1,1} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n,m} & b_{n,m} & \cdots & z_{n,m} \end{pmatrix} \qquad (2.2)$$

On calcule ensuite l'image moyenne Ψ de toutes les images collectées

Cette image peut être vue comme le centre de gravité du jeu d'images (Figure) :

$$\Psi = \frac{1}{N}\sum_{i=1}^{M} \Gamma i \qquad (2.3)$$

On ajuste ensuite les données par rapport à la moyenne.

Figure 2.8 - Image moyenne.

L'image moyenne est alors soustraite de chaque image avec la formule suivante:

$$\Phi_i = \Gamma_i - \Psi, \; i = 1 \ldots M \qquad (2.4)$$

On calcule ensuite la matrice de covariance du jeu de données. Cette matrice peut être vue comme une matrice de moments d'ordre 2 :

$$C = \sum_{i=1}^{M} \Phi_i \Phi_i = AA^T \; , A = [\Phi_1 \Phi_2 \cdots \Phi_M] \qquad (2.5)$$

La prochaine étape consiste à calculer les vecteurs propres et les valeurs propres de cette matrice de covariance C de taille (N × N), c'est-à-dire de l'ordre de la résolution d'une image.

Le problème est que cela peut parfois être très difficile et très long. En effet, si N > M (si la résolution est supérieure au nombre d'images), il y aura seulement (M -1) vecteurs propres qui contiendront de l'information (les vecteurs propres restants auront des valeurs propres associées nulles). Par exemple, pour 50 images de résolution 180 × 200, nous pourrions résoudre une matrice L de 50 × 50 au lieu d'une matrice de 36000 × 36000 pour ensuite prendre les combinaisons linéaires appropriées des images Φ_i.. Le gain de temps de calcul serait considérable, nous passerions d'une complexité de l'ordre du nombre de pixels dans une image à celle de l'ordre du nombre d'images.

Les étapes du processus qui nous permettent d'accélérer les calculs sont décrits ci- dessous :

Considérons les vecteurs propres e_i de C = AA^T, associés aux valeurs propres λ_i On a :

$$Ce_i = \lambda_i e_i \quad (2.6)$$

Les vecteurs propres $v_i$de $L = A^T A$, associés aux valeurs propres μ_i sont tels que :

$$Lv_i = \mu_i v_i \quad (2.7)$$

Soit :

$$A^T A v_i = \mu_i v_i \quad (2.8)$$

En multipliant à gauche par A des deux côtés de l'égalité, nous obtenons :

$$AA^T A v_i = A\ \mu_i v_i \quad (2.9)$$

Puisque C = AA^T, nous pouvons simplifier :

$$C(Av_i) = \mu_i(Av_i) \quad (2.10)$$

De (2.6) et (2.10), nous voyons que Av_iet $\mu_i$sont respectivement les vecteurs propres et les valeurs propres de C :

$$\begin{cases} ei = Av_i \\ \lambda i = \mu_i \end{cases} \quad (2.11)$$

Nous pouvons donc trouver les valeurs propres de cette énorme matrice C en trouvant les valeurs propres d'une matrice L beaucoup plus petite. Pour trouver les vecteurs propres de C, il suffit juste de multiplier les vecteurs propres de L par la matrice A. Les vecteurs propres trouvés sont ensuite ordonnés selon leurs valeurs propres correspondantes, de manière décroissante. Plus une valeur propre est grande, plus la variance capturée par le vecteur propre

Une part de la grande efficacité de l'algorithme PCA vient de l'étape suivante qui consiste à ne sélectionner que les k meilleurs vecteurs propres (ceux avec les k plus grandes valeurs propres). On définit alors un espace vectoriel engendré par ces k vecteurs propres, que l'on appelle *l'espace des visages* E_v (''Face Space'' en anglais).

Les images originales sont projetée dans l'espace des visages pour former une suite de coefficient d'appartenance, ce qui donne por une l'image I_i

$$w_k = e_{k'} \Phi_i \; ; k=1, \cdots, M' \tag{2.12}$$

ces coefficients forment alors un vecteur représentation l'image I_i:

$$\Omega_i^T = [w_1, w_2, w_3, \ldots\ldots, w_{M'}] \tag{2.13}$$

Figure 2.9 - Image moyenne et les eigen faces

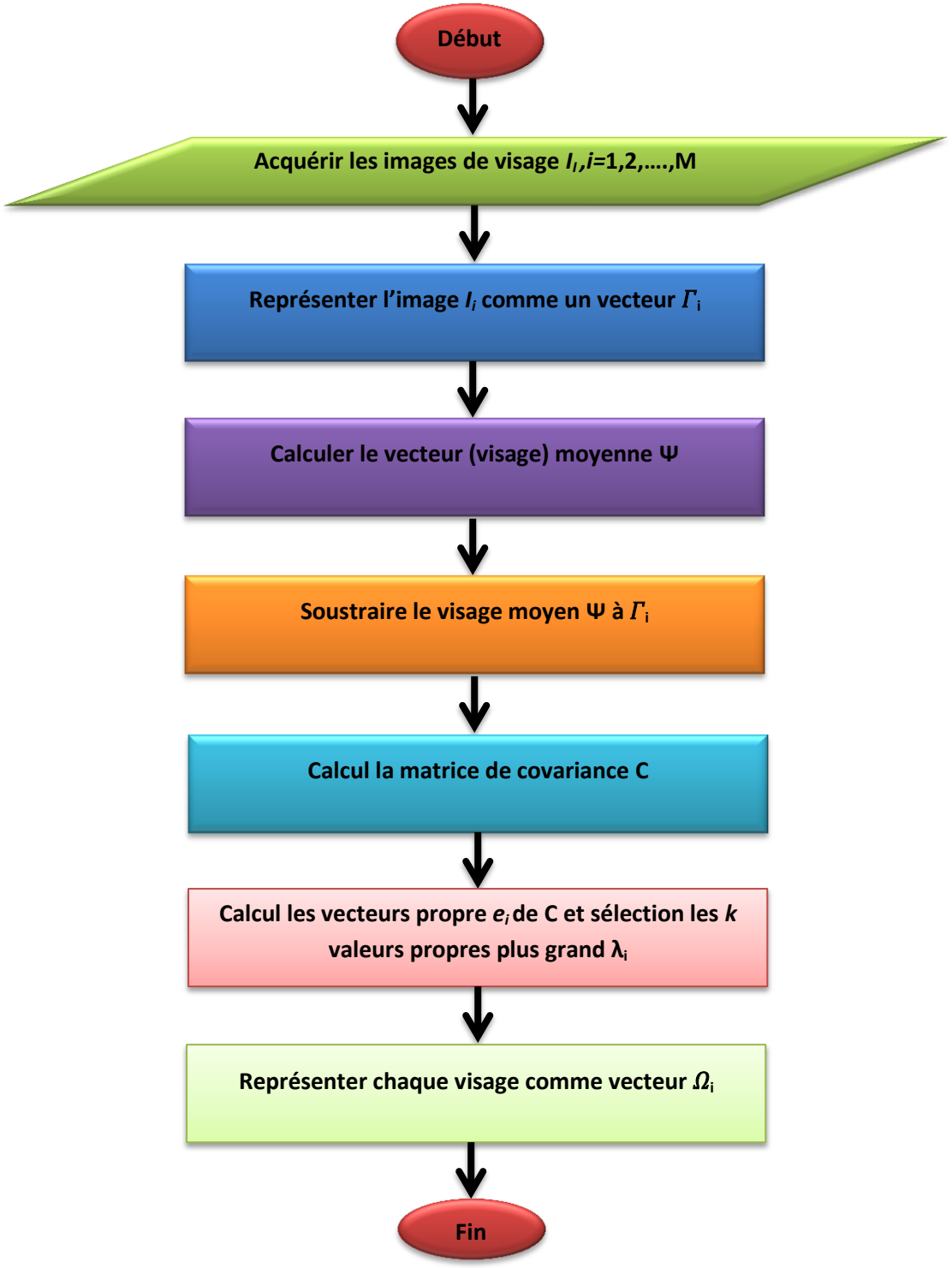


Figure 2.10 - organigramme de la phase d'apprentissage du PCA

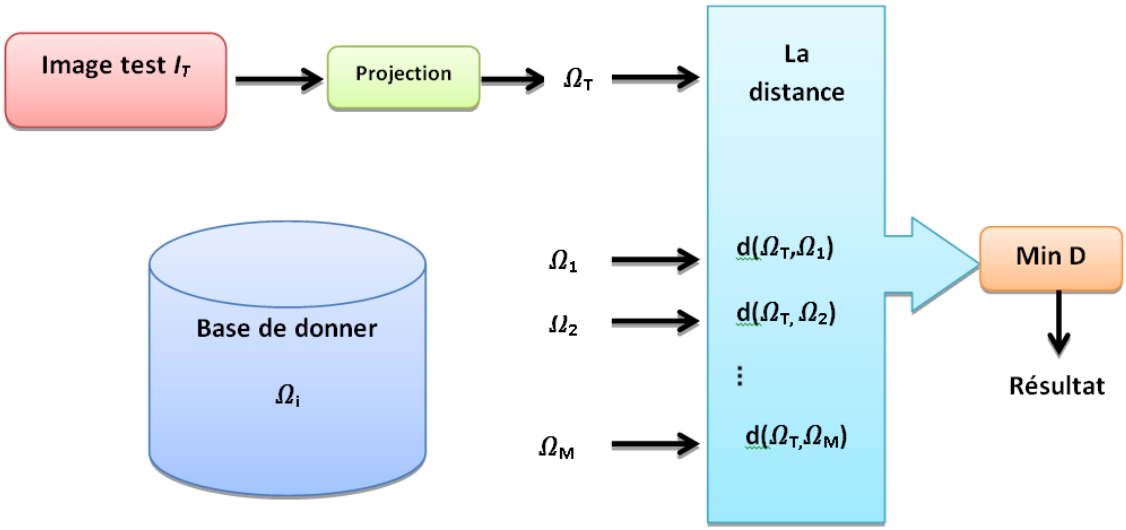


Figure 2.11 - phase de test PCA

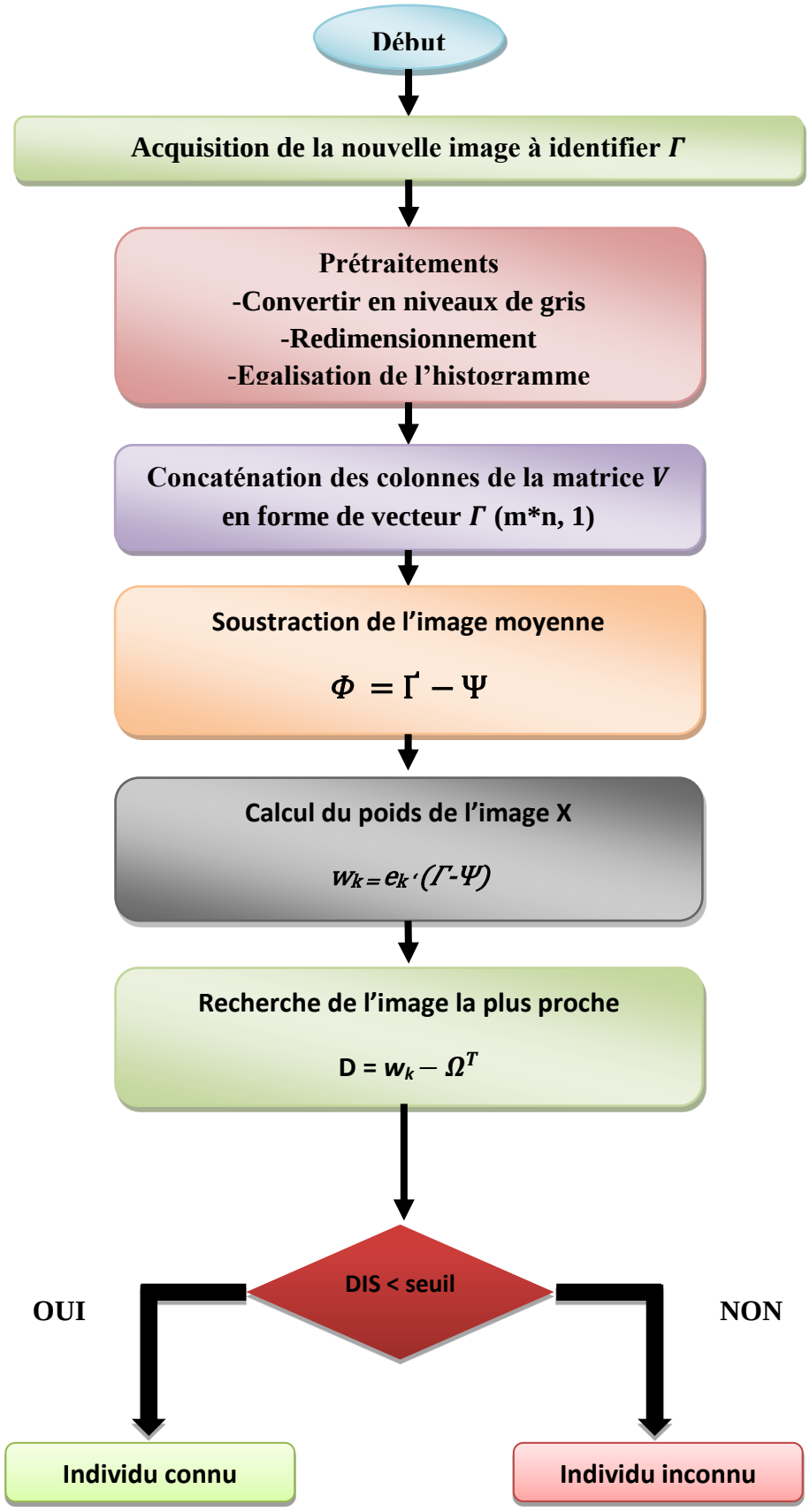


Figure 2.12 - Organigramme de la phase d'identification

2.6.2 Le filtre de Gabor

Un filtre de Gabor est une fonction sinusoïdale à laquelle on a modulée avec une enveloppe gaussienne. Dans le plan fréquentiel cette fonction se transforme en gaussienne. La fonction sinusoïdale est caractérisée par sa fréquence et par son orientation. Ainsi, un filtre de Gabor peut être vu comme un détecteur d'arêtes d'orientation particulière, puisqu'il réagira aux arêtes perpendiculaires à la direction de propagation du sinus. La fréquence du sinus, indique à quelles fréquences le filtre sera sensible et réagira. Il a, de plus, été montré que les fonctions de Gabor forment un ensemble complet, c'est à dire que n'importe quelle fonction peut être exprimée en une somme (infinie) de fonctions de Gabor [20]. Le filtre de base que nous avons utilisé est un filtre de Gabor à symétrie paire et orienté à 45 degrés. Les filtres de Gabor ou filtres **gaussiens** constituent une classe particulière des filtres linéaires ce sont des filtres **orientés**. Ces filtres ont une réponse impulsionnelle de la forme:

$$h(x, y) = g(x', y')e^{2\pi j(Ux+Vy)} \quad (2.14)$$

Où

- $(x', y') = (x \cos \varphi + y \sin \varphi - x \sin \varphi + y \cos \varphi)$, c'est-à-dire les coordonnées (x, y) tournées d'un angle φ, et
- $g(x', y') = \frac{1}{2\pi\sigma^2} e^{(-(x'/\lambda)2+y'2)/2\sigma^2}$.

La réponse impulsionnelle h(x, y) est donc une fonction complexe sinusoïdale modulée par une gaussienne bidimensionnelle de rapport d'axes λ, de facteur de dilatation σ et où φ est l'orientation de l'axe x' par rapport à l'axe x.

2.6.2.1 Résolution et taille du filtre

Pour le filtre de base, mis à part l'orientation, on a 3 degrés de liberté: la taille du filtre, la fréquence fondamentale et les écarts type. Entre la taille du filtre et les écarts type il y a quand même une relation: la taille du filtre doit être suffisamment grande pour que les gaussiennes y tiennent. Dans le cas d'une seule orientation, on trouve que pour une taille 3 fois plus grande que les écarts type, le filtre contient au moins 87% du signal. Si la taille est 4 fois plus grande, le pourcentage est d'au moins 96%. Le fait de couper la gaussienne en

temps est équivalent à convolera la transformée de Fourier de la gaussienne avec un sinus cardinal en fréquence. Si la taille du filtre ne respect pas la taille de la gaussienne, la résolution que nous aurons en fréquence sera celle du sinus cardinal, qui est proportionnel à l'inverse de la taille du filtre. Donc, il ne sert à rien d'essayer d'avoir une bonne résolution en fréquence en utilisant un grand écart type en temps de la gaussienne si après on ne respecte pas la taille [20].

2.7. Mesures de Distance

Lorsqu'on souhaite comparer deux vecteurs de caractéristiques issus du module d'extraction de caractéristiques d'un système biométrique, on peut soit effectuer une mesure de similarité (ressemblance), soit une mesure de distance (divergence).

2.7.1. Distances Euclidiennes

On peut imaginer les variables indépendantes (dans une équation de régression) comme définissant un espace multidimensionnel dans lequel chaque observation peut être tracée. La distance Euclidienne est une distance géométrique dans cet espace multidimensionnel. Celle est calculée comme :

$$\text{Distance}(x,y) = \sqrt{\sum_{i=1}^{n} |x_i - y_i|^2} \qquad (2.15)$$

2.7.2. Distance de Hamming

La distance de Hamming permet de quantifier la différence entre deux séquences de bites. C'est une distance au sens mathématique du terme. À deux suites de bites de même longueur, elle associe le nombre de positions où les deux suites diffèrent.

Le poids de Hamming correspond au nombre d'éléments différents de zéro dans une chaîne d'éléments d'un corps fini.

Soit *A* un alphabet et *F* l'ensemble des suites de longueur *n* à valeur dans *A*. La **distance de Hamming** entre deux éléments *a* et *b* de *F* est le nombre d'éléments de l'ensemble des images de *a* qui diffèrent de celle de *b*.

Formellement, si *d*(.,.) désigne la distance de Hamming :

$$\forall a, b \in F \quad a = (a_i)_{i\in[0,n-1]} \; et \; b = (b_i)_{i\in[0,n-1]} \quad d(a,b) = \#\{i : a_i \neq b_i\}$$

La notation #*E* désigne le cardinal de l'ensemble *E*.

Un cas important dans la pratique est celui des symboles binaires. Autrement dit *A*= {0,1}, On peut alors écrire, si $\oplus$ désigne le ou exclusif.

$$d(a,b) = \sum_{i=0}^{n-1} (a_i \oplus b_i) \tag{2.16}$$

2.8. Conclusion

Dans ce chapitre, nous avons donné la définition et l'architecture des systèmes multimodaux, présenté les différents types et niveaux de fusion, Analyse en composantes principales et nous avons donné un aperçu sur les ondelettes du Gabor.

Chapitre 3

Résultats et discussions

3.1 Introduction

Afin de mesurer les performances d'un système de reconnaissance de **FKP**, les scientifiques ont établi un certain nombre de règles communes permettant de disposer les mêmes critères d'évaluation. Ces critères s'appliquent sur des bases de données également communes et partagées par l'ensemble de la communauté scientifique. Une base de données regroupe plusieurs images de plusieurs personnes.

Ce chapitre représente les résultats de tests effectués avec les algorithmes « PCA » et « Gabor » sur la base de données citée ci-dessous. Rappelons que notre travail consiste à concevoir un système d'identification biométrique de personnes par reconnaissance FKP se basant sur PCA et Gabor qui peuvent être utilisées pour simplifier un ensemble de données, en réduisant sa dimension. on a choisi la fusion du score du « PCA et Gabor » pour améliorer les performances du système qui dépendent (résultats et robustesse, un temps de latence acceptable pour des applications « temps réel »). Nous évaluerons dans ce chapitre les résultats obtenus sur notre base de données.

Notre travail, dans ce cas, se concentre sur la **fusion des scores** qui est le type de fusion le plus utilisé. Elle peut être appliquée à tous les types de systèmes.

3.2 Système de reconnaissance de FKP

Le problème de la reconnaissance de FKP est défini comme suit : étant donné une image de FKP dont on souhaite déterminer l'identité de la personne correspondante. Pour ce faire, il est nécessaire d'avoir des images de référence, sous la forme d'une base de données de

FKP de toutes les personnes connues par le système. A chaque image est associé un vecteur de caractéristiques, ces caractéristiques sont supposées être invariantes pour une même personne, et différentes d'une personne à l'autre. La reconnaissance consiste alors à comparer le vecteur de caractéristiques du FKP à reconnaitre avec celui de chacun des FKP de la base.

Ceci permet de retrouver la personne ayant le FKP le plus ressemblant, qui est celui dont le vecteur est le plus similaire

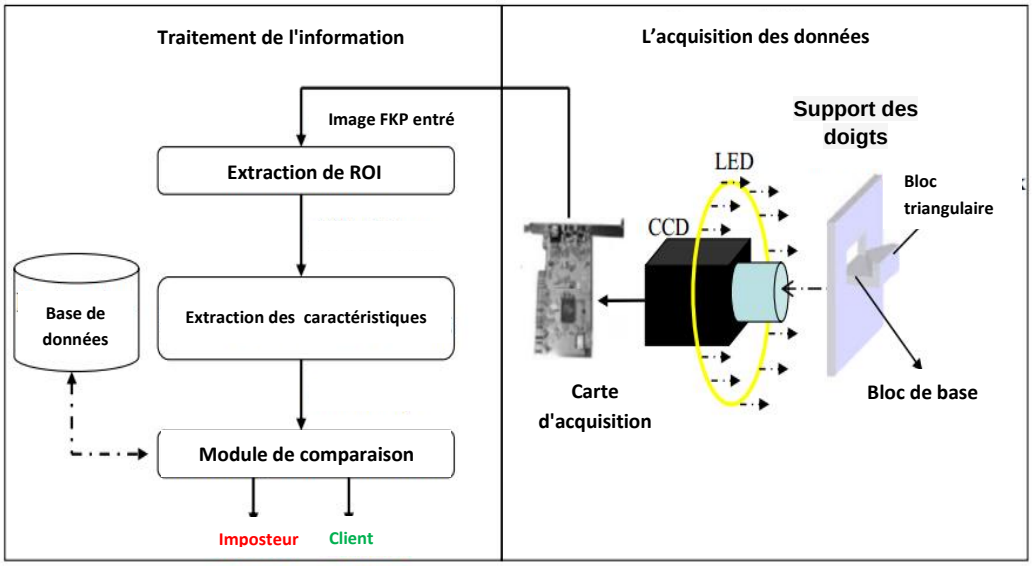


Figure 3.1 Structure du système d'identification personnelle à base du FKP proposé. [21].

Le schéma de principe de notre système d'identification personnelle à base du FKP est montré dans la Figure **3.1**. Le système est composé d'un module d'acquisition de données et un module de traitement de données. Le module d'acquisition de données est composé d'un support de doigt, un anneau LED source de lumière, une lentille, une caméra CCD et une carte d'acquisition. L'image FKP capturée est entrée dans le module de traitement de données qui comprend trois étapes de base: ROI, extraction des caractéristiques, et l'appariement ''maching''. Figure **3.2** montre le dispositif d'acquisition d'image FKP dont la taille globale est 160mm × 125mm × 100mm.

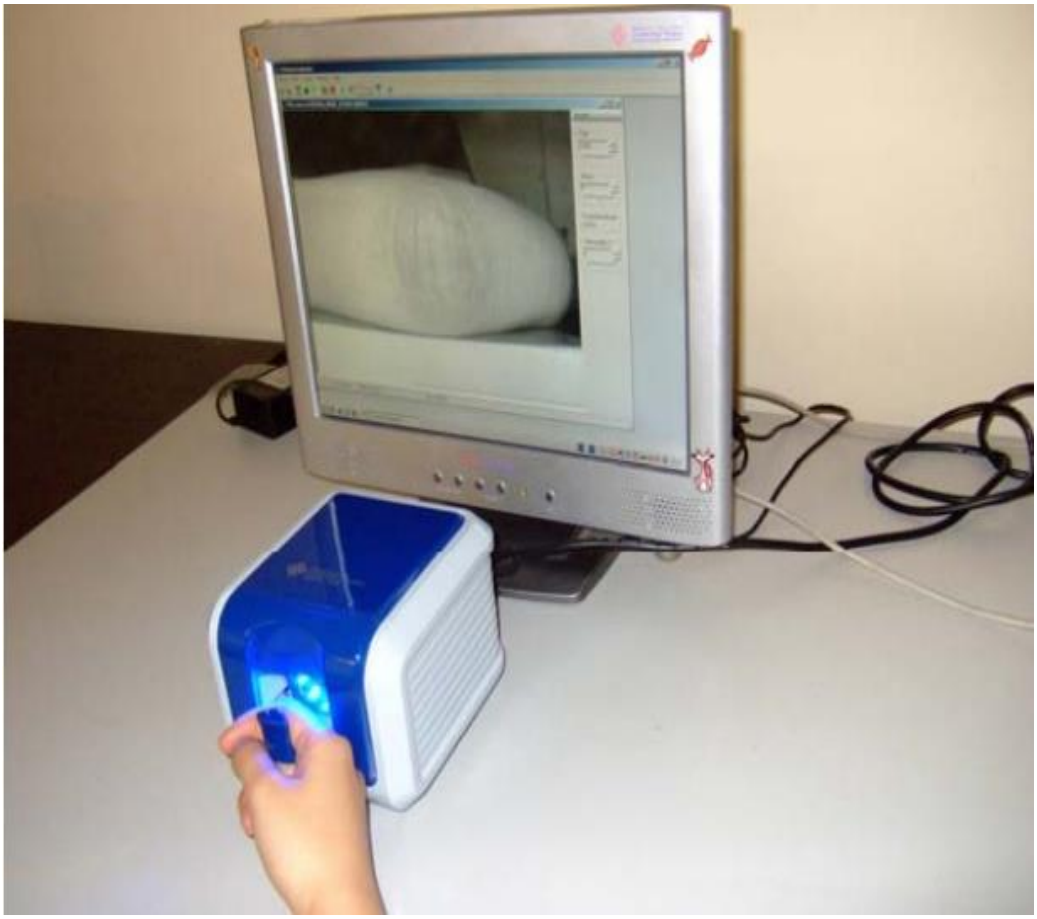


Figure 3.2 L'appareil d'acquisition d'image FKP[21].

3.2.1 La Base de données FKP

Afin d'évaluer le système d'identification des personnes proposé de base-FKP, une base de données FKP a été créé en utilisant le système d'acquisition d'image du FKP .Cette base de données est destinée à être un point de référence pour évaluer la performance de diverses méthodes de reconnaissance FKP, et il est désormais accessible au public. Le FKP images ont été recueillies à partir de 165 volontaires, dont 125 hommes et 40 femmes Entre eux, 143 personnes ont 20 ~ 30 ans et les autres sont 30 ~ 50 ans. Les bénévoles étaient des étudiants et des enseignants de l'Université polytechnique de Hong Kong et à Harbin Institute of Technology **(PolyU)**.

Nous avons recueilli les échantillons en deux sessions distinctes. Dans chaque session, le sujet était demandé de fournir 12 images pour chacun des doigts l'index et le milieu gauche, l'index et le milieu droit. Par conséquent, 48 images de quatre doigts étaient

recueillies auprès de chaque sujet. Au total, la base de données contient 7920 images de 660 doigts différents.

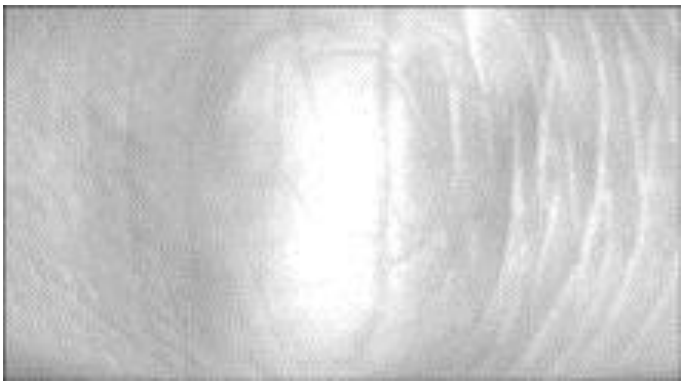


Figure 3.3 - Exemple de la région d'intérêt.

3.2.1.1 Séparation des bases de données

Afin de développer une application de reconnaissance de FKP, il est nécessaire de disposer de deux bases de données : une base pour effectuer **l'enrôlement** et une autre pour **tester** les techniques et déterminer leurs performances, mais Il n'y a pas de règles pour déterminer ce partage de manière quantitatif. Il résulte souvent d'un compromis tenant compte du nombre de données dont on dispose et du temps pour effectuer l'apprentissage. Dans les séries de test que nous avons effectués la base a été scindée de la façon suivante :

• **Images Enrôlement:** La première, la cinquième et la neuvième image de chaque personne servent pour la phase d'apprentissage.

• **Images Tests :** Les 9 images restantes de chaque individu nous ont servi pour la réalisation des différents tests.

Le but est d'évaluer le taux de reconnaissance de différents algorithmes présentés, en suivant un protocole de test basé sur la mesure du taux de reconnaissance

$$\text{Taux de reconnaissance} = \frac{\text{Nombre d'images de test reconnues}}{\text{Nombre totale d'images de test}} \qquad (3.1)$$

3.3. Principe de la fusion de scores

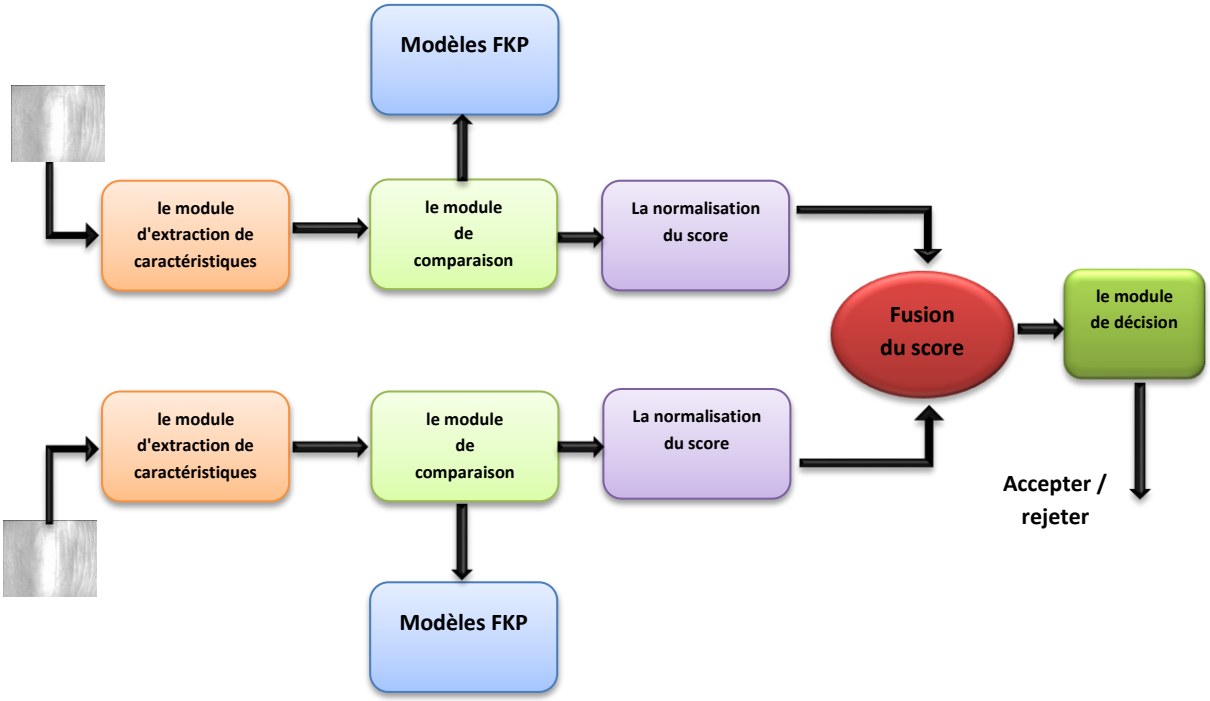


Figure 3.4 - Schéma de la fusion de scores.

La fusion de scores consiste donc à la classification : **OUI** ou **NON** pour la décision finale, d'un vecteur de nombres réels. Il existe deux approches pour fusionner les scores obtenus par différents classifieurs :

1- Approche par combinaison de scores
2- Approche par classification de scores.

Nous étudions un multi systèmes de vérification **FKP** par la première approche **Combinaison de scores** par la **méthode simple** de **la somme, min, max**. La normalisation qui est utilisée est la normalisation par la méthode **Min-Max,**

3.4 Fonctionnement du système

Notre système permet d'illustrer le processus d'identification. Il comporte deux phases : la phase d'apprentissage pendant laquelle les modèles sont construits et la phase d'identification (phase de comparaison). Nous allons décrire dans ce qui suit Phase reconnaissance.

3.4.1. Phase reconnaissance

A cette étape premièrement se fait l'extraction de vecteur de caractéristique de l'image test puis se fait le calcule de la distance entre ce vecteur avec les 495 vecteurs de la phase d'apprentissage, il va afficher l'identité de la personne qui correspond au vecteur qui a la distance minimale avec le vecteur de l'image test.

3.5. Expérimentations sur la FKP

3.5.1 Protocole de test

Des exemples d'images pour chaque personne ont été recueillis en deux sessions. Dans nos expériences, nous avons pris des images collectées dans la première session comme l'ensemble de l'apprentissage et des images recueillies lors de la deuxième session, comme l'ensemble de test. Par conséquent, il y avait (165 × 4=660) classes et (660 × 3=1980) images dans l'apprentissage. Pour obtenir des résultats statistiques, chaque image de l'ensemble test a été jumelé à toutes les images dans l'ensemble d'apprentissage. Si les deux images sont de la même classe, la mise en correspondance entre d'eux a été comptée comme un véritable appariement; sinon il a été considéré comme une adaptation d'imposteur.

Le taux d'égalité d'erreur (EER), est utilisé pour évaluer la précision de vérification. Par ailleurs, la courbe caractéristique (ROC), qui est un terrain de FRR contre FAR pour tous les seuils possibles, obtenus par l'utilisation de chaque méthode de codage évalué seront fournis.

Pour évaluer la performance de notre système**,** on procède aux expérimentations suivantes :

Les tests sur la base FKP ont été réalisés en trois expérimentations :

1- Première expérimentation : dans un premier temps, nous avons mis en œuvre un Système de reconnaissance multi algorithmes sur la modalité FKP. Nous avons étudié les résultats obtenues issues par les algorithmes **PCA** et du filtre de **Gabor**.

2- Deuxième expérimentation : on va faire la fusion au niveau des scores des algorithmes PCA et Gabor de chaque doigt parmi les quatre. Et on compare les résultats obtenus par la fusion : L'Index gauche avec L'Index droit et Milieu gauche avec Milieu droit.

3- Troisième expérimentation : la fusion des scores de L'Index gauche avec le Milieu gauche et L'Index droit avec Milieu droit conçus par les fusions obtenus dans l'étape précédente. Et on compare les résultats de fusion des scores entre L'Index gauche et le Milieu gauche par L'Index et le Milieu droit.

4- Quatrième expérimentation : dans cette dernière expérimentation on va fusionner les résultats obtenu dans l'expérimentation numéro trois (la fusion au niveau des scores des algorithmes PCA et Gabor pour chaque doigt puis on fusionne tous ces résultats), Et on compare ces résultats avec celle de l'expérimentation numéro trois. Aussi dans cette étape on va tester **trois méthodes de combinaison de scores somme, min et max.**

3.5.2 Résultats expérimental et interprétations.

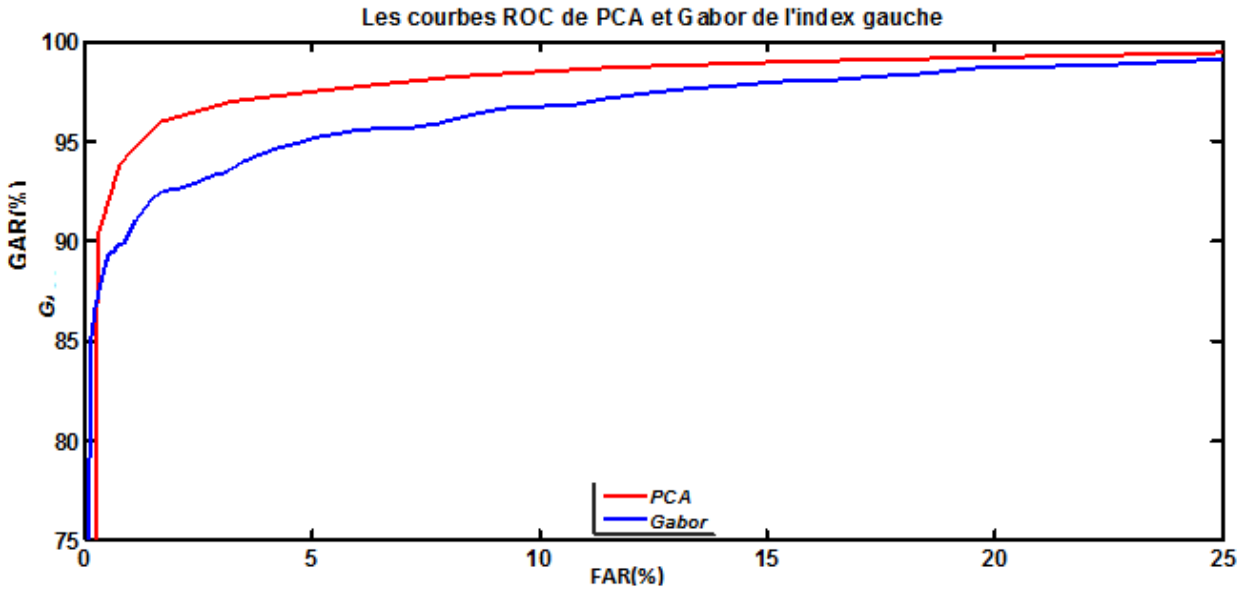
1- les résultats obtenus par PCA et Gabor

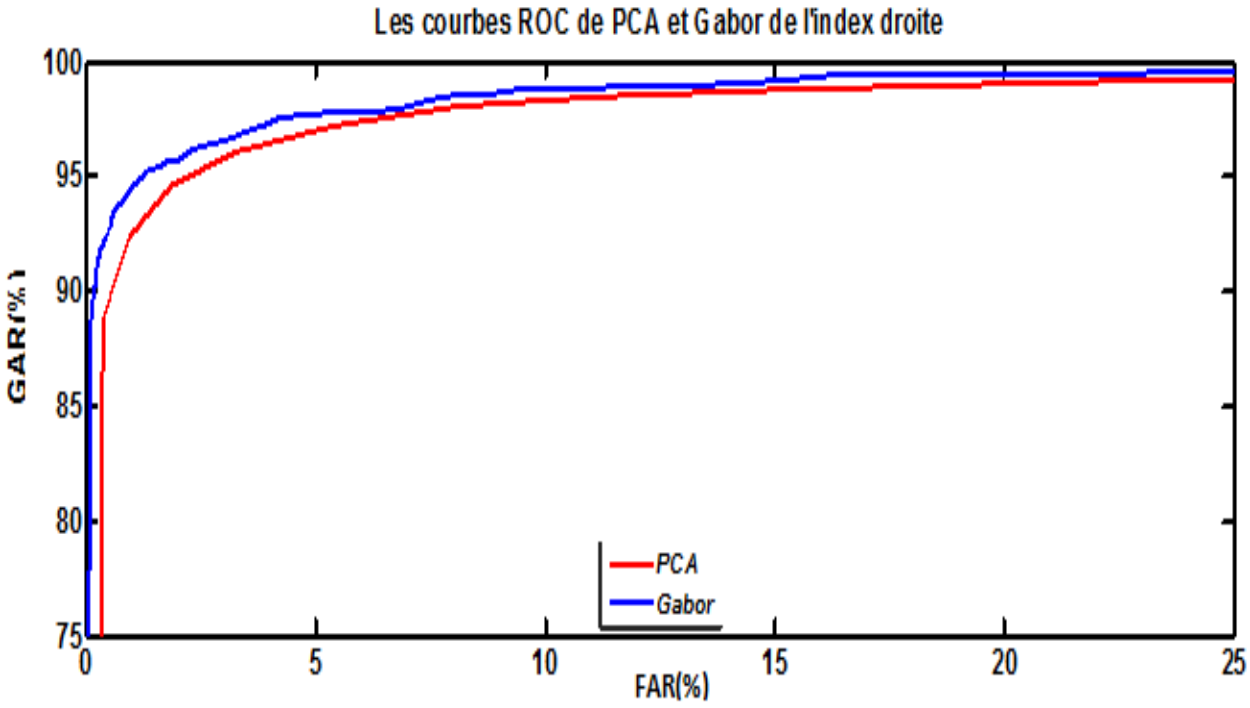
A la fin de l'exécution des deux algorithmes d'évaluation, on à réaliser le tableau ci-après dessous qui contient les résultats obtenus et les taux FAR et FRR puis, nous avons tracé les courbes FAR vs FRR, ROC, DET. Les résultats sont représentés sur les courbes de la Figure **3.5**

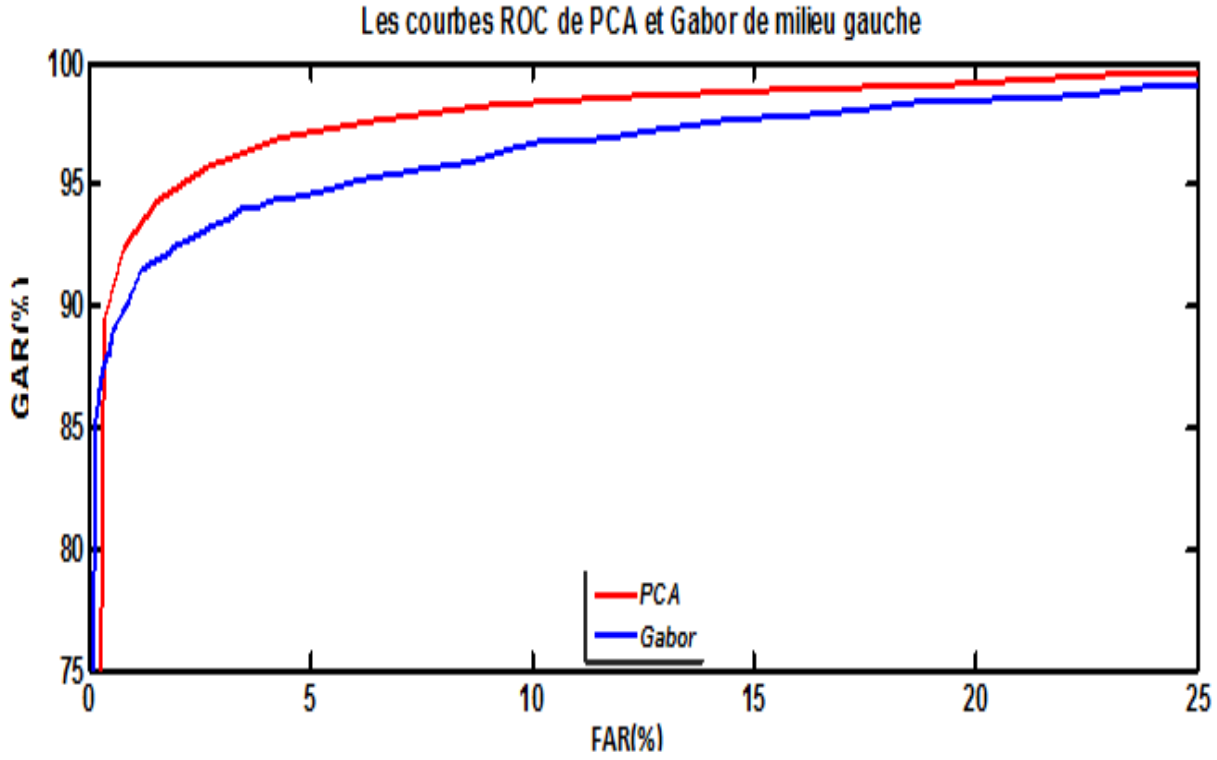
Tableau 3.1 - les résultats obtenu par les deux algorithmes séparés

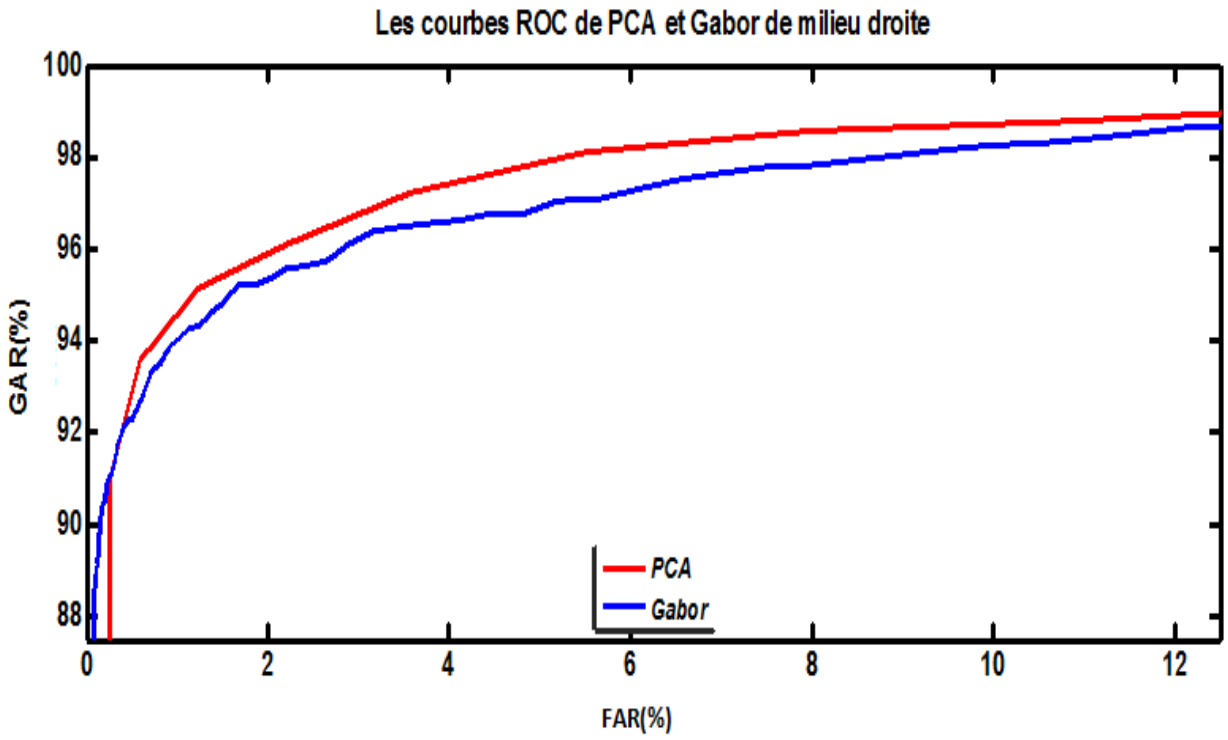
	Les doigts	EER(%)	Seuil
PCA	l'index gauche	3.1093	0.0393
	Milieu gauche	3.3706	0.0446
	l'index droit	3.6704	0.0419
	Milieu droit	3.1074	0.0468
Gabor	l'index gauche	4.9060	0.2957
	Milieu gauche	5.1974	0.2947
	l'index droit	3.2555	0.3216
	Milieu droit	3.5017	0.3311

De ce tableau, on remarque que le PCA nous a donné de bons résultats avec le milieu droit contrairement au Gabor qui fonctionne bien avec l'index droit

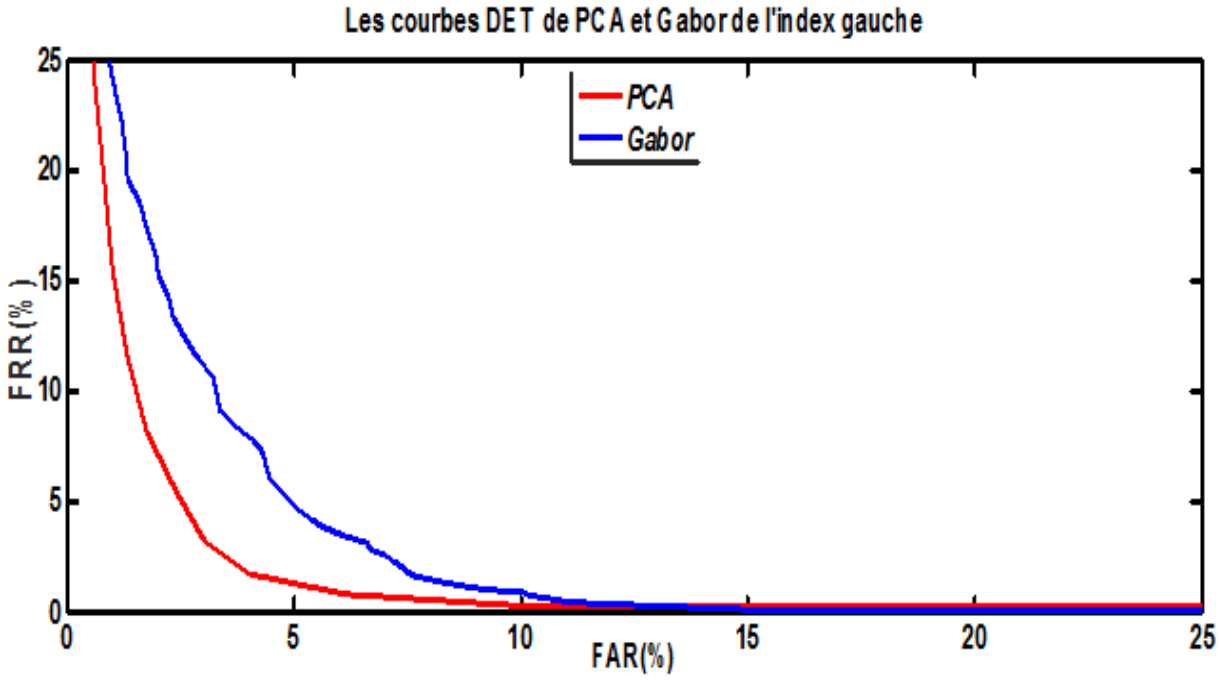


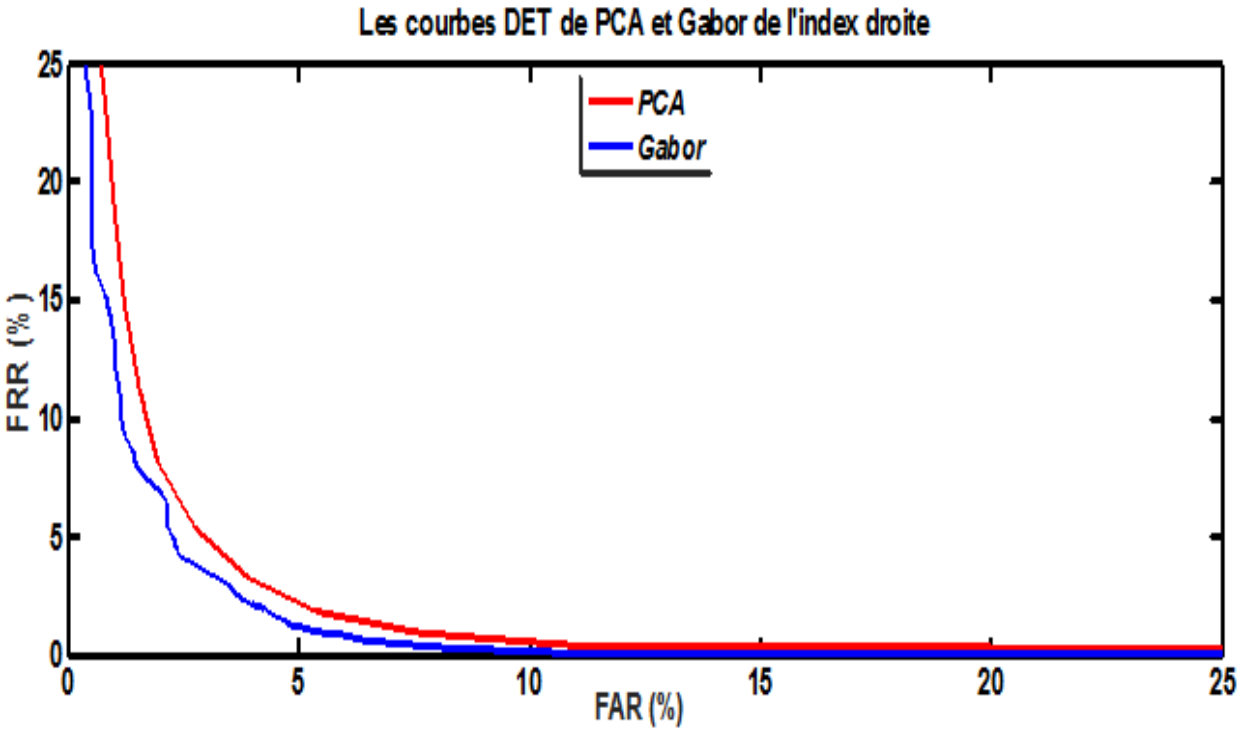

Les courbes ROC de PCA et Gabor de l'index droite
GAR(%)
FAR(%)
PCA
Gabor
100
95
90
85
80
75
0
5
10
15
20
25

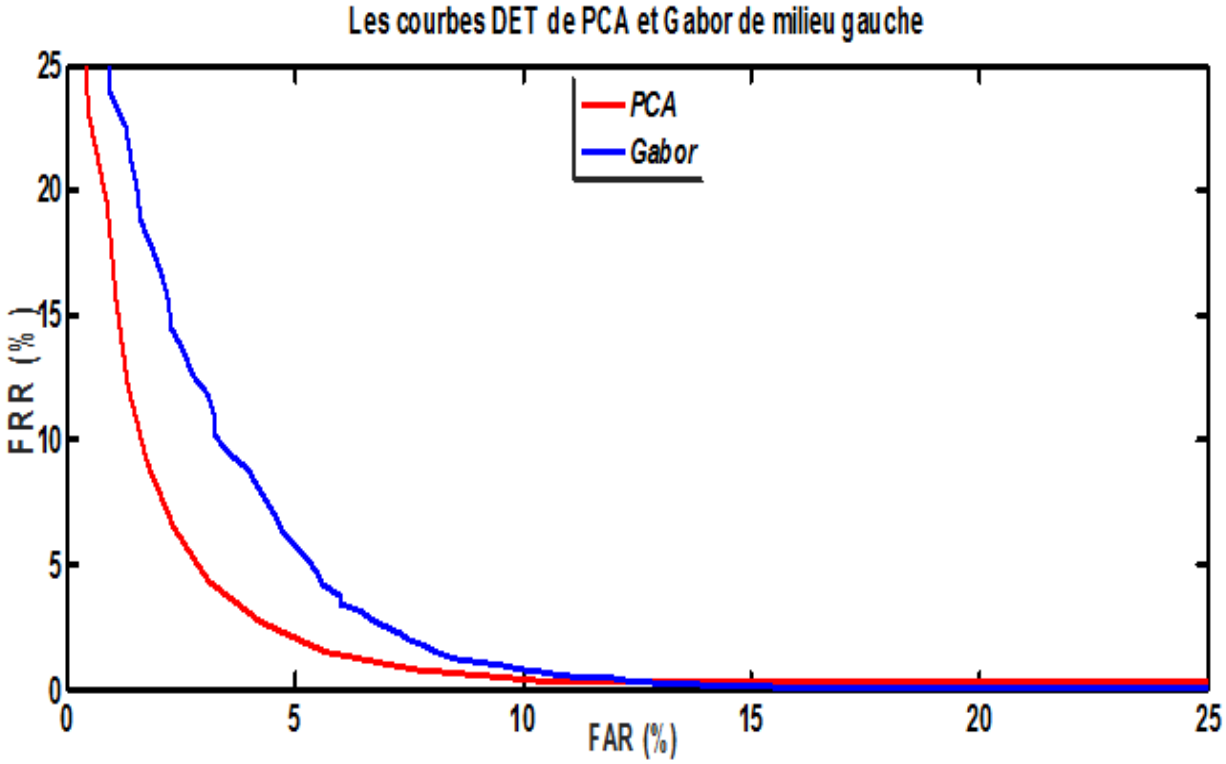

Les courbes ROC de PCA et Gabor de milieu gauche
GAR(%)
FAR(%)
PCA
Gabor
100
95
90
85
80
75
0
5
10
15
20
25

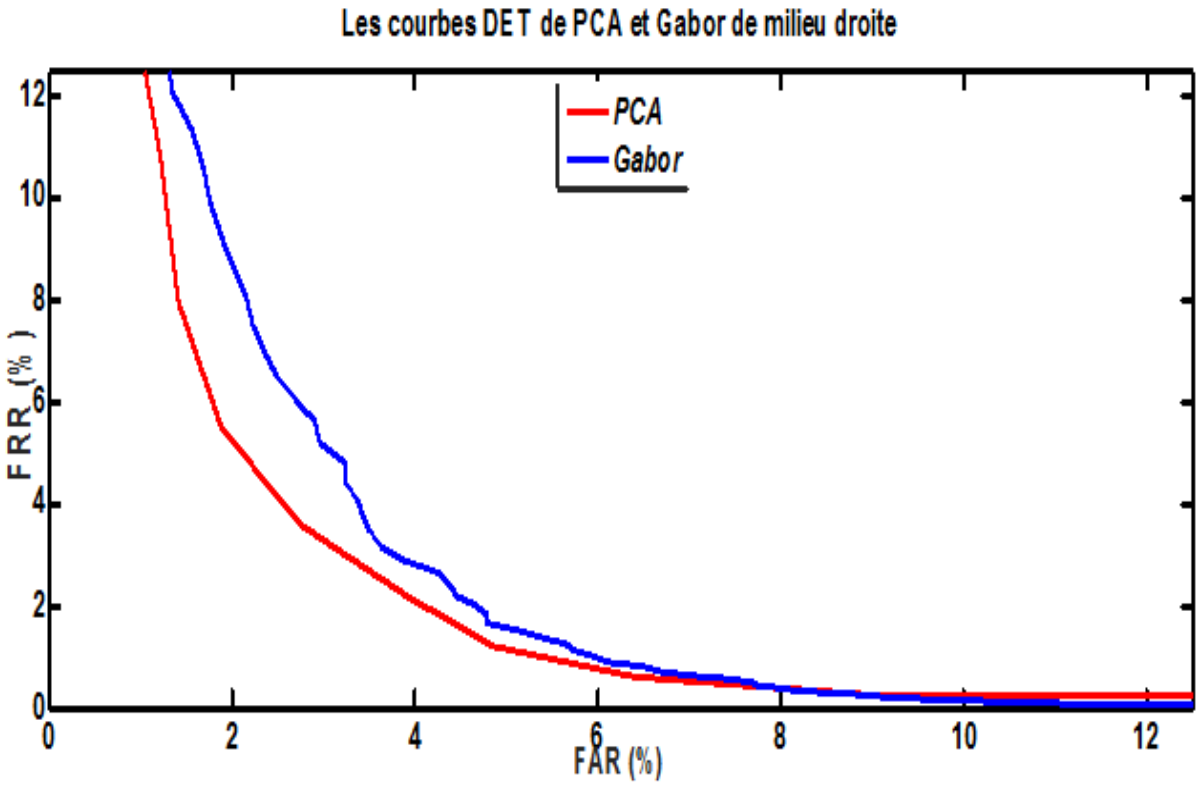


(a) La courbe ROC (GAR Vs FAR)




Les courbes DET de PCA et Gabor de l'index droite
PCA
Gabor
FRR (%)
FAR (%)
0
5
10
15
20
25


Les courbes DET de PCA et Gabor de milieu gauche
PCA
Gabor
FRR (%)
FAR (%)
0
5
10
15
20
25



(b) La courbe DET (FAR Vs FRR)

Figure 3.5 - Courbes obtenues par l'algorithme d'évaluation

A partir des courbes ROC (Figure **3.5** (a)), nous pouvons déduire que l'efficacité des systèmes en utilisant le PCA est mieux par rapport à celle qui utilise le Gabor sauf le système appartient à l'index droit.

Et enfin, la courbe DET (Figure **3.5** (b)) nous fournit un EER de 3 a 5, l'erreur minimal est de milieu droit d'une valeur (3.1074%) avec un seuil de (0.0468%).

2- Fusion : PCA et Gabor

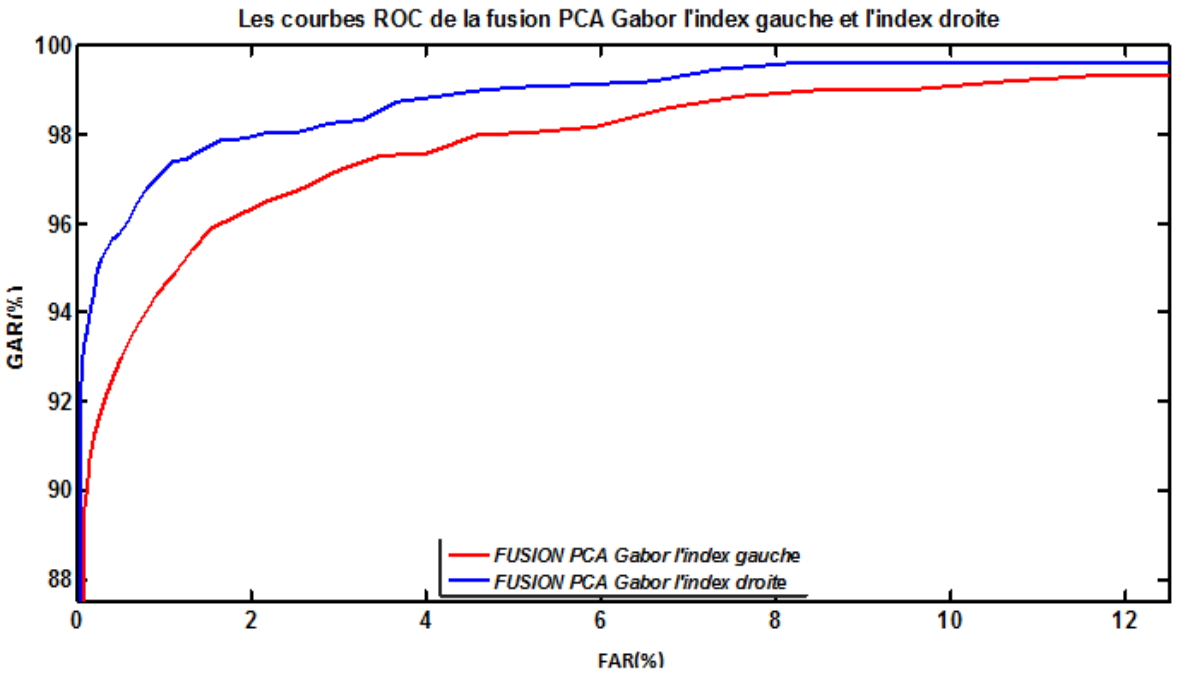
Dans cette deuxième expérimentation, nous avons fusionné le vecteur de score du doigt d'index gauche qu'on a obtenu après d'exécution de l'algorithme PCA avec le vecteur de score du doigt d'index droit qu'on a obtenu après d'exécution de l'algorithme Gabor. On procède de même façon pour les autres doigts.

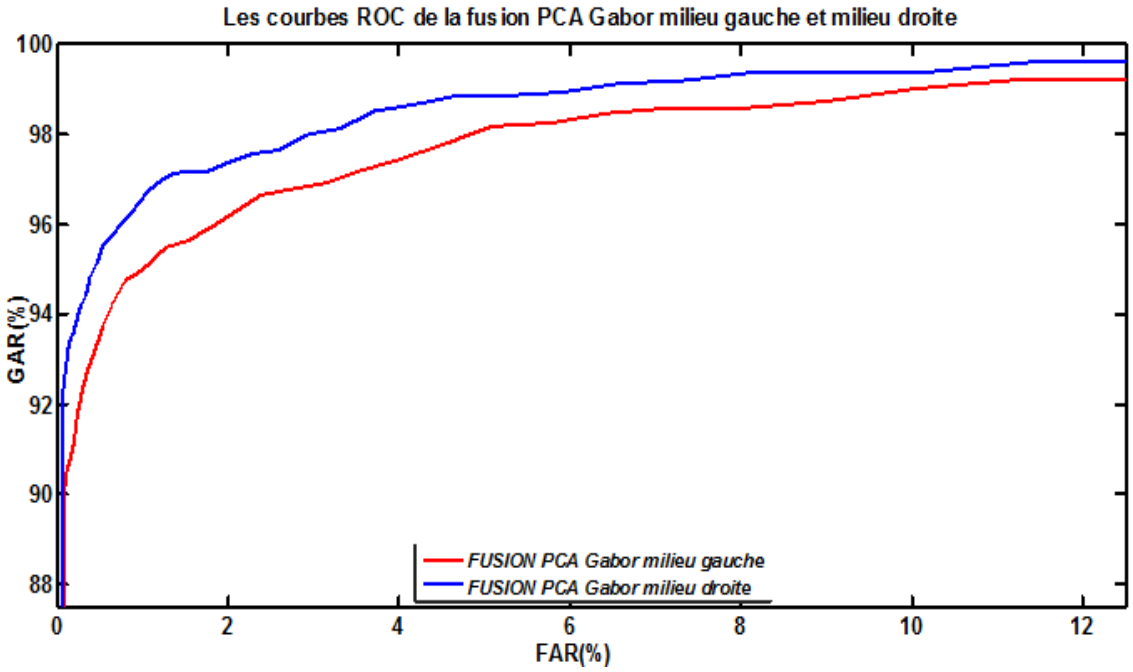
Les scores pour chaque système sont calculés puis soumis à la normalisation des scores. Cette dernière représente une étape très importante. nous avons utilisé la normalisation Min_Max et approche de somme pour la combinaison des scores .

Tableau 3.2 - les résultats obtenu par la fusion des deux algorithmes

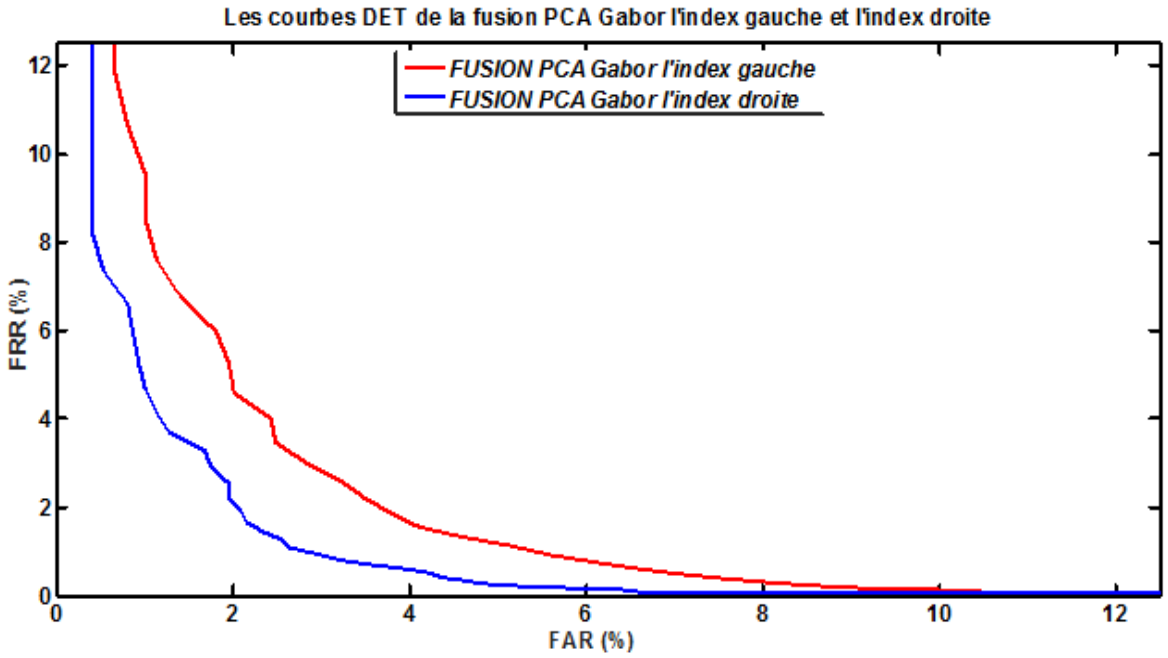
	Les doigts	EER(%)	Seuil
PCA et Gabor	l'index gauche PCA-Gabor	2.9109	0.1780
	Milieu gauche PCA-Gabor	3.1067	0.1993
	l'index droit PCA-Gabor	2.0348	0.2139
	Milieu droit PCA-Gabor	2.4006	0.2235

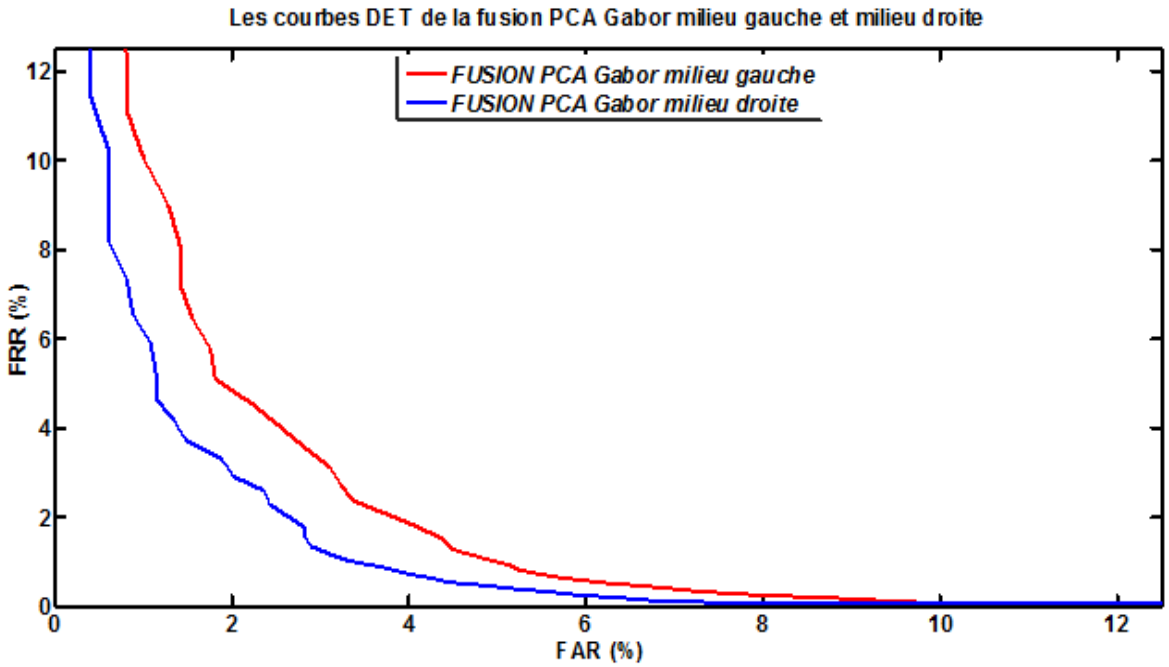
Dans ce tableau on remarque une amélioration aux résultats obtenus par rapport aux résultats de l'étape précédente la diminution des taux d'égalité d'erreurs EER est sur tous les doigts on remarque que l'index droit contient le meilleur résultat.





(a)Les courbes ROC (GAR Vs FRR)





(b) La courbe DET (FAR Vs FRR)

Figure 3.6 - Courbes obtenues après la fusion algorithmique

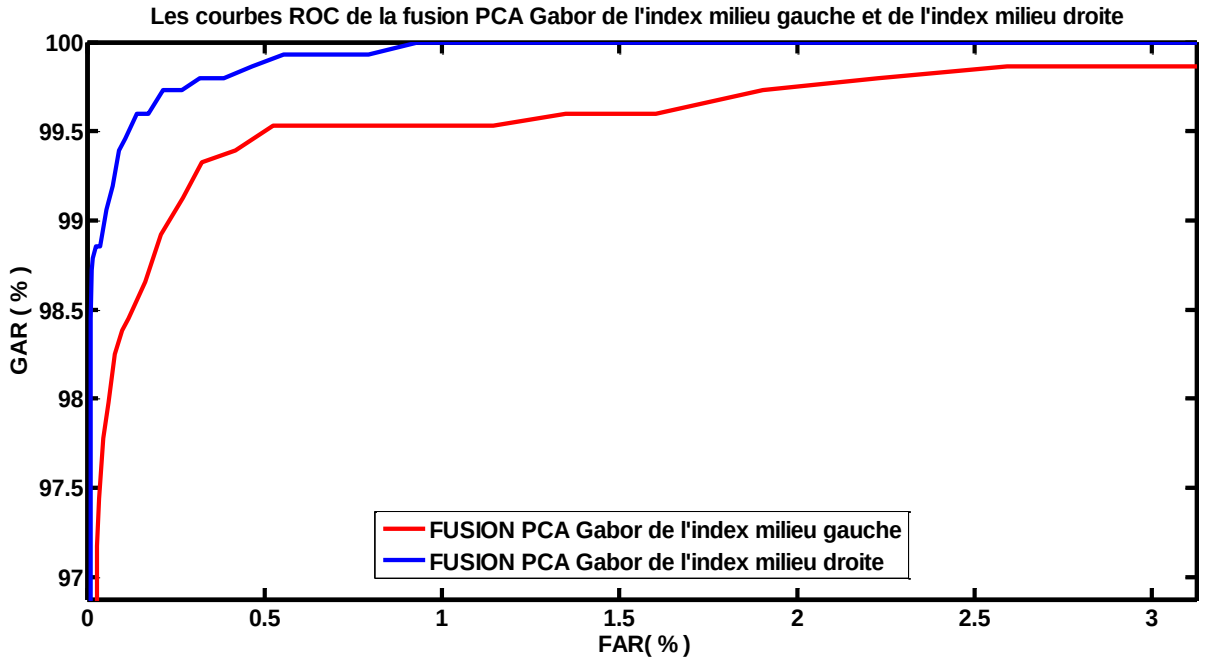
A partir des courbe ROC nous pouvons déduire l'augmentation de l'efficacité du système, d'autre part les courbes DET, nous montre que l'utilisation de fusion des deux méthodes d'une même modalité est mieux par rapport à l'utilisant d'une seul.

3- Dans cette 3ème expérimentation : nous avons fusionné le vecteur de score du doigt d'index gauche (PCA+Gabor) qu'on a obtenu dans la deuxième expérimentation avec le vecteur score du doigt Milieu gauche pour la main gauche, On procède de la même façon pour la main droite.

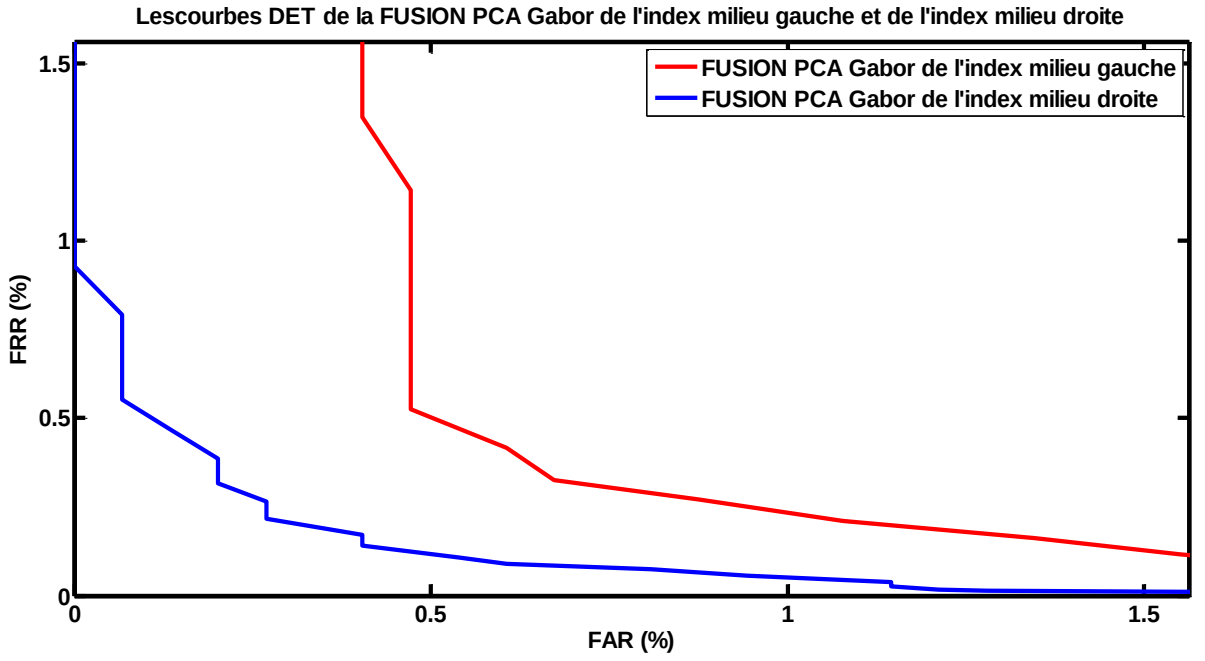
Tableau 3.3 - les résultats obtenu par la fusion des doigts de chaque main

	Les doigts	EER(%)	Seuil
PCA et Gabor	l'index gauche avec Milieu gauche	0.5158	0.1334
	l'index droit avec Milieu droit	0.2675	0.1301

A partir de ce tableau, on remarque la diminution de L'EER après la fusion des doigts et que l'index et le milieu droit ont le meilleur EER d'une valeur de 0.2675 avec un seuil de 0.1301, ces résultats présentent presque la moitié des valeurs obtenus par l'index et le milieu gauche.



(a) La courbe ROC (GAR Vs FAR)



(b) La courbe DET (FAR Vs FRR)

Figure 3.7 - Courbes obtenues après la fusion de l'index avec le milieu de chaque main

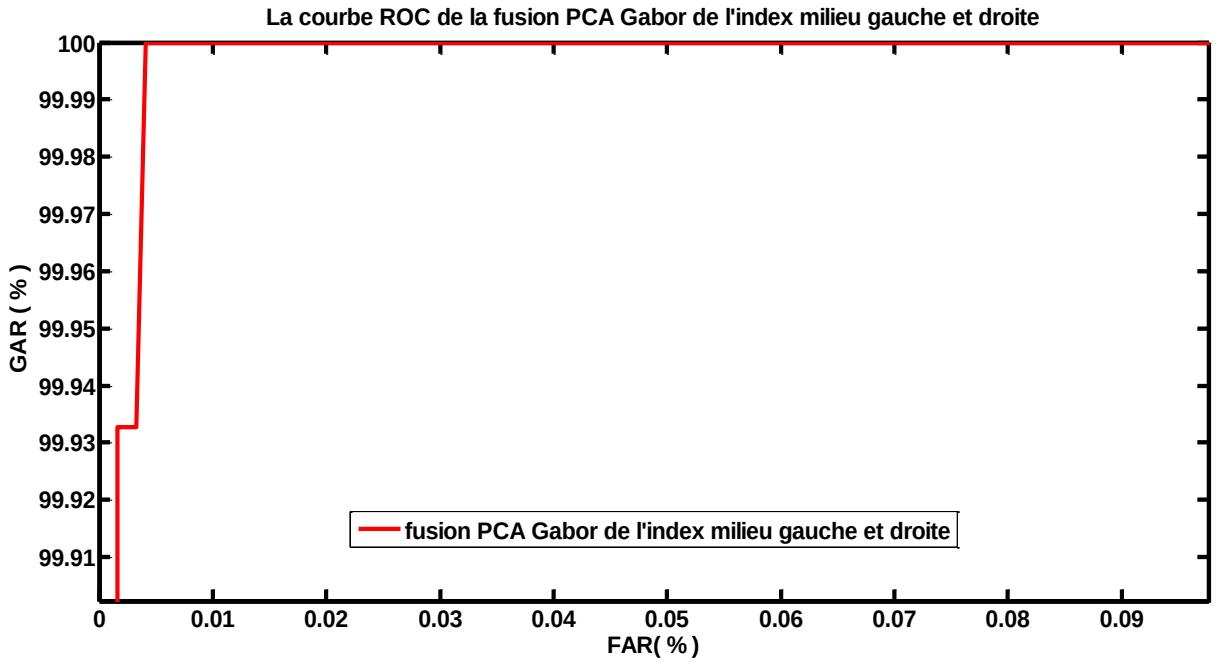
De la courbe ROC (Figure **3.7** (a)), nous pouvons déduire que la fusion du score des doigts de la main droite (l'index avec Milieu) donne de meilleurs résultats que les doigts de la main gauche (l'index avec Milieu) et ces deux résultats sont mieux par rapport à celui des expérimentations **1** et **2**

De la courbe DET (Figure **3.9** (b)), nous pouvons déduire que l'amélioration de l'efficacité du système. Naturellement, si nous choisissons le seuil de meilleur L'EER, notre système d'identification opère avec une marge d'erreur très limitée.

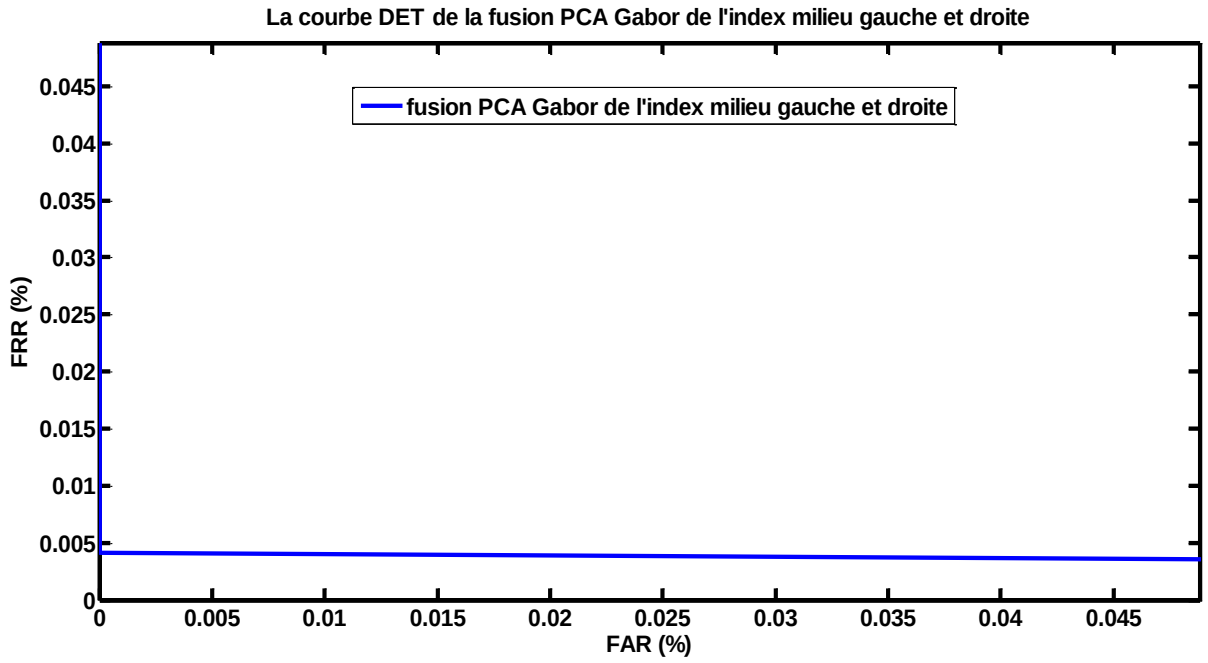
4- Dans cette 4ème expérimentation : nous cherchons de réduire encore les erreurs obtenus. Donc, nous avons fusionné tous les vecteurs score des quatre doigts (PCA+Gabor) qu'on a obtenu. Donc la deuxième expérimentation et testons **trois méthodes de combinaison de score**s pour choisir la meilleur. Les résultats sont cités si dessous.

Tableau 3.4 – Résultats fusion PCA et Gabor l'index gauche et Milieu gauche avec L'index droit et Milieu droit par les quatre méthodes de combinaison de scores

méthodes	EER (%)	Seuil
Somme	**0.004056**	**0.0394**
Max	0.8133	0.2992
Min	1.2136	9.8828×10^{-3}



(a) La courbe ROC



(b)La courbe DET

Figure 3.8 - Courbes obtenues après la fusion de tous les doigts

D'après le Tableau **3.8,** nous constatons que le meilleur résultat de EER est obtenu pour la **méthode simple** du somme de combinaison de score. Il est nettement mieux que les résultats donné, par les autres méthodes.

Sur l'ensemble d'évaluation (Figure **3.8**), nous avons les mêmes remarques que celle obtenues dans les expériences **3** et **2**. On constate que le "système Fusion" est toujours plus performant en comparant avec les systèmes basés sur une seule information dans le meilleur des cas, une EER de (3.1074%). Ces améliorations sont aussi constatées sur tous les points de fonctionnement du système, données par les courbes DETs, on peut remarquer que la courbe DET associée au "système Fusion expérience 4" est la plus proche de l'origine parmi les 4 courbes.

En général, chaque foi on augmente le degré de fusion on obtient un système plus performent et plus robuste.

3.6 Discussion

D'après ces résultats que le système d'identification par FKP est un système fiable. Il permet une bonne séparabilité des classes clients et imposteurs. Nous considérons les résultats obtenus comme satisfaisants. De plus, nous avons étudié l'influence de fusion algorithmique (**PCA+Gabor**) qui nous a donné de bons résultats par rapport au système qui utilise une seule méthode. L'ensemble des tests effectués a permis de conclure, qu'avec l'utilisation de la fusion algorithmique plus la fusion des échantillons (quatre doigts) nous avons apporté une amélioration considérable au taux d'identification grâce à ces fusions, ces résultats induit l'augmentation des performances du système, toute fois le temps de calcul s'est vu légèrement augmenté.

3.7 Conclusion

Dans ce chapitre, nous avons déterminé notre système d'identification biométrique par FKP qui est fondé sur trois modules : un module d'extraction des caractéristiques qui permet de représenter les FKP sous forme de descripteurs de formes de vecteurs caractéristiques, et un module de classification qui permet d'attribuer une classe à la personne que nous venons d'identifier ,avec prises de décision à la fin soit en acceptant la personne, soit en la rejetant en se basant sur un seuil. Nous avons, ensuite, détaillé le fonctionnement du système afin de décrire l'approche de fusion utilisé, visant l'optimisation des deux taux d'erreur FAR et FRR ainsi que le temps d'exécution. Notre méthodologie concernant la fusion du PCA avec le Gabor a permis de rendre l'algorithme plus robuste et a minimisé les deux taux d'erreur FAR

et FRR, et obtenir un seuil presque optimal pour accepter ou rejeter une personne. L'ensemble des tests effectués a permis de conclure, qu'avec l'utilisation de fusion scores PCA_Gabor plus la fusion des échantillons on obtient une amélioration considérable des performances du système.

Conclusion générale

De nos jours, la biométrie est considérée comme le moyen le plus sûr pour la sécurité. Elle est de plus en plus appliquée dans la réalité grâce à ses avantages. Ses application sont divers: applications de contrôle d'accès, applications dans les téléphone portables, application dans l'e-commerce etc...

Dans cet étude on a présenté une vue générale de la biométrie, un survol sur quelques techniques biométriques et on a présenté l'architecture et les modules d'un système biométrique. Nous avons donné aussi un aperçu sur les niveaux de fusion et les techniques de mesure.

Notre travail consiste à la mise au point d'un algorithme robuste destiné à reconnaître un individu par son FKP en utilisant deux méthodes parmi les méthodes les plus utilisées dans ce domaine la premier est l'analyse en composante principale(ACP). L'ACP est une méthode mathématique qui peut être utilisée pour simplifier un ensemble de données, en réduisant sa dimension. Elle est utilisée pour représenter efficacement les images de FKP, qui peuvent être approximativement reconstruites à partir d'un petit ensemble de poids et d'une image de FKP standard. La seconde technique utilisée est un filtre de GABOR, Les filtres de Gabor sont connus comme un moyen d'analyse espace-fréquence très robuste. Cette spécificité a fait des filtres de Gabor un moyen puissant d'analyse de textures et de classification. Les filtres de Gabor analysent la texture d'un objet suivant différentes résolutions et différents angles.

Nous pouvons dire que notre implémentation est fonctionnelle et que les résultats obtenus sont satisfaisants. Nous avons étudié séparément le PCA et le GABOR puis sa fusion qui est beaucoup plus efficace comparant avec le PCA ou le GABOR seul, et cela est bien prouvé dans le Tableau **3.2** et la Figure **3.6**. On peut conclure que la fusion, quel que soit algorithmique ou fusion d'échantillons, donne de meilleurs résultats que ceux obtenus par les systèmes unimodales. Aussi, d'après les résultats du Tableau **3.4**, on remarque que la méthode simple du somme est la meilleur parmi les autres méthodes de combinaison de score.

Dans ce travail, on a réduit l'erreur du (3.1074%) jusqu'a ($4.065*10^{-3}$%) après les fusions, ces résultats illustrent le rôle important de la fusion dans le domaine de la biométrie.

Bibliographie

[1] Peter Gregory And Michael A. Simon, « Biometrics For Dummies », Cisa, Cissp, 2008.

[2] [Anil K. Jain, Arun A. Ross, Karthik Nandakumar] Introduction to Biometrics 2008

[3] [Claus Vielhauer] Biometric User Authentication for IT SECURITY 2006

[4] A.K. Jain, Ruud Bolle, Sharath Pankanti (BIOMETRICS Persona1 Identification in Networked Society 2006

[5] PJames L. Wayman, Anil K. Jain, Davide Maltoni, Da Biometric Systems James L. Wayman, Anil K. Jain, Davide Maltoni, Da Biometric Systems

[6] memoire Etude de la fusion de modalités pour l'authentification en biométrie (visage, voix) Par: OUAMANE Abdelmalik

[7] http://www.abiova.com/dictionnaire%20biometrie%20lettre%20M.asp date 5 03 2015

[8] article (UNE APPROCHE MULTIMODALE POUR LA VERIFICATION BIOMETRIQUE octobre 2011) par ISMAHÈNE DEHACHE(1) &LABIBA SOUICI-MESLATI(2)

[9] Thèse Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris par Nicolas MORIZET 2009

[10] La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées Par Melle Lorène ALLANO 2009

[11] aux bases de personnes virtuelles Contributions `a la dynamique de frappe au clavier : multibiométrie, biométrie douce et mise `a jour de la référence

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

[13] These-Mohamad-ElAbed-Evaluation de systemes biometriques-2011

[14] merouane asmaa IDENTIFICATION BIOMETRIQUE PAR LES VEINES DORSALES DE LA MAIN 2013

[17] Modèles acoustiques à structure temporelle renforcée pour la vérification du locuteur embarquée. Par Anthony LARCHER

[19] La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles

[20] Article A. Ross and A. Jain. "Information fusion in biometrics". Pattern Recognition

Letters, Vol. 24, No. 13, pp. 2115–2125, 2003

[28] mémoire authentification-et-identification-en-biométrie

[30] http://www.tsi.enst.fr/tsi/enseignement/ressources/mti/Gabor/systeme.html 17 04 2015

[31] The Hong Kong Polytechnic University Department of Computing Personal Authentication Using Finger-Knuckle-Print by ZHANG Lin January 2011

[32] Thèse de doctorat de l'INSTITUT NATIONAL DES TELECOMMUNICATIONS Par Melle Lorène ALLANO

[33] Thèse Doctorat en sciences en Automatique Authentification et Identification en biométrie Présentée par : Mébarka BELAHCENE

[18] Handbook of Multibiometrics by [Arun A. Ross, Karthik Nandakumar, Anil K. Jain,]

[15] mbinaison de donnees d espace couleur et de methode de verification d identite

[16] Chapitre 4 Méthodes de Fusion et Normalisation. http://thesis.univ-biskra.dz/944/7/Chap%204%20M%C3%A9thodes%20de%20Fusion.pdf.

[21] http://www.sthda.com/french/wiki/introduction-a-l-analyse-en-composante-principale

[22] http://fr.wikipedia.org/wiki/Analyse en composantes principales

[23] ETUDE DE LA TRANSFORMEE EN ONDELETTES DANS LA COMPRESSION D'IMAGES FIXES Z-E. BAARIR, A. OUAFI

[24] http://etud.insa-toulouse.fr/~flone sa/BEmultimedia/index.php?Dwt

[25] http://fr.wikipedia.org/wiki/Transform%C3%A9e en cosinus discr%C3%A8te

[26] http://lmrs.univ-rouen.fr/Vulgarisation/JPEG/jpeg-DCT.html

[27] http://etud.insa-toulouse.fr/~flone sa/BEmultimedia/index.php?Dct

[29] Secure Biometrics: Finger Knuckle Print, Amravati, India