REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

UNIVERSITE KASDI MERBAH OUARGLA

Faculté des Nouvelles Technologies de l'Information et de la communication

Département de l'Electronique et de la Télécommunication

Mémoire

MASTER ACADEMIQUE

Domaine : Electronique

Spécialité : Automatique

Présenté par :

SAIDAT DJEMAA

GUEZIZ FATIHA

Thème

Identification des personnes par l'empreinte de l'articulation des doigts

Soutenu publiquement

Le : 02/06/2016

Devant le jury :

Mr. D. SAMAI	**MCB**	**Président**	**UKMOuargla**
Mr. A R. BENCHABANE	**MCB**	**Examinateur**	**UKM Ouargla**
Mr. N. NACERI	**MAB**	**Examinateur**	**UKM Ouargla**
Mr. Z. TIDJANI	**MAA**	**Encadreur/rapporteur**	**UKM Ouargla**

Année Universitaire : 2015 /2016

Remerciments

Je remercie en premier lieu Dieu qui m'a donné ce bien là et pour que je vie ce jour et la force et la patience pour terminer ce travail.

Remercier la personne qui m'a aidé à réaliser ce travail dans les meilleures conditions mon encadreur monsieur Tedjani Zakaria qui a proposé et a dirigé ce travail. Nous tenons à remercier Mr Ben Saïd Khaled Pour l'aider. Sa disponibilité, sa patience tout au long de ce travail nous a été bénéfique.

Je remercie monsieur le président de jury, ainsi que les membres de jury d'avoir accepté de juger ce travail.

Je tiens à remercier les responsables et tout le personnel du département d'Electronique d'Ouargla pour les facilités qu'ils m'ont accordés pour terminer ce travail.

Je tiens à remercier ma famille pour leur apport affectif et leurs sacrifices.

Le travail de mémoire que j'ai effectué doit beaucoup à certaines personnes que je tiens à les remercier sincèrement.

Enfin, je remercie tous ceux qui ont contribué de près ou de loin à ma formation et à l'élaboration de ce modeste mémoire.

Dédicace

Je dédie ce mémoire:

À mes très chers parents pour leur soutient durant tout mon cursus scolaire et qui m'ont permis de réussir dans mes études.

Et mes frères et mes sœurs

A tous la famille Gueziz

À tout mes amis en plus Nacerddine maabedi

Et À toutes les professeurs et enseignants

A tout la promotion deuxième master Automatique

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

FATIHA

Dédicace

Je dédie ce mémoire:

A ma mère avec toute mon affection, Pour leur soutien tout au long de Mon vie Bourses d'études

A Ma grand-mère

A tout mes amis

Et mes frères et mes sœurs.

A tout mes amis

A tous la famille Saidat

À toutes les professeurs et enseignants que j'ai eu durant tout mon cursus scolaire et qui m'ont permis de réussir dans

mes études

A tout la promotion deuxième master Automatique

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

DJEMAA

Table des matières

Chapitre II : La biométrie multimodale

Chapitre III : Extraction des caractéristiques par la méthode de HOG

Chapitre IV : Résultats et discussions

Liste des figures

C-HOG	Circulaire-Histogramme de Gradient Orienté
EER	Equal Error Rate
FAR	False Acceptance Rate
FKP	Finger Knuckle Print
GAR	Genuine Acceptance Rate
HOG	Histogramme de Gradient Orienté
MAD	Médian
MB-HOG	Multi Block - Histogramme de Gradient Orienté
Min-Max	Minimum-Maximum
PIN	Personale Identification Nombre
Q LQ	Quadratique Linéaire Quadratique
R-HOG	Rectangulaire- Histogramme de Gradient Orienté
ROC	Receiver Operating Curve
ROI	Region Of Interest
Tanh	Tangente hyperbolique

Introduction général

Introduction générale

Les systèmes de reconnaissance biométriques, utilisés de plus en plus tant dans le domaine privé que public, comportent de nombreux avantages pour les personnes qui les introduisent et les personnes concernées. Toutefois, l'utilisation de données biométriques pour l'identification ou la vérification d'une identité prétendue comporte également des risques quant au respect des droits et des libertés fondamentales.

Ces systèmes de reconnaissance reposent sur l'analyse de caractéristiques physiologiques ou comportementales du corps humain. L'utilisation de données biométriques pour la reconnaissance comporte des risques pour les personnes concernées: en particulier le non respect du droit à l'autodétermination informationnelle, l'usurpation d'identité, la création d'un identifiant unique global, l'exploitation d'informations complémentaires sur la personne concernée contenues dans les données biométriques.

Cette thématique est d'autant plus importante au regard des risques liés aux perspectives d'utilisation future de caractéristiques biométriques comme identifiant unique global; à savoir pour apparier des données provenant de diverses sources afin de réaliser un profil de personnalité à l'insu des personnes concernées.

La méthode d'identification basée sur des caractéristiques biométriques est préférable à des mots de passe traditionnels on code PIN. De nombreux travaux ont été réalisés sur l'optimisation séparée des modalités biométriques, et ont proposé une approche d'intégration de plusieurs modalités biométriques (en l'occurrence deux modalités) afin de pallier aux problèmes de la vérification biométrique uni modale.

Dans cette perspective, un de ces systèmes a été choisi d'être étudié, c'est le système qui utilise l'empreinte des doigts FKP (Finger-Knuckle-Print) comme caractéristique biométrique de reconnaissance par image. Son modèle est unique pour chaque individu aussi elle ne représente pas un gène pour l'utilisateur. Nous allons focaliser dans ce travail sur l'étude d'un système complet d'identification par FKP comme trait biométrique. Le but est de développer une extraction robuste du modèle biométrique par l'utilisation de la méthode de l'histogramme de gradient orienté et en suite choisir le meilleur résultat après la comparaison de ces modèles**.**

Nous allons organiser ce mémoire comme suit :

Dans le premier chapitre, nous présentons quelques définitions de base liées à la biométrie et le principe de fonctionnement et performances des systèmes biométriques.

Dans le deuxième chapitre, nous introduirons quelques notions dans la biométrie multimodale et traitons la question de la fusion et ses différents niveaux, ainsi que les principales méthodes de normalisation des scores.

Dans le troisième chapitre, nous allons présenter des généralités sur les méthodes d'extraction des caractéristiques, et développer l'utilisation du descripteur de l'histogramme de gradient orienté (HOG : Histogram of Oriented Gradient). Différentes méthodes de calcul des distances seront aussi présentées.

Dans le quatrième chapitre, présentera les résultats de tests effectués avec les algorithmes HOG et Multi Bloc-HOG (MB-HOG) sur la base de données FKP et une étude comparative on utilisant plusieurs distances, ainsi que la fusion de données.

En fin, nous terminerons par une conclusion générale.

CHAPITRE I

Biométrie pour l'identification

I.1 Introduction

La biométrie est la science qui étudiée les méthodes de vérification ou l'identification d'identité, qu'on utilise pour différencier des personnes entre elles en se basant sur la reconnaissance des caractéristiques biologiques (physiologiques ou comportementales) de l'individu. Elle représente un moyen puissant de vérification d'identité dans quelques applications une fois correctement mise en application. D'ailleurs, une fois combinée avec les autres techniques de vérification (des clefs et des mots de passe) un certain niveau de sécurité peut être atteint**.**

Nous introduirons dans ce chapitre quelques notions et définitions de base liées à la biométrie. Après définition, nous allons présenter les modes de fonctionnement d'un système biométrique et se principales modules. Ensuite, nous développerons les critères d'évaluation des performances de tels systèmes.

I.2 La biométrie

I.2.1 Définition

La biométrie vise à identifier les personnes à partir de leurs caractéristiques physiques. L'utilisation de la biométrie s'est répandue énormément dans la vie quotidienne et trouve de nombreuses applications ; pour pénétrer dans un lieu et y circuler librement, pour accéder au poste de travail, retirer de l'argent, etc. La biométrie tend à remplacer peu à peu les codes d'accès et les mots de passe qui peuvent être changées ou volées. De nombreux travaux de recherche ont été menés et en cherche toujours des nouvelles méthodes. La biométrie peut être définie comme étant ''la reconnaissance automatique d'une personne en utilisant des traits distinctifs**".** **[1]**

I.2.2 Les modalités de la biométrie

Tout d'abord, il est nécessaire de comprendre que la biométrie regroupe différents domaines d'exploitation des facteurs biologiques qui restent identifiables au long terme. Ainsi plusieurs modalités biométriques sont utilisées pour identifier des personnes : le visage, l'iris, les empreintes digitales, la main, la rétine et la signature, la frappe au clavier, la voix. **(Voir la figure I.1**)

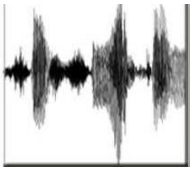
			
L'empreinte digitale	**Le visage**	**L'iris**	**La rétine**
			
La main	**La signature**	**La frappe au clavier**	**La voix**

Figure I.1 : Certaine diversité des techniques biométriques.

I.3 Catégories de technologies biométriques

Il existe plusieurs techniques biométriques utilisées dans différentes applications et secteurs, on peut en distinguer deux catégories : **[2]**

I.3.1 Biométrie morphologique (physique)

Elle est basée sur l'identification de traits physiques particuliers qui pour toute personne, sont uniques et permanents dans ce qui suit :

a - Empreinte digitale

Empreinte digitale est la caractéristique d'un doigt. On le croit que chaque empreinte digitale est unique. Chaque personne a ses propres empreintes digitales avec l'unicité permanente. Ainsi les empreintes digitales sont utilisées depuis longtemps pour l'identification et l'investigation juridique. Une empreinte digitale se compose de beaucoup des rides et sillons. Ces rides et sillons présentent de bonnes similitudes dans chaque petite fenêtre locale. **[2]**

b - Visage

Le visage est la biométrie la plus commune et la plus populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction

visuelle. Les caractéristiques jugées significatives pour la reconnaissance du visage sont: les yeux, la bouche et le tour du visage. **[3]**

c - L'iris

L'utilisation de l'iris comme caractéristique biométrique unique de l'homme a donné lieu à une technologie d'identification fiable et extrêmement précise. L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'œil, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. **[4]**

d - 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 stable durant la vie. 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. L'analyse biométrique de la rétine est la technologie la plus difficile à mettre en œuvre. **[5]**

e - Géométrie de La main

La géométrie de la main est une technologie biométrique récente. Comme son nom l'indique, elle consiste à analyser et à mesurer la forme de la main, c'est-à-dire mesurer la longueur, la largeur et la hauteur de la main d'un utilisateur. Cette technologie offre un niveau raisonnable de précision est relativement facile à utiliser. Cependant elle peut être facilement trompée par des jumeaux ou par des personnes ayant des formes de la main proches. **[4]**

I.3.2 Biométrie comportementales

Elle se base sur l'analyse de certains comportements d'une personne dans ce qui suit :

a - La 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…etc. L'acceptation de cette technique est très bonne car la signature est un geste commun pour

tout le monde, n'est pas très précise car la signature peut être affectée par des facteurs physique et émotionnels. **[5]**

b - La dynamique de frappe au clavier

La dynamique de frappe au clavier est caractéristique de l'individu, quelque sorte la transposition de la graphologie aux moyens électroniques les paramètres suivants sont généralement pris en compte **: [2]**

- Vitesse de frappe.
- Suite des lettres.
- Mesure de temps de frappe.
- Pause entre chaque mot.
- Reconnaissance de mot(s) précis.

c -La voix

La biométrie de la voix traite des données qui proviennent à la fois de facteurs physiologiques dépendants de l'âge, du sexe, de l'accent et de facteurs comportementaux comme la vitesse et le rythme. Ils ne sont en général pas imitables. C'est la seule technique qui permette à l'heure actuelle de reconnaître une personne à distance et qui est en général bien accepté par les usagers. Cependant cette technique est très facilement falsifiable et nécessite en plus une excellente qualité d'enregistrement**. [3]**

Chaque technologie possédant des avantages et des inconvénients, acceptables ou inacceptables suivant les applications. Ces solutions ne sont pas concurrentes, elles n'offrent ni les mêmes niveaux de sécurité ni les mêmes facilités d'emploi. Le **tableau I.1** résume une comparaison des traits biométriques

Tableau I.1 : comparaison des traits biométrique.

Technique	Avantages	Inconvénients
Empreintes digitales	- Coût - Ergonomie moyenne	- Acceptabilité moyenne - Possibilité d'attaque
Forme de la main	-Très ergonomique - Bonne acceptabilité	-Système encombrant et coûteux -Perturbation possible par des blessures
Visage	- Coût -Bonne acceptabilité	- Jumeaux, déguisement vulnérabilité aux attaques (facile à falsifier)
Rétine	- Fiabilité - Pérennité	- Acceptabilité très faible - Contrainte d'éclairage
Iris	- Fiabilité	- Acceptabilité très faible - Contrainte d'éclairage
Voix	- Facilité	-Vulnérable aux attaques (faciles à falsifier)
Signature	- Ergonomie	- Dépendant de l'état émotionnel de la personne peu fiable
Frappe au clavier	- Ergonomie	- Dépendant de l'état physique de la personne peu fiable

I.5 Modes de fonctionnement d'un système biométrique

Les systèmes biométriques peuvent fournir trois modes de fonctionnement à savoir mode d'enrôlement**,** mode vérification ou bien en mode d'identification

I.5.1 Le mode d'enrôlement

C'est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier. 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 et enfin stockées dans une base de données**. [6]** Ce mode est illustré par la **Figure I.2**

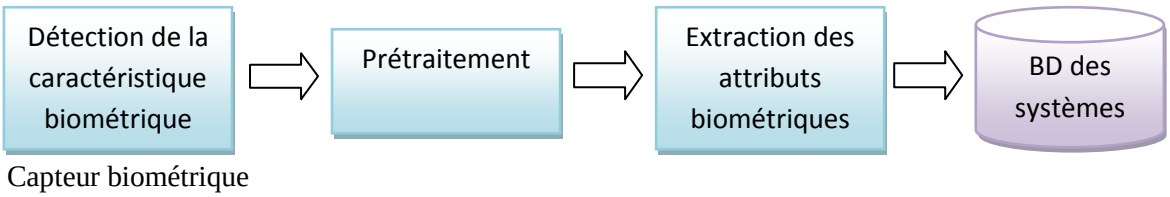


Figure I.2 : Mode d'enrôlement d'un système biométrique.

I.5.2 Le mode vérification ou authentification

Le système vérifie l'identité d'une personne en comparant les données biométriques acquises avec celles stockées dans la base de données. Dans un tel système, la personne revendique une identité, généralement via un code PIN (Personal Identification Number), un nom d'utilisateur, une carte à puce, etc., le système effectue alors une comparaison on appariement (1 : 1) afin de déterminer si la déclaration est vraie ou non **(Voir la Figure I.3)**. **[3]**

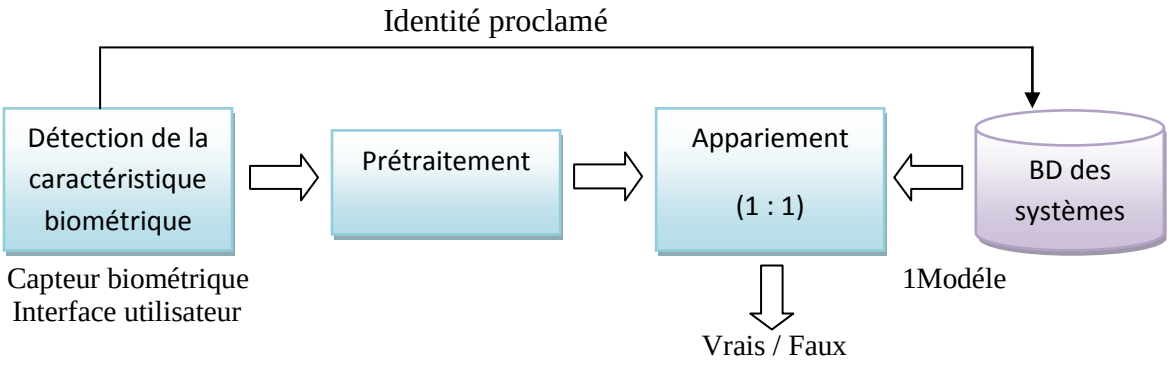


Figure I.3 : Mode de vérification d'un système biométrique.

I.5.3 Le mode identification

Le système doit deviner l'identité de la personne. Il répond à une question de type : qui suis- je ? Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données. En général, lorsque l'on parle d'identification, on suppose que le problème soit fermé, c'est-à-dire toute personne qui utilise le système possède un modèle dans la base de données. Dans ce mode, le système effectue un appariement (1 : N) pour identifier la personne en question comme illustré à la **Figure I.4**

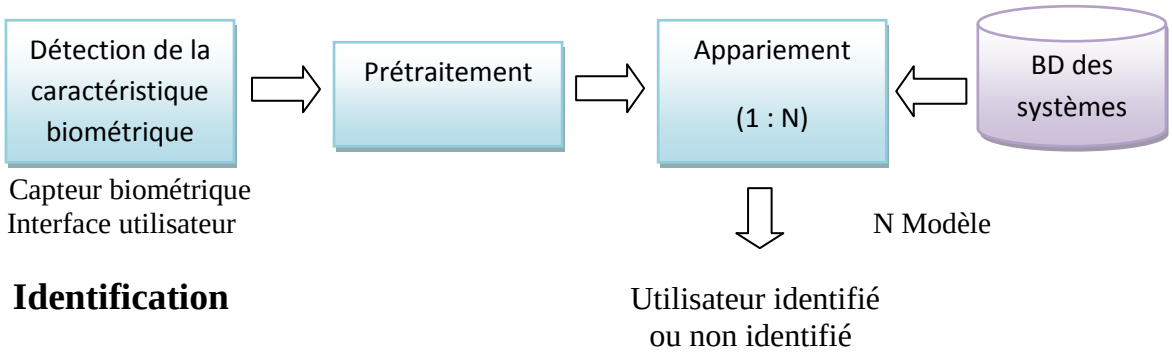


Figure I.4 : Mode d'identification d'un système biométrique.

I.6 Principaux modules du système biométrique

Un système biométrique est composé de quatre modules principaux, chacun des ces modules est définis dans ce qui suit. **[6]**

I.6.1 Module capteur biométrique

Correspond à la lecture de certaines caractéristiques morphologique ou comportementales d'une personne, au moyen d'un terminal de capture biométrique (ou capteur biométrique) à l'aide d'une interface utilisateur.

I.6.2 Module d'extraction de caractéristiques

Prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données (modèle extrait). Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe.

I.6.3 Module comparaison

Compare les caractéristiques biométriques d'une personne soumise à contrôle avec les signatures mémorisées. Ce module fonctionne soit en mode vérification (pour une identité proclamée) ou bien en mode identification (pour une identité recherchée).

I.6.4 Module base de données

Stocke les modèles biométriques des utilisateurs enrôlés. Cette base de donnée sera utilisé comme, conteneur de modèle de référence en vue de vérification ou d'identification

I.7 Evaluation des performances des Systèmes biométriques

Chaque caractéristique (ou modalité) biométrique a ses forces et ses faiblesses, et le choix dépend de l'application visée. On ne s'attend à ce qu'aucune modalité biométrique ne réponde efficacement aux exigences de toutes les applications. Plusieurs études ont été menées afin d'évaluer les performances des systèmes biométriques. Ces études sont basées sur quatre critères d'évaluation : **[6]**

I.7.1 Intrus vit*e*

Ce critère permet de classifier les systèmes biométriques en fonction de l'existence d'un contact direct entre le capteur utilisé et l'individu à reconnaître.

I.7.2 Fiabilité

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

I.7.3 Coût

Doit être modéré. À cet égard nous pouvons dire que la reconnaissance faciale ne nécessite pas une technologie coûteuse. En effet, la plupart des systèmes fonctionnent en utilisant un appareil à photo numérique de qualité standard**.**

I.7.4 Effort

Requis par l'utilisateur lors de la saisie de mesures biométriques, et qui doit être réduit le plus possible.

Un système biométrique peut faire deux types d'erreurs. Il peut rejeter un utilisateur légitime et dans ce premier cas on parle de faux rejet (false rejection). Il peut aussi accepter un imposteur et on parle dans ce second cas de fausse acceptation (false acceptance). La performance d'un système se mesure donc à son taux de faux rejet (False Rejection Rate ou FRR) et à son taux de fausse acceptation (False Acceptance Rate ou FAR). **[7]**

- **Le FAR (False Acceptance Rate)**

Ce taux représente le pourcentage d'individus reconnus par le système biométrique. Le système classe alors deux caractéristiques provenant de deux personnes différentes comme appartient à la même personne. **[5]**

$$\mathbf{FAR} = \frac{\textbf{Nombre des imposteurs acceptés}}{\textbf{Nombre totale d'accés imposteurs}} \qquad \textbf{(I.1)}$$

- **Le FRR (False Rejection Rate)**

La fréquence des rejets par rapport aux personnes qui doivent être correctement vérifiée. Quand un utilisateur autorisé est rejeté il ou elle doit représenter leurs caractéristiques biométriques au système. **[3]**

$$\mathbf{FRR} = \frac{\textbf{Nombre des clients rejetés}}{\textbf{Nombre totale d'accés clients}} \qquad \textbf{(I.2)}$$

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

- **L'EER (Equal Error Rate)**

Le point d'équivalence des erreurs est le taux d'exactitude croisée, est déterminé par le point d'intersection entre la courbe du taux de fausses acceptations et la courbe du taux de faux rejets, on peut aussi définir le taux d'erreur égal (Equal Error Rate ou EER) comme suit :

$$\mathbf{EER} = \frac{\textbf{Nombre de fausse acceptations+Nombre de faux rejets}}{\textbf{Nombre totale d'accés}} \qquad \textbf{(I.3)}$$

La Figure I.5 illustre l'EER à partir des courbes EER (θ) et FAR (θ) avec θ et le paramètre seuil de décision (Threshold).

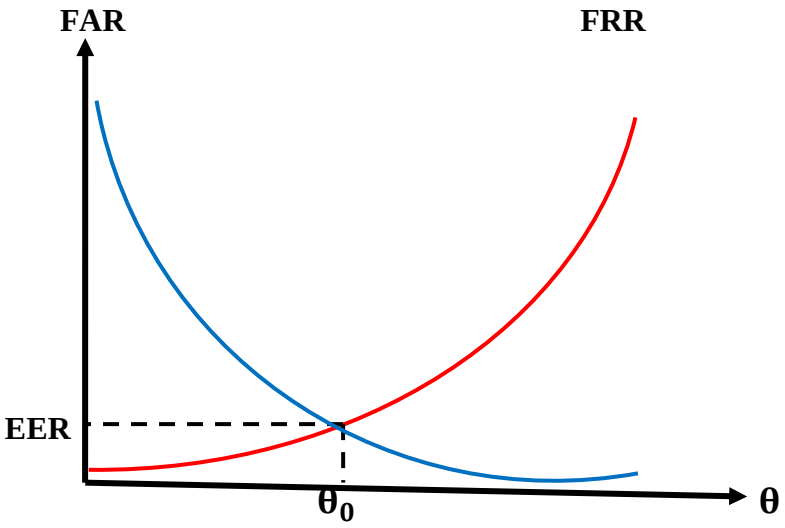


Figure I.5 : Graphe démonstratif de l'EER

$\boldsymbol{\theta_0}$: Seuil correspondant au point d'équivalence des erreurs

Les performances d'un système biométrique peuvent être présentées graphiquement à l'aide de la courbe ROC (Receiver Operating Characteristic), illustrée par à la (**Figure I.6).** Cette courbe permet de représenter graphiquement la performance d'un système de vérification pour les différentes valeurs de θ. Le taux d'erreur égal (Equal Error Rate ou EER) correspond au point FAR=FRR, c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice.

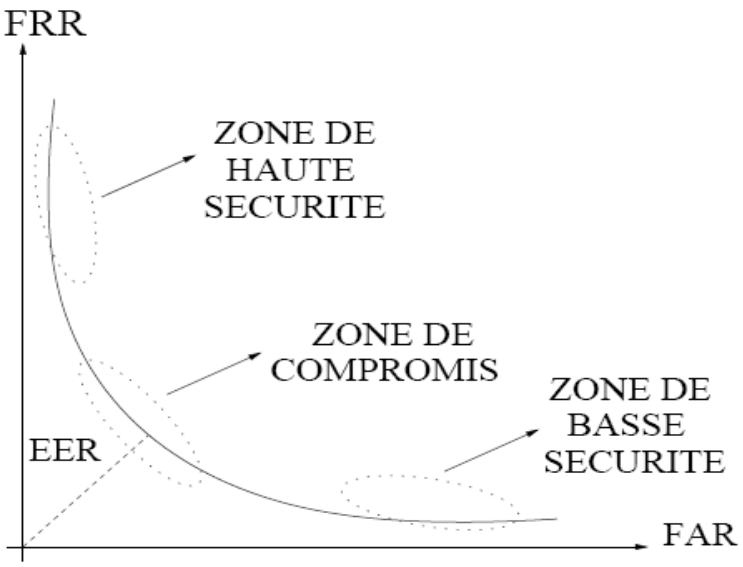


Figure 1.6 : Courbe ROC

Il est fréquemment utilisé pour donner un aperçu de la performance d'un système biométrique. Cependant, il est important de souligner que l'EER ne résume en aucun cas toutes les caractéristiques d'un système biométrique. Le seuil θ doit donc être ajusté en fonction de l'application ciblée : haute sécurité, basse sécurité ou compromis entre les deux. **[4]**

Le but fondamental de tout système biométrique opérant au niveau score, est de pouvoir séparer au maximum les distributions de score des imposteurs et des authentiques **(Figure I.7).** En minimisant la zone de recouvrement entre ces deux distributions, on améliore la performance globale du système en augmentant le taux de reconnaissance. **[8]**

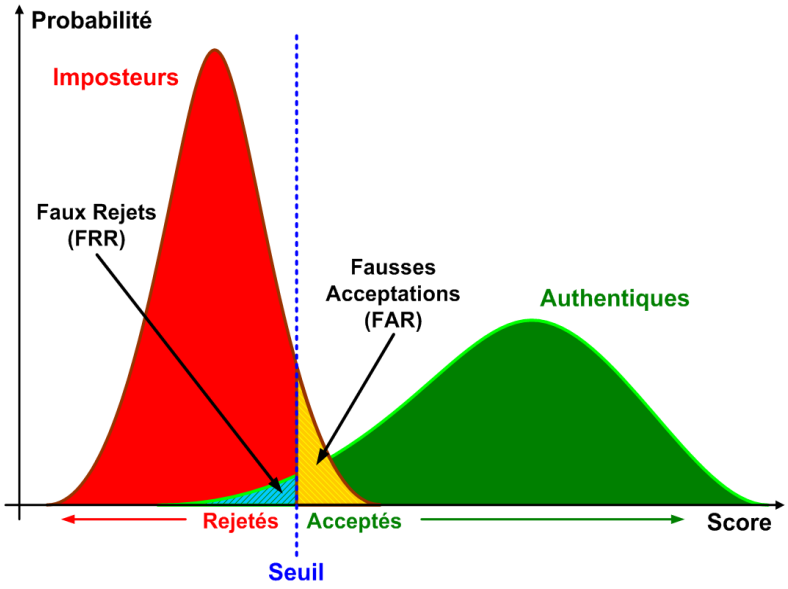


Figure I.7 : Illustration du FRR et du FAR.

I.8 Applications du système biométrique

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. **[6]**

I.8.1 Applications commerciales

Telles que l'ouverture de réseau informatique, la sécurité de données électroniques, l'e-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.

I.8.2 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.

I.8.3 Applications légales

Telles que l'identification de corps, la recherche criminelle, l'identification de terroriste, etc**. [6]**

I.9 Conclusion

Dans ce chapitre, nous avons introduit le concept des systèmes biométriques, leur architecture et leurs différentes applications. Nous avons aussi constaté que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre. Parmi les critères d'évaluation de la qualité du système biométrique, nous avons présente les toux des erreurs (FAR, FRR et ERR) ainsi que les courbes ROC selon qu'on est en mode identification ou vérification.

CHAPITRE II

Notion à la multi biométrie

II.1 Introduction

La biométrie multimodale qui consiste à combiner plusieurs systèmes biométriques, est de plus en plus étudiée **[9].** En effet, elle permet de réduire certaines limitations des systèmes biométriques, comme l'impossibilité d'acquérir les données de certaines personnes ou la fraude intentionnelle, tout en améliorant les performances de reconnaissance. Ces avantages apportés par la multi modalité aux systèmes biométriques sont obtenus en fusionnant plusieurs systèmes biométriques.

Dans ce chapitre nous traitons la question de la fusion et ses différents niveaux. Particulièrement la fusion des caractéristiques et des scores qui font l'objet de notre travail. Les principales méthodes de normalisation des scores, de fusion par combinaison seront aussi présentées.

II.2 Différentes approches de la multi biométrie

La fusion d'éléments biométriques peut se référer à de nombreux scénarios différents. La **Figure II.1** illustre les cinq principales approches des systèmes multi biométriques ou aussi appelés multimodaux. **[10]**

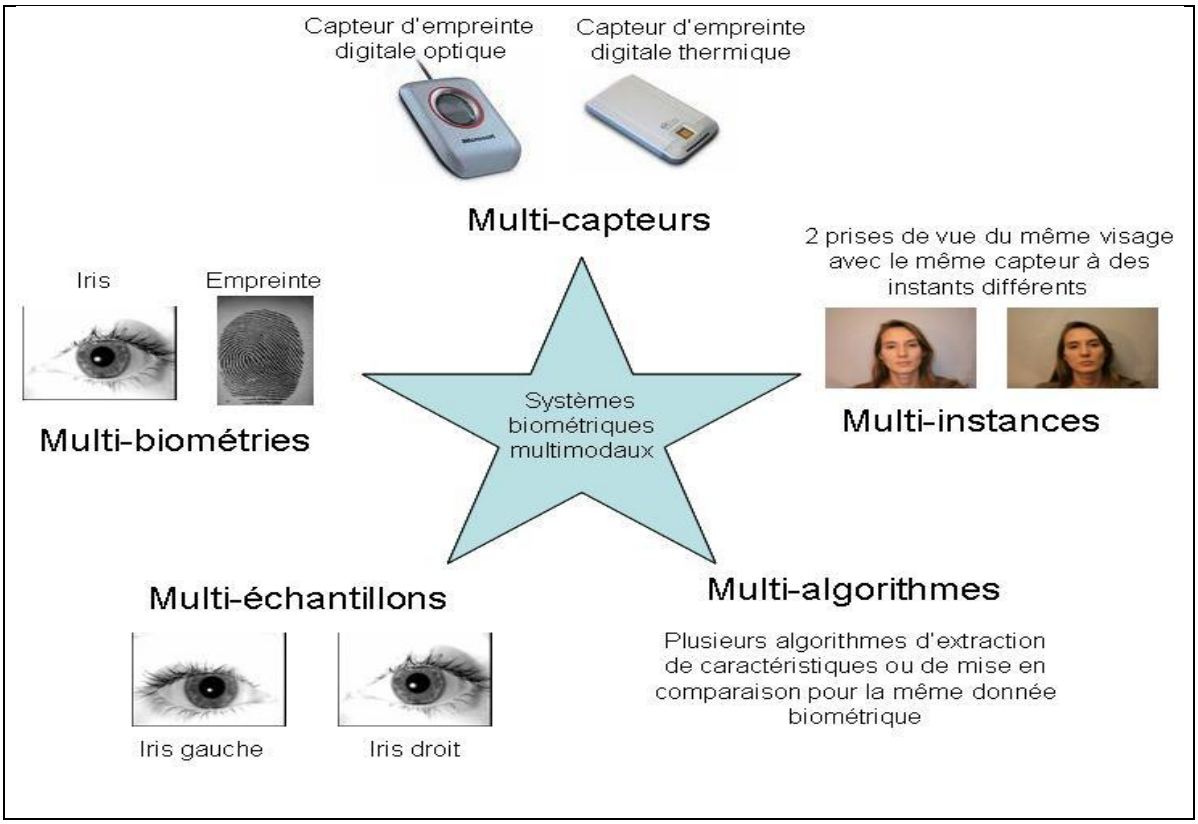


Figure II.1 : Différentes approches des systèmes multimodaux.

II.2.1 Systèmes multi-algorithmes

Cette classe désigne les systèmes qui utilise plusieurs algorithmes d'extraction des caractéristiques (de même type ou de types différents) à partir d'une seule modalité biométrique.

II.2.2 Systèmes multi-capteurs

La même caractéristique biométrique est capturée à l'aide de divers capteurs pour extraire des informations à partir de différentes images enregistrées**. [11]**

II.2.3 Systèmes multi-instances

Dans ces systèmes on associe 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. **[9]**

II.2.4 Systèmes multi-échantillons

Cette classe désigne les systèmes où un même capteur est utilisé pour obtenir plusieurs variantes ou représentations complémentaires d'une seule modalité biométrique. C'est le cas des systèmes utilisant l'iris droit ainsi que le gauche par exemple. **[12]**

II.2.5 Systèmes multi-caractères

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.

II.2.6 Systèmes hybrides

Sont des systèmes dynamiques en utilisés pour désigner un système multi biométrique qui intègre un sous-ensemble des cinq scénarios décrits précédemment. **[12]** Les systèmes hybrides disposent donc de plus d'information que les systèmes précédents.
Nous pouvons aussi trouver d'autre systèmes tels que :

II.2.7 Systèmes séries

Qui peut être privilégiée dans certaines applications ; par exemple si la multi-modalité est utilisée pour donner une alternative pour les personnes ne pouvant pas utiliser l'empreinte digitale. Pour la majorité des individus seule l'empreinte est acquise et traitée

mais pour ceux qui ne peuvent pas être ainsi authentifiés on utilise un système à base d'iris alternativement **(Voir la Figure II.2)**. **[10]**

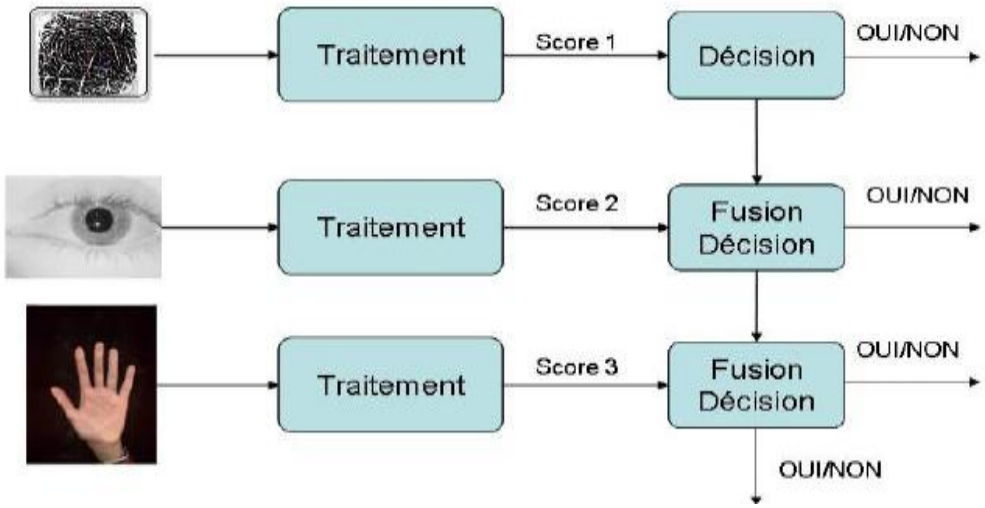


Figure II.2 : Système multi biométrique en série

II.2.8 Systèmes parallèles

Ce type de système est le plus utilisé car il permet d'incorporer toutes les informations disponibles et donc d'améliorer les performances du système. En revanche, l'acquisition et le traitement d'un grand nombre de données biométriques est coûteux en temps et en matériel, et réduit le confort d'utilisation **(Voir la Figure II.3)** . **[10]**

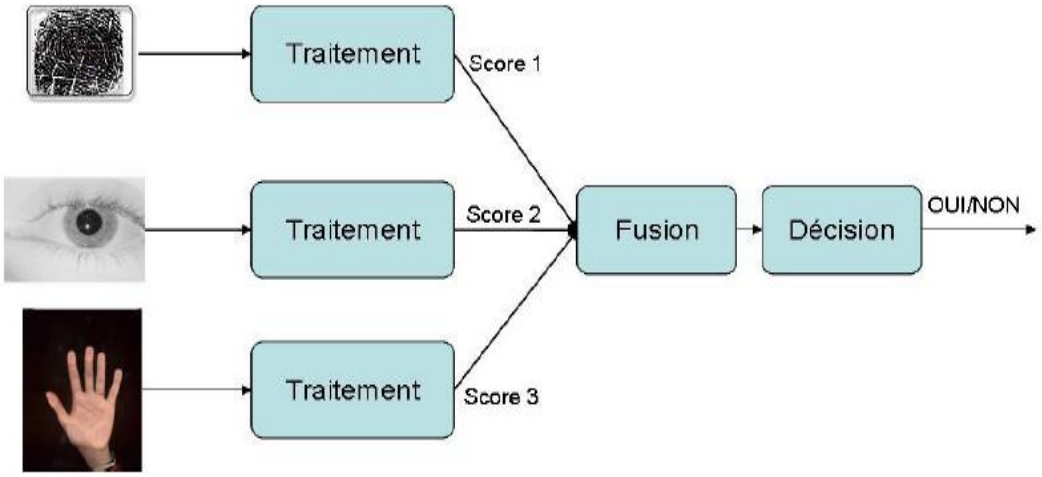


Figure II.3 : Système multi biométrique en parallèle**.**

II.3 Niveau de Fusion

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. comme montre la **Figure II.4**

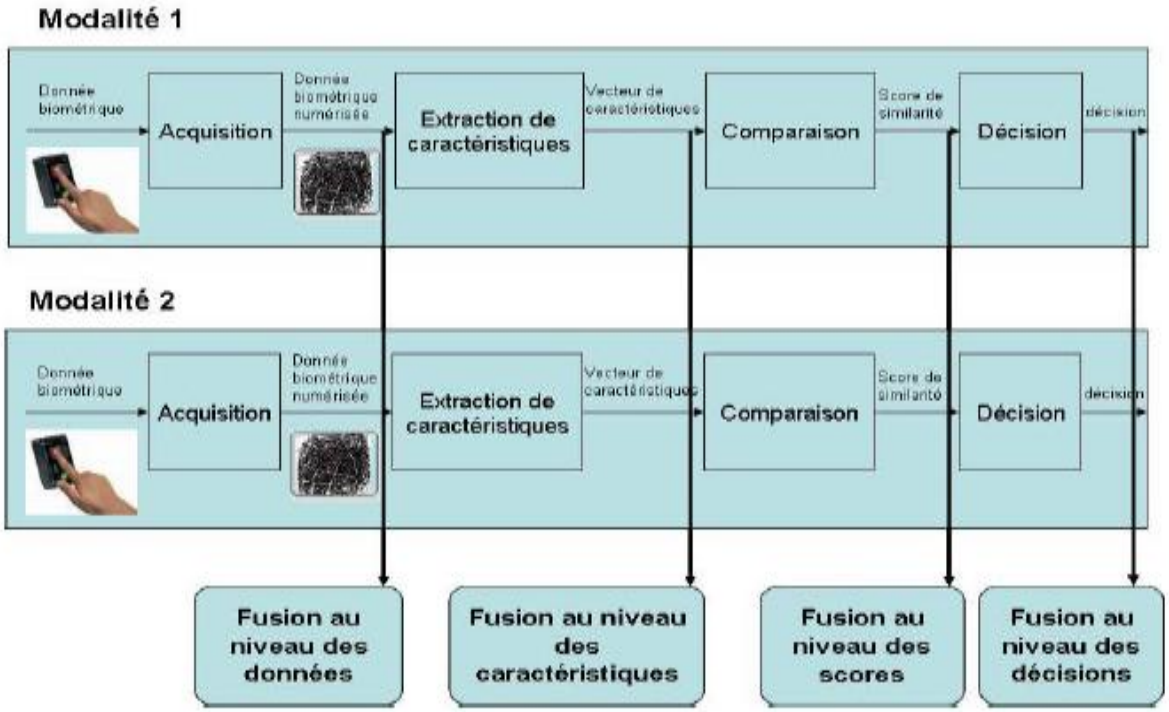


Figure II.4 : Les différents niveaux de fusion

II.3.1 Fusion au niveau des capteurs

Les données acquises de détection de la même caractéristique biométrique avec deux ou plusieurs capteurs sont combinées. La fusion au niveau du capteur n'est applicable que si les sources multiples représentent des échantillons de la même caractéristique biométrique soit en utilisant un seul capteur ou des capteurs compatibles différents.

II.3.2 Fusion au niveau caractéristique

Chaque processus biométrique produit une série des caractéristiques. Le processus de fusion combine ces collections de caractéristiques en un unique ensemble ou vecteur de caractéristiques. **[13]**

II.3.3 Fusion au niveau de score

Lorsque chaque système biométrique émet un score de correspondance indiquant la proximité de la donnée d'entrée à un modèle, l'intégration peut être faite au niveau du score du match. Ceci est également connu sous le nom de fusion au niveau de la mesure ou au niveau de confiance.

II.3.4 Fusion au niveau de décision

La fusion au niveau de décision 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**. **[10]**

II.4 Fusion des scores

Nous allons maintenant nous intéresser aux méthodes de fusion de scores. Ces méthodes combinent les informations des scores issus des modules de comparaison à ce niveau. Un système de fusion est constitué de deux modules, un module de fusion et un module de décision **(Voir la Figure II.5)**.

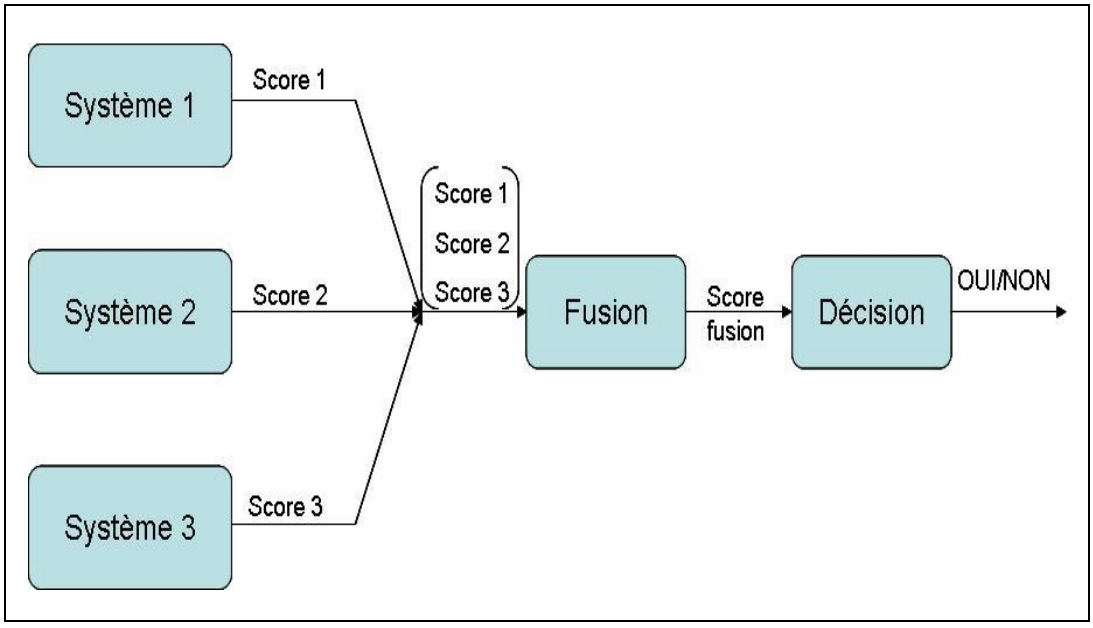


Figure II.5 : Schéma de la fusion des scores

II.4.1 Normalisation des Scores

Les méthodes de normalisation des scores ont pour objectif de transformer individuellement chacun des scores issus des systèmes pour les rendre homogènes avant de les combiner. Les différentes techniques de normalisation des scores sont : **[5]**

- 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 **(MED).**
- Normalisation par la méthode **tangente hyperbolique (Tanh).**
- Normalisation par une fonction **double sigmoïde.**

II.4.1.1 Normalisation par la méthode Min-Max

La normalisation Min-Max conserve la distribution de scores originale à un facteur d'échelle près et transforme tous les scores dans l'intervalle [0,1]. Le score normalisé Min-Max noté S_{ik} pour le score de test S_{ik} est donné par **(II.1):**

$$S_{ik}' = \frac{S_{ik} - \min(\{S_i\})}{\max(\{S_i\}) - \min(\{S_i\})'} \qquad \textbf{(II.1)}$$

S_{ik} le $k^{ème}$ score de sortie du $i^{ème}$ système, où **i = 1, 2, ..., N** et **k = 1, 2, ..., M**

II.4.1.2 Normalisation par la méthode Z-Score

Pour une distribution arbitraire, la moyenne et l'écart-type sont respectivement des estimateurs raisonnables de position et d'échelle.

$$S_{ik}' = \frac{S_{ik} - \mu}{\sigma} \qquad \textbf{(II.2)}$$

Où **μ** est la moyenne arithmétique et **σ** l'écart-type des données.

Cette méthode n'est pas robuste. De plus, la normalisation Z-Score ne garantit pas un intervalle commun pour les scores normalisés provenant de différents systèmes.

II.4.2 Combinaison des Scores

Les méthodes de combinaisons des 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 la moyenne, le produit, le minimum, le maximum ou la médiane. **[9]**

- Combiner les scores par la moyenne consiste à calculer S tel que :

$$S = \frac{1}{N}\sum_{i=1}^{N} S_i \qquad \textbf{(II.7)}$$

- Combiner les scores par le produit consiste à calculer S tel que :

$$S = \prod_{i=1}^{N} S_i \qquad \textbf{(II.8)}$$

- Combiner les scores par le minimum consiste à calculer S tel que :

$$S = \min(S_i) \qquad \textbf{(II.9)}$$

- Combiner les scores par le maximum consiste à calculer S tel que :

$$S = \max(S_i) \qquad \textbf{(II.10)}$$

- Combiner les scores par la médiane consiste à calculer S tel que :

$$S = \text{med}(S_i) \qquad \textbf{(II.11)}$$

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 :

$$S = \sum_{i=1}^{N} w_i S_i \qquad \textbf{(II.12)}$$

La somme pondérée permet de donner des poids différents 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.

II.5 Conclusion

Dans Ce chapitre nous avons présenté les différents principes de la multi-biométrie, particulièrement nous a permis de connaitre un certain nombre des méthodes de fusion des scores, et on comprend bien la nécessité de normaliser les scores avant de les combiner.

CHAPITRE III

Extraction des caractéristiques par la méthode HOG

III.1 Introduction

Les caractéristiques biométriques sont une solution alternative aux anciens moyens de vérification d'identité. L'avantage de ces caractéristiques biométriques est d'être universelles, c'est-à-dire présentes chez toutes les personnes à identifier. Ces caractéristiques sont utilisées afin de décrire et ainsi différencier les objets. D'autre part, elles sont mesurables et uniques : deux personnes ne peuvent pas posséder exactement la même caractéristique. Elles sont aussi permanentes ce qui signifie qu'elles ne varient pas ou peu au cours du temps.

A travers ce chapitre, nous allons présenter des généralités sur les méthodes d'extraction des caractéristiques. En particulier, nous allons développer l'utilisation du descripteur de l'histogramme de gradient orienté. Différentes méthodes de calcul des distances seront aussi présentées. A la fin, nous terminons par une conclusion.

III.2 L'extraction des caractéristiques

Cette étape représente le cœur du système de reconnaissance, on extrait de l'image les informations qui seront sauvegardées en mémoire pour être utilisées plus tard dans la phase de décision. Le choix de ces informations utiles revient à établir un modèle pour l'image, elles doivent être discriminantes et non redondantes. L'analyse est appelée représentation, modélisation ou extraction des caractéristiques. L'efficacité de cette étape a une influence directe sur la performance du système de reconnaissance**. [14]**

Le problème de l'extraction des caractéristiques est parfois établi comme une transformation linéaire qui projette les vecteurs des caractéristiques sur le sous-espace transformé défini par les directions concernées. Etant donne un vecteur des caractéristiques **X** d'une dimension **D**, une matrice **K*D** est appliquée pour obtenir un vecteur **Y** des caractéristiques transformées de dimension **K (K<D)**. La matrice est estimée de sorte que, du point de vue de la classification, la redondance est supprimée et les caractéristiques transformées ne retiennent que les informations pertinentes, ce qui a pour effet, en théorie, d'optimiser les performances pour les valeurs cibles de **K**, et devrait surpasser les performances des caractéristiques de base, vu qu'on a supprimé les éléments nuisibles ou qui prêtent à confusion et, plus probablement, de mieux estimer le modèle des paramètres (plus robuste).**[15]**

III.3 Généralité sur les méthodes de l'extraction des caractéristiques

Les méthodes de reconnaissance peuvent être classées en trois grandes approches. Une approche globale ces méthodes sont basées sur des techniques d'analyse statistique bien connues. Il n'est pas nécessaire de repérer certains points caractéristiques d'image. Nous pouvons distinguer deux types de techniques parmi les méthodes globales les techniques linéaires et les techniques non linéaires voir la **(Figure III .1).** L'avantage principal de ces méthodes est qu'elles sont relativement rapides à mettre en œuvre et que les calculs de base sont d'une complexité moyenne.

Une approche locale basée sur des modèles utilisent des connaissances à priori que l'on possède sur la morphologie d'image et s'appuient en général sur des points caractéristiques de celui-ci. Toutes ces méthodes ont l'avantage de pouvoir modéliser plus facilement les variations de pose, d'éclairage et d'expression par rapport aux méthodes globales. Enfin il existe des méthodes hybrides qui permettent d'associer les avantages des méthodes globales et locales en combinant la détection des caractéristiques géométriques (ou structurales) avec l'extraction des caractéristiques d'apparence locales. **[4]**

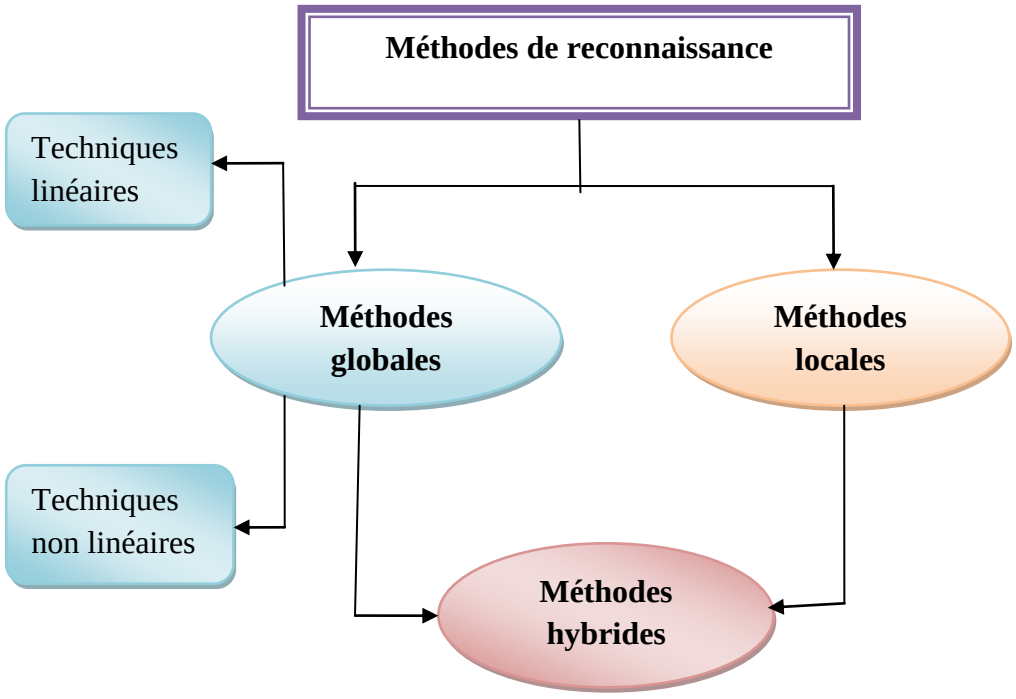


Figure III.1 : Les différentes méthodes d'extraction dans un système de reconnaissance biométrique.

III.4 Histogramme de Gradient Orienté (HOG)

III.4.1 Définition

Un histogramme de gradient orienté (HOG) est une caractéristique utilisée en vision par ordinateur pour la détection d'objet. La technique calcule des histogrammes locaux de l'orientation du gradient sur une grille dense, c'est-à-dire sur des zones régulièrement réparties sur l'image. **[16]** Il définit dans une région les proportions de pixels dont l'orientation du gradient appartient à un certain intervalle. Ces proportions caractérisent la forme présente dans cette région. La méthode s'est montrée particulièrement efficace pour la détection de personnes**. [17]**

III.4.2 Description générale

L'idée importante derrière le descripteur HOG est que l'apparence et la forme locale d'un objet dans une image peuvent être décrites par la distribution de l'intensité du gradient ou la direction des contours. Ceci peut être fait en divisant l'image en des régions adjacentes de petite taille, appelées cellules, et en calculant pour chaque cellule l'histogramme des directions du gradient ou des orientations des contours pour les pixels à l'intérieur de cette cellule. La combinaison des histogrammes forme alors le descripteur HOG. Pour de meilleurs résultats, les histogrammes locaux sont normalisés en contraste, en calculant une mesure de l'intensité sur des zones plus larges que les cellules, appelées des blocs, et en utilisant cette valeur pour normaliser toutes les cellules du bloc. **[16]**

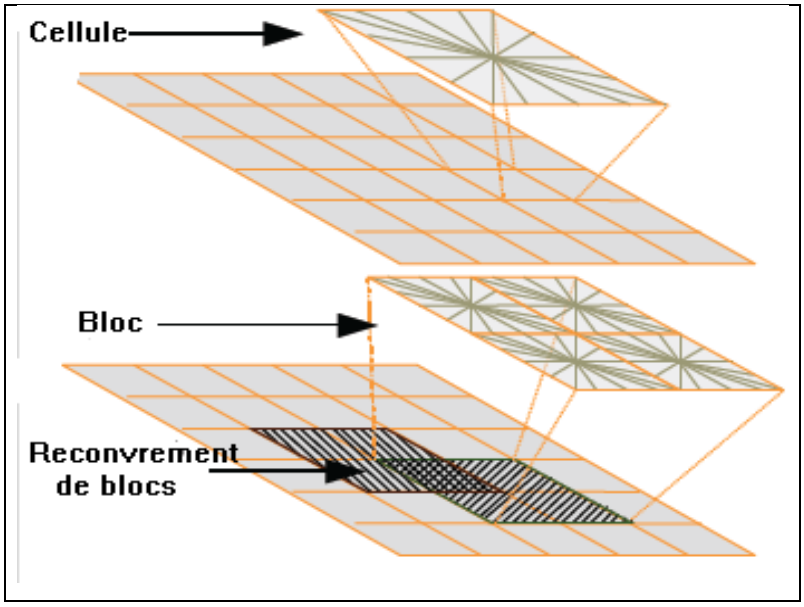


Figure III.2 : Le descripteur de forme locale du HOG

III.4.3 Construction du descripteur

III.4.3.1 Calcul du gradient

Une étape de prétraitement peut être effectuée avant le calcul du gradient, afin que les couleurs de l'image soient normalisées et une correction gamma correcte. Cette étape ne s'est finalement pas avérée nécessaire, la normalisation du descripteur lui-même s'avérant suffisante. La première étape de la méthode est le calcul du gradient, la méthode la plus courante pour cela consistant à appliquer un filtre dérivatif 1-D centré, dans les directions horizontales et verticales. Les masques suivants sont utilisés pour cela : [-1; 0; 1] et $[1;0;1]^T$.

Dans le cas des images couleurs, le gradient est calculé séparément pour chaque composante, et on retient pour chaque pixel le gradient de plus grande norme. D'autres types de masques plus complexes ont été testés, comme des filtres de Sobel (3x3), ou des masques diagonaux, ou non centrés**. [16]**

III.4.3.2 Construction de l'histogramme

La seconde étape est la création des histogrammes de l'orientation des gradients. Ceci est fait dans des cellules carrées de petite taille de (4x4 à 12x12) pixels. Chaque pixel de la cellule vote alors pour une classe de l'histogramme, en fonction de l'orientation du gradient à ce point. Le vote du pixel est pondéré par l'intensité du gradient en ce point. Les histogrammes sont uniformes de 0 à 180° (cas non signé) ou de 0 à 360° (cas signé). Prendre en compte le signe du gradient n'améliore pas les performances pour la détection de personnes, mais peut être significatif pour d'autres types d'objets. **[16]**

III.4.3.3 Formation des blocs

Une étape importante est la normalisation des descripteurs afin d'éviter les disparités dues aux variations d'illumination. Cette étape introduit également de la redondance dans le descripteur. Pour cela, les auteurs regroupent plusieurs cellules dans un bloc, qui est l'unité sur laquelle est effectuée la normalisation. Les blocs se recouvrent, donc une même cellule participe plusieurs fois au descripteur final, comme membre de blocs différents. Deux types de géométrie de blocs sont proposées : rectangulaire (R-HOG) ou circulaire (C-HOG) **(Voir la figure III.3)**. **[16]**

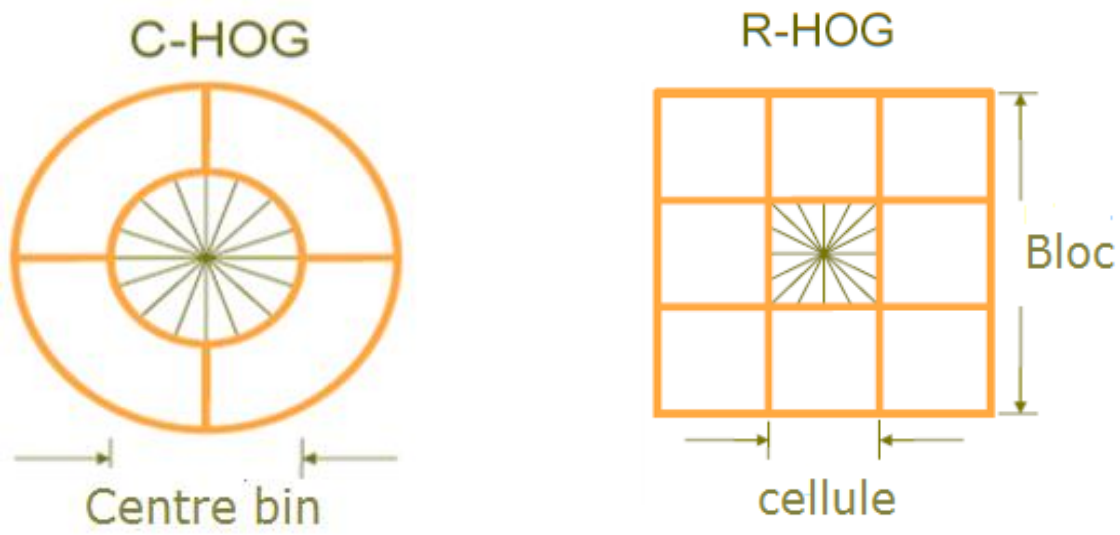


Figure III.3 : Les formes des blocs C-HOG et R-HOG

III.4.3.4 Normalisation des blocs

Selon l'éclairage ou le contraste entre le premier et l'arrière plan, les valeurs des HOGs peuvent varier de façon importante, bien que la personne ait la même posture. Le modèle concerné de la base de données est alors moins proche et le descripteur est alors moins performant.

Afin d'uniformiser les vecteurs de caractéristiques, une normalisation du vecteur de caractéristiques $\mathbf{V_{bloc}}$ est réalisée. Soit **N** la taille du vecteur. Les différentes normalisations testées sont : **[17]**

- **Norme L1** : moyennage par la norme 1 du vecteur

$$\mathbf{V_{bloc}^{L1}(i)} = \frac{\mathbf{V_{bloc}(i)}}{\sum_{K=1}^{N} \mathbf{V_{bloc(k)}}} \qquad \textbf{(III.1)}$$

- **Norme L1sqrt** : la racine carré de la norme L1 est prise afin de traiter le vecteur de caractéristiques comme une densité de probabilité.

$$\mathbf{V_{bloc}^{L1sqrt}(i)} = \sqrt{\frac{\mathbf{V_{bloc}(i)}}{\sum_{K=1}^{N} \mathbf{V_{bloc(k)}}}} \qquad \textbf{(III.2)}$$

- **Norme L2** : moyennage par la norme 2 du vecteur :

$$\mathbf{V_{bloc}^{L2}(i)} = \frac{\mathbf{V_{bloc}(i)}}{\sqrt{\sum_{K=1}^{N} \mathbf{V_{bloc(k)^2}}}}$$

(III.3)

- Norme **2** à hystérésis : des changements non linéaires d'illumination peuvent causer des saturations lors de l'acquisition et provoquer des changements brutaux de magnitude. L'influence des gradients de hautes magnitudes est ici réduite en seuillant à 0,2 après une normalisation L2. Une normalisation unitaire est finalement réalisée pour obtenir la norme L2 à hystérésis. **[17]**

L'algorithme de réalisation du descripteur HOG est réalisé comme suit :

1- Calculer gradient pour chaque cellule.
2- Vote pondéré dans les cellules spatiales et orientation.
3- Calculer le HOG de chaque cellule de la fenêtre.
4- Regrouper des cellules en blocs.
5- Création du vecteur de caractéristiques.
6- Normalisation du vecteur de caractéristiques.

III.5 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).

La première catégorie de distances est constituée de distances Euclidiennes et sont définies à partir de la distance de Minkowski d'ordre **p** dans un espace euclidien (déterminant la dimension de l'espace euclidien). Considérons deux vecteurs

$X = (x_1, x_2, \dots \dots, x_n)$ et $Y = (y_1, y_2, \dots \dots, y_n)$, la distance de Minkowski d'ordre **p** notée L_p est définie par : **[18]**

$$L_P = \left(\sum_{i=1}^{n} (|x_i - y_i|)^p\right)^{1/p} \quad \textbf{(III.4)}$$

III.5.1 Distances Euclidiennes

La distance Euclidienne est une distance géométrique dans cet espace multidimensionnel. Il existe deux distances Euclidiennes :

a - Distance City-Block

Pour **p = 1** on obtient la distance City-Block :

$$L_1(x, y) = \sum_{i=1}^{n} |x_i - y_i| \quad \textbf{(III.5)}$$

b- Distance Euclidienne (L2)

Pour **p = 2** on obtient la distance euclidienne :

$$L_2(x, y) = \sqrt{\sum_{i=1}^{n} |x_i - y_i|2} \quad \textbf{(III.6)}$$

Les objets peuvent alors apparaître de façons très différentes selon la mesure de distance choisie comme montre l'exemple de la **figure III.4** :

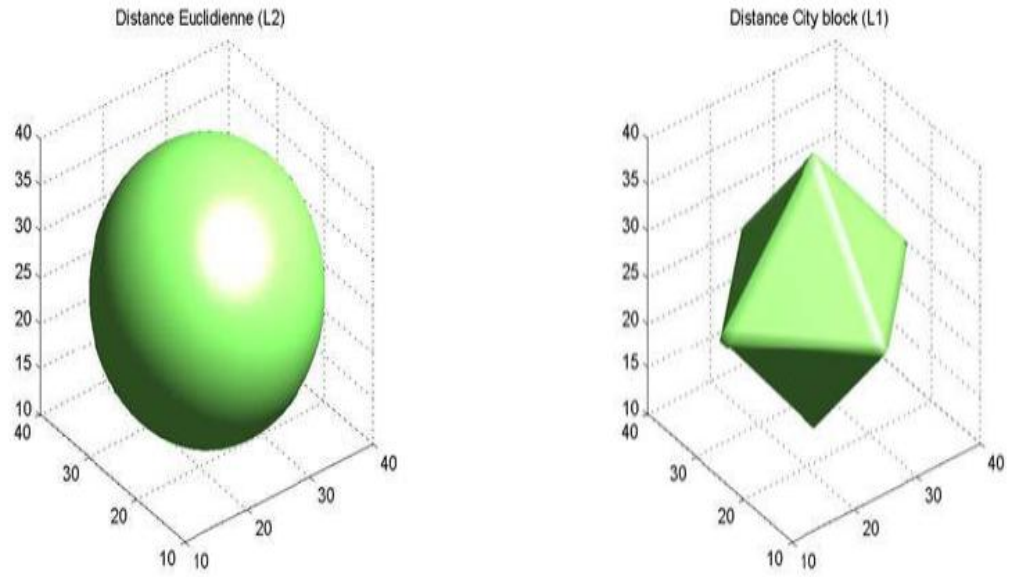


Figure III.4 *:* Représentation d'une sphère avec la distance Euclidienne et la distance City-Block.

III.5.2 La distance intersection d'histogramme

La distance intersection d'histogramme entre deux histogrammes peut être calculée avec la fonction suivant :

$$\mathbf{L(x, y) = \frac{1-\sum_{i=1}^{n} \min(x,y)}{\min\left(\sum_{i=1}^{n}(x),\ \sum_{i=1}^{n}(y)\right)}} \qquad \textbf{(III.7)}$$

Si les histogrammes **x** et **y** ne contiennent pas le même nombre de chiffres, alors cette mesure ne sera pas symétrique. **[19]**

III.6 Conclusion

Dans ce chapitre, nous avions de donné quelques notions et définitions pour l'extraction des caractéristiques et les différentes méthodes utilisées, qui se divisent en trois catégories à savoir les méthodes globales, locales et hybrides. Ensuite, comme pour l'approche pixel, il est nécessaire d'extraire des caractéristiques comme les histogrammes de gradients orientés pour décrire nos objets. Afin d'obtenir une description plus fine de chaque objet. Dans le prochain chapitre, nous allons développer l'application des variantes de l'algorithme du HOG en identification.

CHAPITRE IV

Résultats et discussions

IV.1 Introduction

En observant que le motif de la texture produite par la flexion de l'articulation du doigt est très distinctif, nous présentons un système d'authentification biométrique basée sur l'empreinte du doigt (FKP: Finger-Knuckle-Print). Dans **[5]** un dispositif spécifique d'acquisition de données a été conçu pour capturer les images FKP. La carte convexe locale de direction de l'image FKP a été extraite sur la base du quel le système coordonnée locale est mis en place pour aligner les images et une région d'intérêt est utilisée pour l'extraction de caractéristiques.

Dans ce chapitre, nous allons présenter l'environnement ainsi que le système de reconnaissance FKP, et la base de donnée utilisée. Les résultats de l'application des algorithmes HOG et MB-HOG seront présentés et discutés. Une comparaison de l'application de différentes méthodes de calcul de distances sera aussi examinée.

IV.2 Environnement du travail

Dans cette section, nous présenterons l'environnement matériel et logiciel de notre travail

IV.2.1 Environnement matériel

Afin de mener à bien ce projet, il a été mis à notre disposition un ensemble de matériel dont les caractéristiques sont les suivantes :

– Nom d'ordinateur : Elwaha -Pc

–Groupe de travail : WORKGROUP

– Processeur : Intel® coré(TM) i3-3110M CPU @ 2.40 GHz 2.40 GHz

– RAM : 4.00 Go de RAM

– Type de système : système d'exploitation 32 bits

– OS : Microsoft Windows 7

IV.2.2 Outils de développement

Nous avons eu recours lors de l'élaboration de notre système au logiciel Matlab (8.3.0.532) que nous présenterons ci-dessous.

Matlab est de langage informatique technique à haut niveau et environnement interactif pour le développement d'algorithmes; il est utilisé à des fins de calcul numérique.

Matlab permet de manipuler des matrices, d'afficher des courbes et des données, de mettre en œuvre des algorithmes, de créer des interfaces utilisateurs, et peut s'interfacer

avec d'autres langages comme le C, C++, Java, et Fortran. Il dispose de plusieurs boites à outils en particulier celle du traitement d'images.

IV.3 Système de reconnaissance FKP

Les systèmes biométriques basés sur FKP fournissent des renseignements personnels riches pour la reconnaissance automatique des individus sur la base des lignes principales, les rides et les crêtes du doigt.

Dans notre travail proposé, nous utilisons FKP pour la reconnaissance, car il a tant d'avantages dans le domaine de la biométrie sur les images d'empreintes digitales. On voit que le modèle de la peau sur le doigt porte-fusée est très riche en raison de la texture des plis de la peau et les plis et, par conséquent, peut être considéré comme un identificateur biométrique.

En outre, les avantages de l'utilisation de FKP comprennent facilement accessible, invariant aux émotions et à d'autres aspects comportementaux tels que la fatigue, les caractéristiques stables et l'acceptabilité de la société. Depuis, l'articulation des doigts sera légèrement plié lorsqu'il est capturé. Les modèles de peau inhérents peuvent être clairement capturés et donc les caractéristiques uniques FKP peuvent être mieux exploitées. **[17]**

Le schéma de principe de notre système d'authentification personnelle FKP est montré dans la **(Figure IV.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.

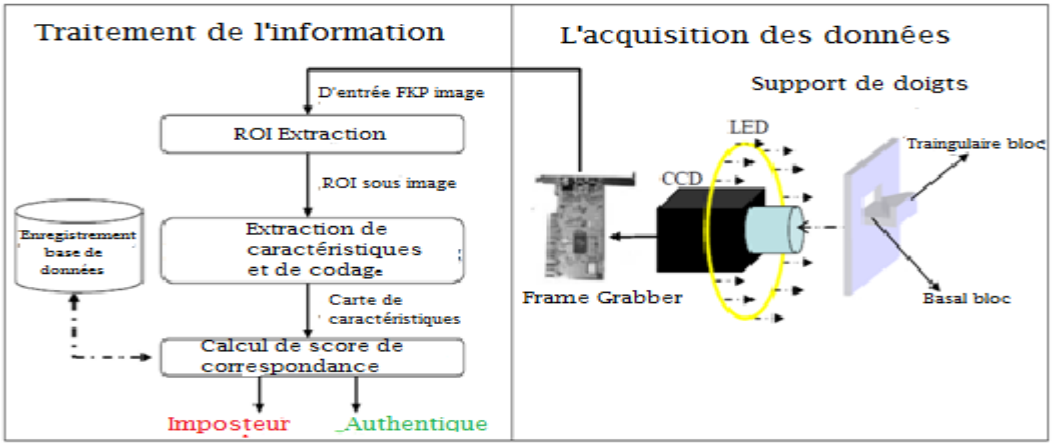


Figure IV.1 : Structure de système d'authentification personnelle à base du FKP.

L'image FKP capturée est envoyé vers le module de traitement de données qui comprend trois étapes de base: extraction de région d'intérêt (ROI), extraction des caractéristiques et codage, et l'appariement ''matching''. **La Figure IV.2** montre un dispositif d'acquisition d'image FKP dont la taille globale est 160mm × 125mm × 100mm. **[18]**

Figure IV.2 : Appareil d'acquisition d'image FKP.

IV.4 La base de données FKP

La base de données FKP se compose de 7920 images des expressions de FKP de 165 personnes distinctes. L'idée de base derrière cette nouvelle modalité est d'utiliser la zone autour des phalanges du doigt comme un trait biométrique **(Figure IV.3)**.

Pour cette base de données, chaque personne est représentée par 48 images de 4 doigts (milieu / index de la main droite et milieu / index de la main gauche). **[19]**

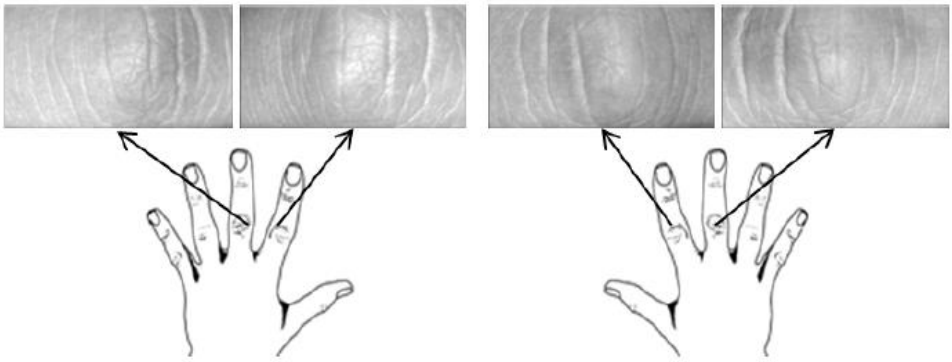


Figure IV.3 : Exemples des images de la base de données FKP

IV.4.1 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'apprentissage 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 effectué la base a été scindée de la façon suivante :

- **Images apprentissages**

La première, la cinquième et la neuvième image de chaque personne servent pour la phase d'apprentissage.

- **Images Tests**

Les neuf 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 présenté, en suivant un protocole de test basé sur la mesure de taux de reconnaissance.

IV .5 Expérimentations sur la FKP

IV.5.1 Protocol de test

Nous avons mis en œuvre un système de reconnaissance à base de l'algorithme HOG avec la modalité FKP. Dans cette expérimentations, il y avait 660 (165 x 4) classes et 1980 (660 × 3) images dans l'apprentissage. Pour obtenir des résultats statistiques, en ajustant la mise en correspondance seuil, un courbe ROC (Receiver Operating Characteristic), qui est la variation du taux de véritable acceptation (GAR) contre taux de faux rejet (FRR) pour tous les seuils possibles, peuvent être créés. Sinon il a été considéré comme une adaptation d'imposteur, est le taux d'erreur égal (EER). La courbe ROC peut refléter la performance globale d'un système biométrique.

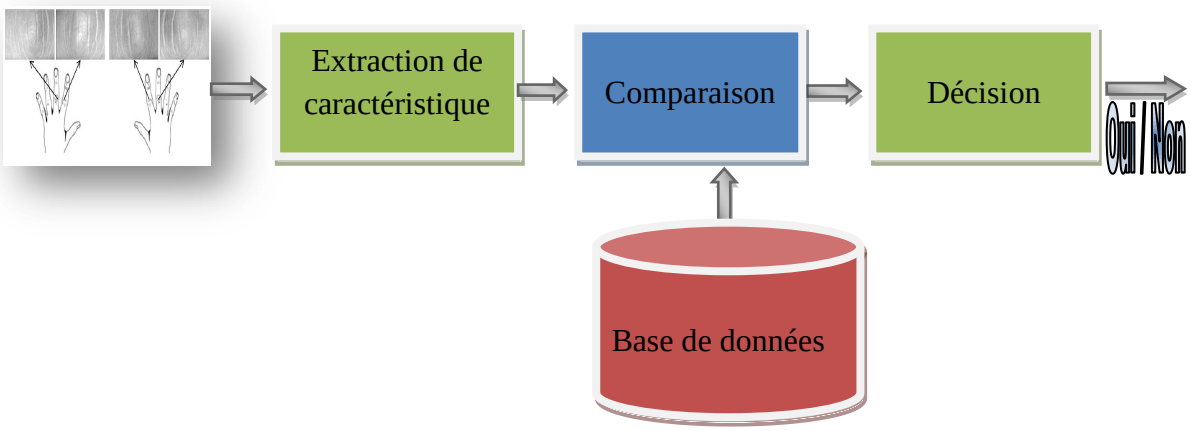


Figure IV .4 : Un système biométrique uni modale

Afin de montrer et expliquer la performance du système proposé clairement, quatre expérimentations ont été menées. Dans chaque expérimentation, nous avons évalué et comparé les performances codage des méthodes d'extraction de caractéristiques sur la base de données FKP

1- Première expérimentation

Dans un premier temps, nous avons mis en œuvre un système de reconnaissance en appliquant l'algorithme de HOG sur la modalité FKP de 4 type de doigts l'index gauche et l'index droit, milieu gauche et milieu droit de chaque personne.

2- Deuxième expérimentation

Dans le deuxième temps, nous avons mis en œuvre un système de reconnaissance à partir des meilleurs résultats obtenu de première expérimentation, nous appliquons l'algorithme du HOG en MB-HOG. Il dispose de 6 blocs.

3- Troisième expérimentation

Dans un troisième temps, nous avons réalisé la fusion au niveau des scores des algorithmes de MB-HOG de l'index gauche avec milieu gauche et l'index droit avec milieu droit, en suit on va fusionner les résultats obtenu dans la fusion des quatre doigts.

4- Quatrième expérimentation

Dans le quatrième temps, nous avons comparés les résultats de système de reconnaissance à partir la variation de la distance dans le module de comparaison dans le meilleur système.

IV.5.2 Résultats expérimentales et interprétation

IV.5.2.1 Les résultats obtenus dans la première expérimentation

A la fin de l'exécution l'algorithme d'évaluation de HOG, nous avons réalisé **le tableau IV .1** ci-après qui contient les résultats obtenus et les taux GAR et FRR, EER et Threshold. Avec **GAR** = **1- FRR**.

Tableau IV.1 : Les résultats obtenus par l'algorithme de HOG

	Type des doits	FRR(%)	GAR(%)	EER(%)	Threshold
HOG	L'index gauche	**10.1010**	**89.8990**	**3.03**	**0.1509**
	L'index droit	**9.1582**	**90.8418**	**2.896**	**0.1355**
	Milieu gauche	**10.2357**	**89.7643**	**2.626**	**0.148**
	Milieu droit	**9.8316**	**90.1684**	**2.694**	**0.166**

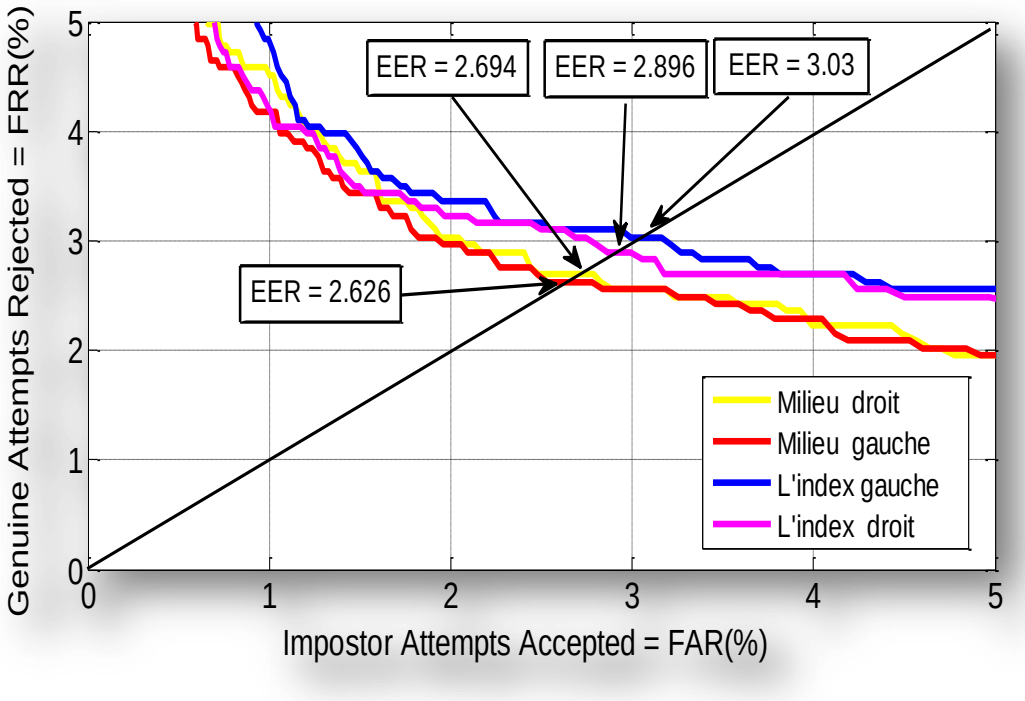


Figure IV. 5 : La courbe ROC du HOG appliqué aux doigts gauche et droit.

Les résultats expérimentaux montrent que le HOG donne meilleurs résultats avec le doigt milieu gauche. En termes de valeur moindre dans l'EER. Ce qui conduit par conséquent à un résultat que les variations de la pose des doigts de la main droit sont moins sévères que celle de la main gauche. Des variations remarquables de poses des doigts causeraient des déformations graves entre deux images FKP du même doigt, qui conduisent à plus de défini à la reconnaissance FKP.

IV.5.2.2 Les résultats obtenus dans la deuxième expérimentation

Après l'exécution l'algorithme de MB- HOG avec 6 blocs. Nous avons réalisé le **tableau IV.2**

Tableau IV.2 : Les résultats obtenus par l'algorithme de MB-HOG

	Type de doit	NB	FRR(%)	GAR(%)	EER(%)	Threshold
MB-HOG	Milieu gauche	1	10.2357	89.7643	2.626	0.148
		2	4.0404	95.9596	1.491	0.1489
		3	3.1650	96.8350	0.8754	0.1468
		4	3.3670	96.6330	1.212	0.185
		5	6.0606	93.9394	1.791	0.1895
		6	7.4074	92.5926	2.626	0.225

La courbe du ROC est montrée par **la Figure IV.6**

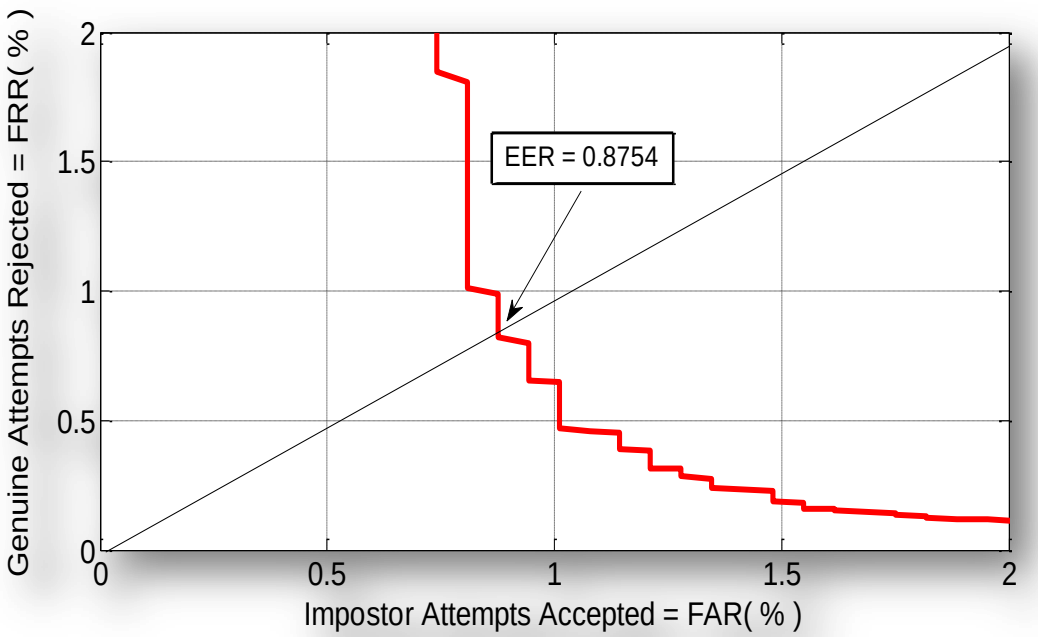


Figure IV.6: La courbe ROC de l'application du MB-HOG au doigt milieu gauche avec 3 blocs.

Après l'exécution de l'algorithme de MB-HOG, nous avec remarqué les bons résultats dans ces de 3 blocs où l'erreur EER est inférions à 0.78.

IV.5.2.3 Les résultats obtenus dans la troisième expérimentation

Nous avons testé différents systèmes de fusion des doigts avec les deux règles de fusion. Les résultats sont présentés dans **le tableau IV.3**

Tableau IV.3 : Les résultats obtenus par la fusion des doigts de main.

	Type des doits	EER(%)	Threshold
MB_HOG	Index gauche et milieu gauche	**0.0274**	**0.1159**
	l'index droit et milieu droit	**0.1347**	**0.1675**
	index gauche et milieu gauche, l'index droit et milieu droit	**0.000**	**0.014**

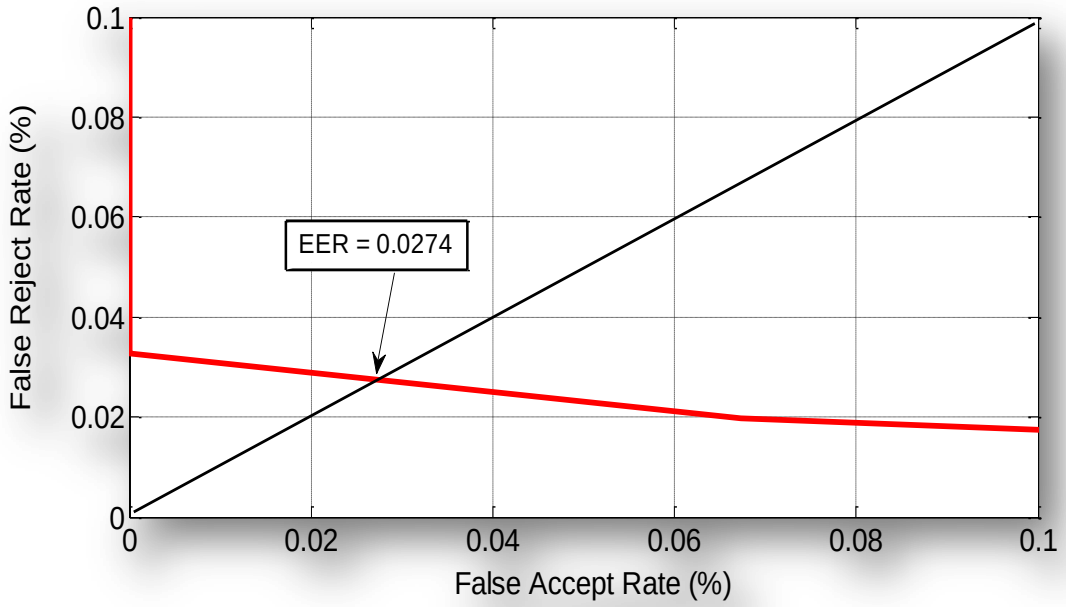


Figure IV. 7 : La courbe ROC de la fusion de l'index gauche et milieu gauche.

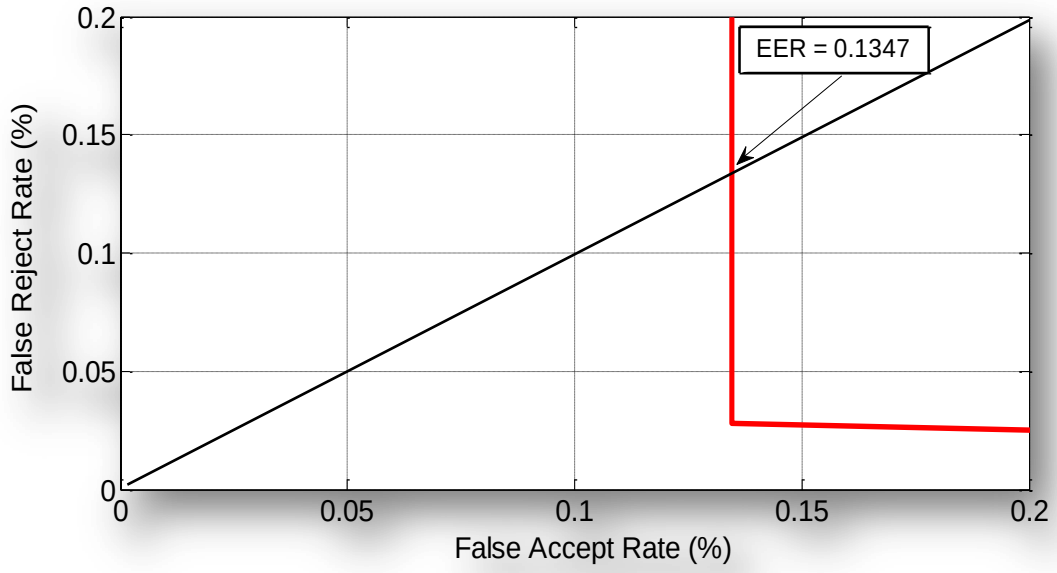


Figure IV. 8 : La courbe ROC de la fusion de l'index droit et milieu droit.

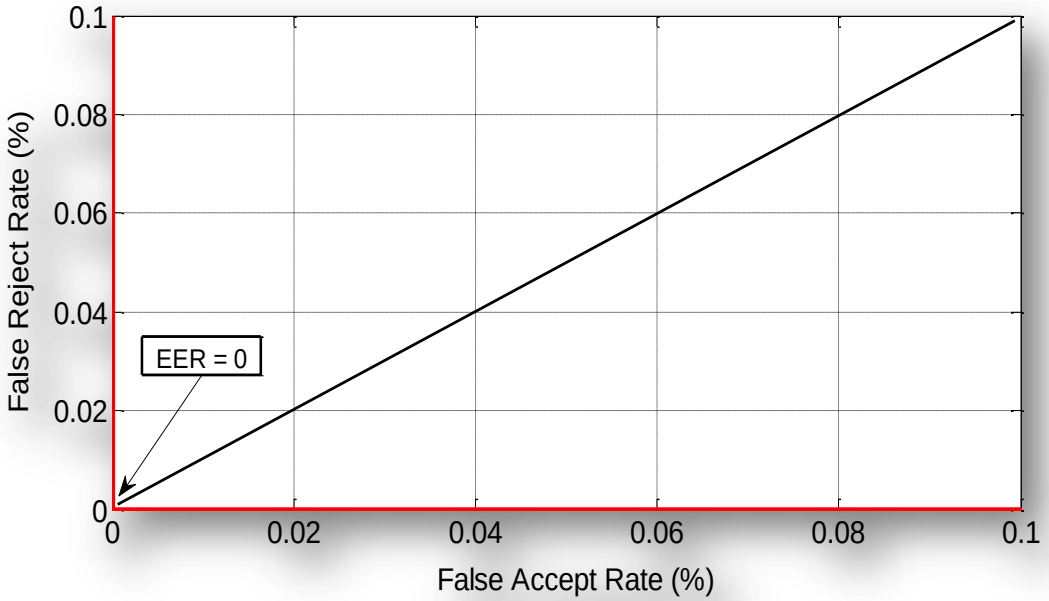


Figure IV. 9: La courbe ROC de la fusion de l'index droit et milieu droit, l'index gauche et milieu gauche.

On remarque que par l'intégration des informations à partir de plusieurs doigts performances de reconnaissance améliorées sont largement.

IV.5.2.4 Les résultats obtenus par quatrième expérimentation

Dans cette étape, nous examinons les performances du système biométrique en utilisant MB-HOG pour l'extraction des caractéristiques avec 3 blocs. Pour la comparaison nous utilisons plusieurs méthodes de distance. Les résultats obtenus sont regroupés dans **le tableau IV.4**. Les courbes des erreurs sont présentées dans **la Figure (IV.10)**.

Tableau IV.4: Les résultats obtenus pour différentes méthodes de distance.

Type	GAR(%)	FRR(%)	EER(%)	Threshold
Euc dist	96.8350	3.1650	0.8755	0.1468
Sq dist	96.8350	3.1650	0.8830	0.0938
Corr dist	96.8350	3.1650	0.8830	0.0938
Angle	96.8350	3.1650	0.8754	0.146
Quad diff	96.8350	3.1650	0.8831	0.0938
Max diff	79.1246	20.8754	5.262	0.147
Min diff	1.8182	98.1818	38.37	0.0767
Minkowski	95.4209	4.5791	1.2	0.1382
Intersect dis	97.8451	2.1549	0.5388	0.1269
Chisq	98.0471	1.9529	0.6734	0.109
Kldiv	7.1380	92.8620	18.79	0.1747
Jeffrey	98.0471	1.9529	0.6734	0.1019

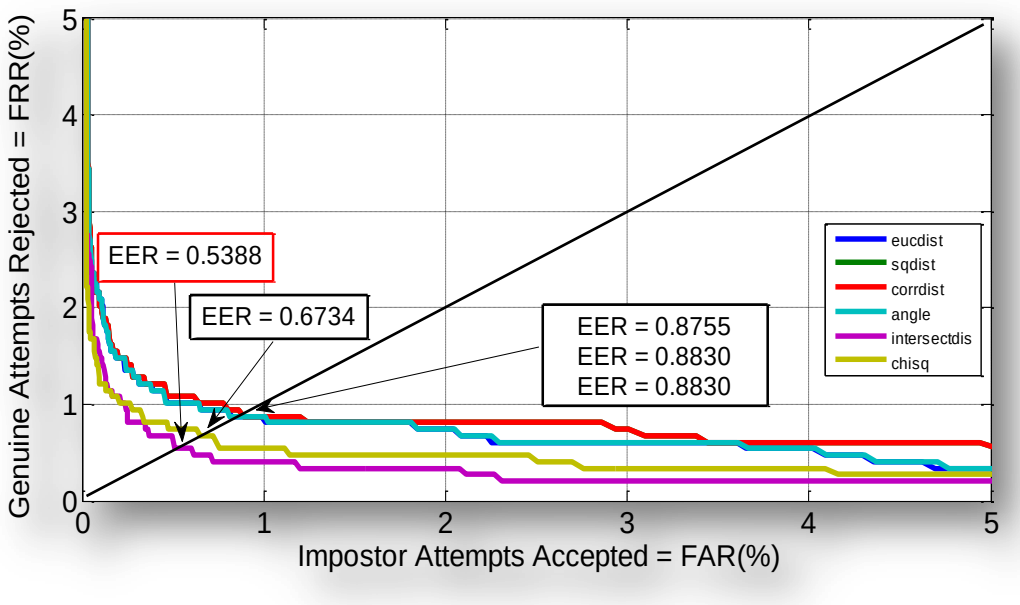


Figure IV. 10 : La courbe ROC de la mesure des certains distances de MB-HOG avec le nombre-bloc 3

IV.6 Discussion

Le doigt milieu gauche donne une meilleure erreur EER par rapport à l'autre modalité. Ceci est dû au fait que Le milieu gauche capte quelques structures de veine d'articulation de doigt. Ces informations additionnelles permettent de bien différencier les différentes identités.

L'utilisation de la méthode multi-blocs améliore les résultats du HOG. Cela est vrai vu que la caractérisation est effectuée selon des zones (ou blocs). Le chevauchement des blocs assure la liaison entre les vecteurs associés aux blocs pour refléter à la fin une même identité. Les tailles des vecteurs extraites par HOG est de 81, cependant celui du MB-HOG (3 blocs) est de 729 ce qui produit avec une meilleure résolution.

En vue d'améliorer en plus nos résultats, nous allons essayer de fusionner les différent scores des différentes échantillons afin d'obtenir un système multimodal.

Les erreurs dans le cas des doigts gauche sont inférieures (EER = 0.0274), cependant la fusion des scores des deux modalités gauche et droite améliore nettement cette erreur (EER< 0.0009) ce qui est négligeable.

Pour la décision, l'application de la méthode de distance « intersect dis » montre des meilleurs résultats. L'erreur EER est réduite à 0.5388%.

IV.7 Conclusion

Dans ce chapitre, nous concluons avec les résultats obtenus que l'approche appliquée d'identification biométrique en utilisant les articulations des doigts (FKP) avec l'application des algorithmes de HOG.

Les erreurs EER ont été considérablement améliorées via le choix des paramètres des différents modules dans le système biométrique. Avec la méthode de distance « intersect dis », la fusion des scores des deux modalités doigts gauche et droite donne des très bon résultats dans le cas de l'algorithme MB-HOG.

Conclusion général

Conclusion générale

Dans ce travail, nous avions développé l'application de variantes de l'algorithme de l'histogramme du gradient orienté (HOG) pour l'identification des personnes où nous avions utilisé les empreintes des articulations des doigts comme modalité.

Dans une première étape, cet algorithme consiste à quantifier en direction (en orientation) et en module les variations de l'intensité des pixels porteurs d'information ensuite à partager les points, selon des classes d'orientation, et à sommer les modules des points de chaque classe (intraclasse). L'ensemble de ces valeurs constituera le vecteur caractéristique de l'empreinte.

Les résultats obtenus montrent l'efficacité de l'algorithme du HOG dans l'identification des personnes. L'erreur EER était de moins de 2.626% dans le cas des doigts gauches. Cependant, une nette amélioration a été présentée avec l'application de la variante multi blocs (MB-HOG). Ici, la partition de l'image en plusieurs zones a permis de réduire cette erreur à moins de 0.8754% dans le cas de 03-blocs. Même que chaque bloc possède son propre vecteur caractéristique, c'est grâce au recouvrement (chevauchement) de ces blocs que le simple assemblage de ces vecteurs produit un unique vecteur représentatif qui identifie mieux la personne.

La multi-modalité biométrique a été appliquée en fusionnant au niveau des scores les deux modalités doigts gauches et doigts droites avec une mesure de distance par la méthode Min-Max. Une erreur EER nulle a prouvé sa très grande efficacité de ce choix.

L'application de différents mesure de distance a montré la relative supériorité de la norme « intersect dis ».

D'après l'étude effectuée, nous constatons bien que la méthode du HOG ou MB-HOG, se base sur la simple sommation des modules selon les classes prédéfinies par l'orientation du gradient. Ainsi, nous proposons d'expérimenter l'inverse, en examinant le classement des points dans un bloc selon le module et non l'orientation et de trouver une fonction d'agrégation entre les modules de cette classe au lieu de la fonction somme.

Résumé

Biométrique d'authentification personnelle est une méthode efficace pour reconnaître automatiquement, avec une grande confiance, l'identité d'une personne. En observant que le motif de la texture produite par la flexion de l'articulation du doigt est très distinctif, dans cet article, nous présentons un nouveau système d'authentification biométrique à l'aide du doigt-Knuckle-Print (FKP) imagerie.

Pour correspondre deux FKPs, un système d'extraction de caractéristiques combine l'orientation et l'ampleur des informations en utilisant la méthode de l'histogramme du gradient orienté. La base de données FKP qui se compose de 7920 images de 660 doigts différents est mise en place pour vérifier l'efficacité du système proposé et on obtient des résultats prometteurs. Le système proposé FKP atteint le taux de reconnaissance beaucoup plus élevé.

Abstract

Biometric personal authentication based is an effective method to automatically recognize, with great confidence, the identity of a person. To match two FKPs, a feature extraction system that combines the orientation and extent of the information using the method of the histogram of oriented gradient. A proposed FKP database that consists of 660 images of 7920 different fingers is set up to check the effectiveness of the proposed system and promising results are obtained. The proposed system FKP reached much higher recognition rate. It provides a practical solution to the of finger-based biometric systems.

ملخص

المصادقة البيومترية هي وسيلة فعالة للتعرف آليا على هوية الأشخاص بطريقة ناجعة.

للمطابقة بين نموذجان لبصمة الأصابع , نقدم نظام استخراج الخصائص.يقوم بتركيب معلومات تخص اتجاه و شدة التغير في الصورة و ذلك باستخدام طريقة الرسم البياني للتدرج الموجه. لهذا الغرض نستخدم قاعدة بيانات لصور مفاصل الأصابع و التي تحوي 660 صورة ل 7920 لأصابع مختلفة من اجل التحقق من فعالية النظام المقترح و قد تحصلنا عل نتائج واعدة. النظام المقترح اثبت نسبة عالية في تحديد الهوية و هو بذلك يقدم حل عملي إضافي لأنظمة التعرف البيومترية.

.

Bibliographie

[1] A. Nait-Ali, Régis fournier, << Traitement du signal et de l'image pour la biométrie >>, L'ouasir, 2012.

[2] A. Ben Khalif et F. Abes, << Identification d'individus par reconnaissance d'empreintes palmaires >>, Mémoire de fin d'étude, Université Kasdi Merbah, Ouargla, 2008.

[3] S. Akrouf, << Une approche multimodale pour l'identification du locuteur >>, Thèse de Doctorat, Université Ferhat Abbas, Setif, 2011.

[4] S. Boudjellal, << Détection et identification des personnes par méthode biométrique >>, Mémoire de Magister, Université Mouloud Mammari, Tizi-Ouzou

[5] O. Moulay Brahim et M. Arbaoui, << Identification des personnes par les articulations des doigts >>, Mémoire de Master, Université Kasdi Merbah, Ouargla, 2015.

[6] S. Guerfi Ababsa, << Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D >>, Thèse de Doctorat, Université d'Evry Val d'Essonne, 2008.

[7] H. Guesmi, << Identification de personnes par fusion de différentes modalités biométriques >>, Thèse de Doctorat, Université de Rennes, French, 2014.

[8] N. Morizet, << Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris >>, Thèse de Doctorat, Paris, 2010 https://pastel.archives-ouvertes.fr/pastel-00005811

[9] L. Allano**,** << La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles >>, Thèse de doctorat, Université d'Evry Val d'Essonne, 2009.

[10] Chapitre 4 Méthodes de Fusion et Normalisation. http://thesis.univbiskra.dz/944/7/Chap%204%20M%C3%A9thodes%20de%20Fusion.pdf. 10/03/2016, 19 :23.

[11] Vérificateurs biométriques Introduction http://users.utcluj.ro/~elupu/Curs/fileloader.php?fileName=upload/Cursuri/Traitement_de_la_parole/C11/ASRSV11_F.pdf. 07/14/2016, 21:17.

[12] I. Dehache et L. Souici-Meslati, << Une approche multimodale pour la vérification biométrique >>, Université Badji Mokhtar, Annaba, 2011

[13] A Chaari, << Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée >>, Thèse de Doctorat, Université d'Evry Val d'Essonne, 2010

[14] Chapitre 1 Système de Reconnaissance de Visage. http://thesis.univbiskra.dz/944/4/Chap%201%20Syst%C3%A8me%20RV%20sept%2012.pdf. 24/04/2016, 10:11.

[15] A. Harrag, << Extraction des données d'une base: application a l'extraction des traits du Locuteur >>, Thèse de Doctorat, Université Ferhat Abbas, Setif, 2011.

[16] https://fr.wikipedia.org/wiki/Histogramme_de_gradient_orient%C3%A9. 07/03/2016, 17 :45.

[17] C. Migniot, << Segmentation de personnes dans les images et les vidéos >>, Thèse de Doctorat, Université de Grenoble, Français, 2012.

[18] A. Bettahar et F. Saber, << Extraction des caractéristiques pour l'analyse biométrique d'un visage >>, Mémoire de Master, Université Kasdi Merbah, Ouargla, 2014

[19] M. Stokely, << HistogramTools for Distributions of Large Data Sets >>, Version 0.3.2 as of July 29, 2015.

[20] E. Perumal et S. Ramachandran, << A Multimodal Biometric System Based on Palmprint and Finger Knuckle Print Recognition Methods >>, India, 2015

[21] L. Zhang, D. Zhang and H. Zhu, << Online Finger-Knuckle-Print Vérification for Personal Authentication >>, The Hong Kong Polytechnic University

[22] C. Moujahdi, << Protection des systèmes de sécurité biométriques contributions à la protection des modèles biométriques >>, Thèse de Doctorat, Université Mohammed V – Agdal, Rabat, 2014.