République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

ECOLE NATIONALE POLYTECHNIQUE

DÉPARTEMENT D'ÉLECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention du diplôme d'Ingénieur d'Etat en Electronique

Thème :

Conception d'un système biométrique FKP

Encadré par :

Mme L.HAMAMI

Mr H.BOUCENNA

Réalisé par :

Mlle Nadjla BETTAYEB

Mlle Razika BOUZAR

Promotion : Juin 2013

Remerciement

Que Dieu soit loué pour nous avoir permis d'arriver au terme de ce travail.

Nous remercions et exprimons notre reconnaissance à quiconque ayant allumé une bougie dans le chemin de la science et ayant occupé les tribunes du savoir pour nous éclairer.

Nous tenons aussi à exprimer nos remerciements et notre gratitude à :

- Notre encadreur, Pr. HAMMAMI pour avoir dirigé ce travail jusqu'à son terme, pour le temps qu'elle nous a consacré et pour ses précieux conseils.

- Les Membres du jury, Pr GURTI et Mr SAADAOUI, pour l'enrichissement de cette recherche à travers leurs bénéfiques remarques et orientations conséquentes.

- Mr AISSANI, pour l'aide qu'il nous a apporté, et pour nous avoir fait bénéficier de son savoir-faire et pour sa disponibilité.

- Nous remercions également tous les enseignants de l'Ecole Nationale Polytechnique, et spécialement ceux des départements des Sciences Fondamentales et d'Electronique, pour leur apport en savoir

Nous remercions enfin tous nos collègues plus particulièrement : Fatima, Amine, Zineb, Chams-Edin, Nesrine, Abde-Elhak, Ryana et Ahmed qui sans eux nos expériences ne serons jamais terminé et tous ceux qui nous ont aidées, de près ou de loin, ne serait-ce qu'à travers leurs encouragements.

DEDICACE

A celle qui m'a consacré tout son cœur, jusqu' à ses battements incessants, tout son espoir qui se compte en termes de soupirs infinis, Mon Ange qui, jamais ne se plaint, ne demande de contre-partie, à part que je sois comme elle a tant espéré. A celle qui n'a jamais cessé de prier Dieu pour que tous mes pas soient couronnés de succès et mes vœux soient exaucés. A celle qui a assumé pleinement sa responsabilité à mon égard. Je lui souhaite longue et heureuse vie.

Ma mère…

A celui qui s'est incliné pour ma droiture, qui s'est donné tant de mal pour ma dignité, qui m'a appris que mon aise ne se réalise qu'à travers tant d'efforts fournis de ma part, qui m'a fait connaître que le savoir n'est complet qu'en lui adjoignant la morale. A celui qui a été et restera mon soutien inépuisable me permettant de franchir tous les obstacles passés et futurs. A celui qui a illuminé mon chemin.

Mon cher PAPA…

A ceux qui étaient toujours en ma compagnie, cheminant ensemble les divers domaines et les sentiers de la vie. A ceux qui sans eux la vie n'est pas meilleure.

Lamiya et Abdenour…

A tous les membres de ma grande famille, BETTAYEB ET BOULIFA.

A qui ont partagé avec moi les bons comme les mauvais moments de la vie, les douleurs comme l'espoir, celles qui m'ont côtoyé durant les meilleures périodes de la vie, mes chères amies et surtout : Zineb, Imene, nesrine et Khaoula.

A celle qui a partagé avec moi la charge de ce travail et a beaucoup supporté ma paresse, mon binôme Razika.

A tous mes collègues de l'école nationale polytechnique, à tous ceux qui ont marqué ma vie grâce aux bons souvenirs qu'ils y ont laissés.

A tous ceux-là, je dédie ce fruit de mes efforts.

نجلاء

Dédicace

Je dédie ce travail à celle qui m'a donné la vie, le symbole de tendresse, qui s'est sacrifiée pour mon bonheur et ma réussite, qui m'a éclairé mon chemin et qui m'a encouragé et soutenue toute au long de mes études, à ma mère...

A mon père, qui a veillé tout au long de ma vie à m'encourager, à me donner l'aide et me protéger...

Que dieu les garde et les protège

A mon frère jumeau Mohamed Ali...

A mes adorables sœurs Mounira, Fouzia et Aicha...

A mon neveu Ahmed...

A MES AMIS...

A celle qui a partagé avec moi la charge de ce travail et a beaucoup supporté ma paresse, mon binôme Nedjla...

A tous ceux qui me sont chers...

RAZIKA

ملخص: تصميم نظام بيومتري FKP

مع التطور التكنولوجي الكبير الذي يشهده عصرنا الحالي عرف المجال البيومتري تطورا كبيرا من ناحية كفاءة وفعالية الانظمة او من ناحية التقنيات البيومترية المستعملة ، ونتطرق في هذه المذكرة إلى دراسة احدى هذه التقنيات البيومترية الحديثة ألا وهي (FKP) التي تعتمد على دراسة بصمة مفصل الاصبع ، ولتقييم فعالية هذه التقنية قمنا بتطبيق خوارزميتين تعتمدان على خاصية الترميز (CompCode et ImCompCod & MagCode) لاستخلاص خصائص صور بصمات المفصل والمقارنة بين هاتين الخوارزميتين . وقد تمت محاكاة هذه الدراسة في برنامج MATLAB كما قمنا ايضا بإنشاء واجهة تعريفية وتحقيقية لاختبار سيرورة النظام .

الكلمات المفتاحية : صور ، بصمة مفصل الاصبع ، MATLAB ، CompCode، ImCompCod&MagCode

Résumé : Conception d'un système biométrique FKP

Avec le développement technologique, le domaine de la biométrie a connu un grand essor que ce soit au niveau des performances des systèmes ou des techniques biométriques. Dans ce mémoire, on va étudier une des techniques biométriques récentes, la «FKP » qui consiste à différencier entre les personnes en se basant sur les empreintes de l'articulation du doigt. Pour évaluer cette technique nous avons appliqué deux algorithmes issus des méthodes basées codage (CompCode, ImCompCod & MagCode) pour l'extraction des caractéristiques des images FKP et la comparaison entre ces algorithmes. Cette étude a été simulée sur MATLAB. Nous avons aussi construit une interface d'identification et de vérification pour tester la marche à suivre par le système.

Mots clés : images, empreinte de l'articulation du doigt, MATLAB, CompCode, ImCompCod & MagCode.

Abstract: Design of a biometric system FKP

Due to the development of science and technology nowadays, the biometric field has known a great evolution in both system performance and biometric techniques. In this thesis, we are going to deal with one of the recent techniques which is called the (FKP: Finger Knuckle Print) that identifies people based on their knuckle print. To evaluate the precision of its performance, we had applied two coding based algorithms, which are :(CompCode, ImCompCode & MagCode) to extract the features of the FKB images and compare these algorithms ,this study was simulated on MATLAB program , we also make an identification and verification interface to test the system

Key words: images, Finger Knuckle Print, MATLAB, CompCode, ImCompCod & MagCode

Liste des Abréviations

BL-POC: Band-Limited Phase Only Correlation
CCD: Charge Coupled Device
CMC: Cumulative Match Characteristic
DCT: Discrete Cosine Transform
DET: Detection Error Tradeoff
EER: Equal Error Rate
FAR: False Acceptation Rate
FKP: Finger Knuckle Print
FRR: False Rejection Rate
LDA: Linear Discriminant Analysis
LED: Light Emitting Diode
LI: Left Index
LPP: Locality Preserving Projections
LM: Left Middle
MMDA: Multi-Manifold Discriminant Analysis
OCLPP: Orthogonal Complex Locality Preserving Projections
OLDA: Orthogonal Linear Discriminant Analysis
PCA: Principal Component analysis
PHT: Probabilistic Hough Transform
POC: Phase Only Correlation
RANSAC: Random Sample Consensus
RI: Right Index
RM: Right Middle
ROC: Receiver Operating Characteristic
ROI: Region of Interest
RVB: Rouge, Vert et Bleu
SURF: Speeds-Up Robust Features
UID: User IDentification
WER: Weighted Error Rate

Liste des Figures

Liste des Tableaux

Table des matières

Introduction générale

La biométrie, qui est la discipline permettant de reconnaître l'identité d'une personne à partir de ses caractéristiques physiologiques ou comportementales, a attiré et attire encore plus l'attention dans la dernière décennie à cause de l'accroissement du besoin sécuritaire dans plusieurs domaines et en raison de ses nombreuses applications qui offrent plusieurs avantages par rapport aux techniques classiques de reconnaissance comme les clés, les mots de passe, les cartes, etc. qui sont exposés au vol, à la perte ou à la falsification.

De nos jours et avec le développement technologique, plusieurs techniques biométriques ont été découvertes ou utilisées comme : l'iris, la voix, le visage, la dynamique de frappe au clavier, l'ADN, etc. Chacune de ces modalités biométriques a ses propres avantages et inconvénients. Ainsi, les chercheurs n'ont jamais cessé de rechercher de nouveaux types d'identificateurs biométriques dans le but d'améliorer les systèmes existants pour satisfaire nos besoins.

La FKP Finger-Knuckle-Print, qui se réfère à la texture de la surface extérieure autour de l'articulation des phalanges du doigt, est l'une des techniques les plus récentes qui a vu le jour dans les années 2000 et qui a donné de bons résultats par rapport aux autres techniques. Dans ce travail, nous présentons un nouveau système d'authentification biométrique à base d'images FKP, nous allons ainsi l'étudier, le concevoir et le tester.

Ce mémoire sera réparti en quatre chapitres :

Dans le premier chapitre, on donnera quelques notions fondamentales sur la biométrie. On présentera tout d'abord les systèmes biométriques en s'intéressant à leurs architectures et performances. Par la suite on fera une étude comparative des différentes modalités biométriques qui existent.

Dans le second chapitre, un état de l'art de la FKP sera fourni. Ce chapitre sera consacré à une étude comparative des différents algorithmes utilisés dans cette technique biométrique.

Le troisième chapitre fera l'objet d'une étude théorique des méthodes basées codage (coding based-method) en exposant les différents algorithmes utilisés et leurs principes. Une description du système conçu dans notre projet sera donnée en explicitant les différentes étapes suivies.

Le quatrième et dernier chapitre donne les résultats obtenus par le système biométrique réalisé. La programmation et la simulation seront faites sur «Matlab» pour la validation et l'évaluation des performances du système de reconnaissance.

Chapitre 1 La biométrie

1. INTRODUCTION

De nos jours, le développement économique, culturel et technologique et le besoin de sécurité pour protéger nos affaires de façon sûre et efficace nous ont poussés à utiliser la biométrie comme moyen d'identification à la place des anciens moyens comme les clés ou les cartes qui sont exposées au vol, à la perte et à la falsification. La biométrie a montré ses avantages par rapport aux anciens systèmes. C'est pourquoi elle est utilisée de plus en plus largement dans le domaine privé ainsi que dans le secteur public.

Qu'est-ce que l'on entend par la biométrie ? Quelles sont ses différentes technologies ? De quoi se compose un système biométrique ? Enfin, quels sont les applications et les contraintes de cette technique ? C'est ce que nous présenterons dans ce premier chapitre.

2. DEFINITION [1]

La biométrie recouvre l'ensemble des procédés et des technologies tendant à l'identification et l'authentification de l'individu à l'aide de ses caractéristiques morphologiques (Odeur, sang, ADN, cheveux,…etc.), physiologiques (empreintes, forme de la main, forme du visage ou de l'iris,…etc.) ou comportementales (dynamique de signature, dynamique de frappe sur un clavier, parole, démarche…, etc.). Ces caractéristiques qui permettent la reconnaissance des personnes sont appelées « modalités biométrique». Les données biométriques sont par définition uniques et propres à chacun : elles ne peuvent donc pas être oubliées, copiées, contrefaites ou volées !

3. ARCHITECTURE D'UN SYSTEME BIOMETRIQUE [2]

Un système biométrique est un système qui possède en entrée l'acquisition des données biométriques à partir d'un appareil de mesure (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité,…etc.). Il extrait l'ensemble des caractéristiques à partir des données acquises et les compare avec celles enregistrées dans la base de données.

Selon le contexte d'application, on distingue deux modes d'utilisation distincts d'un système biométrique : le mode d'identification et le mode de vérification.

- **Mode d'identification :** ce mode implique l'identification d'une personne parmi un ensemble composé de N individus. A l'aide de la base de données disposée dans le système biométrique, on compare les données fournies par l'utilisateur avec celles contenues dans la base afin de trouver la personne correspondante.

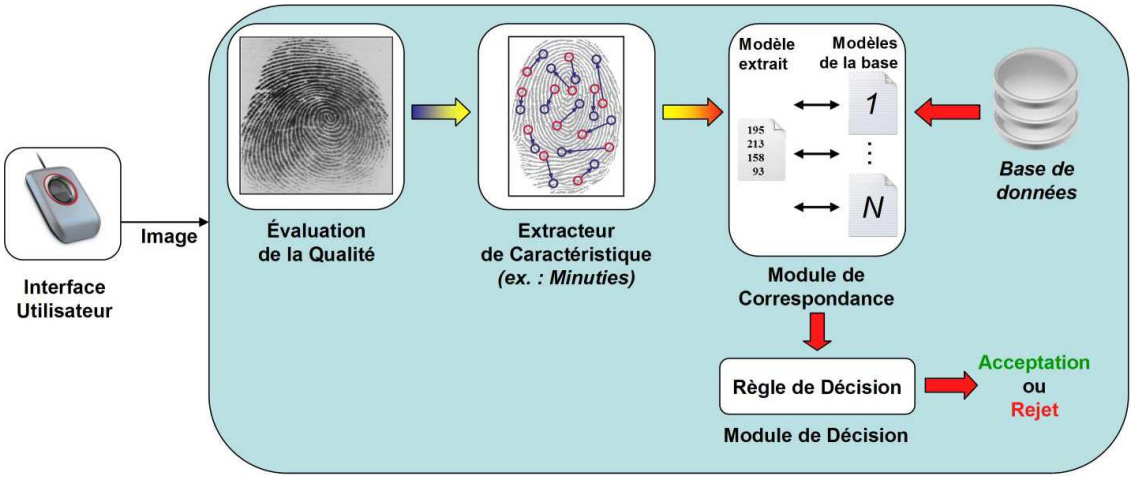


Figure 1.1 Identification d'une personne dans un système biométrique

- **Mode de vérification :** ou d'authentification, ce procédé est plus simple. L'utilisateur doit fournir une donnée et un identifiant. Le système valide l'identité d'une personne en comparant la donnée contenue dans la base de données biométriques correspondante à l'identifiant avec celle de l'utilisateur. Un tel système devra simplement prendre une décision d'acceptation ou de rejet.

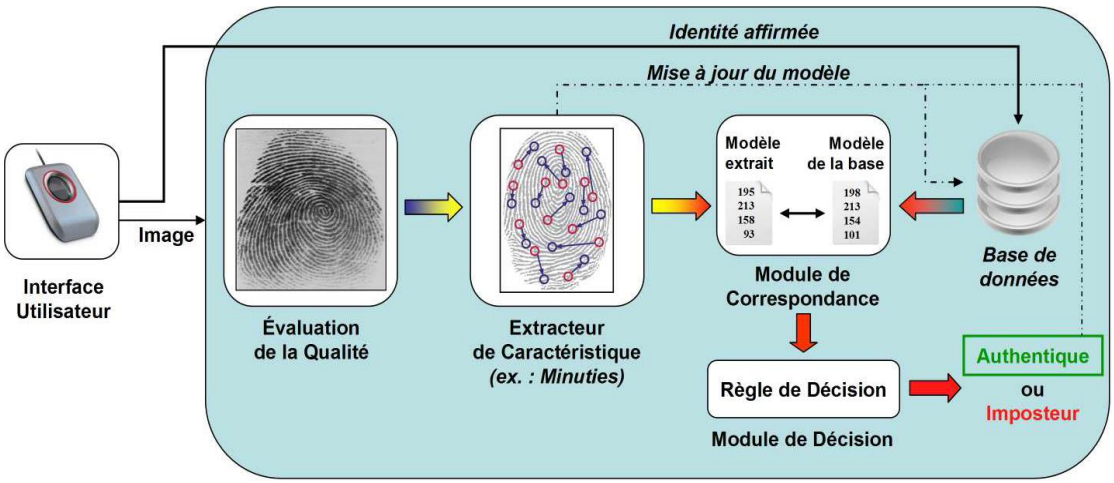


Figure 1.2 Authentification d'une personne dans un système biométrique

Un système biométrique comporte deux phases essentielles: le module d'apprentissage et celui de reconnaissance et une phase facultative qui est le module d'adaptation [4].

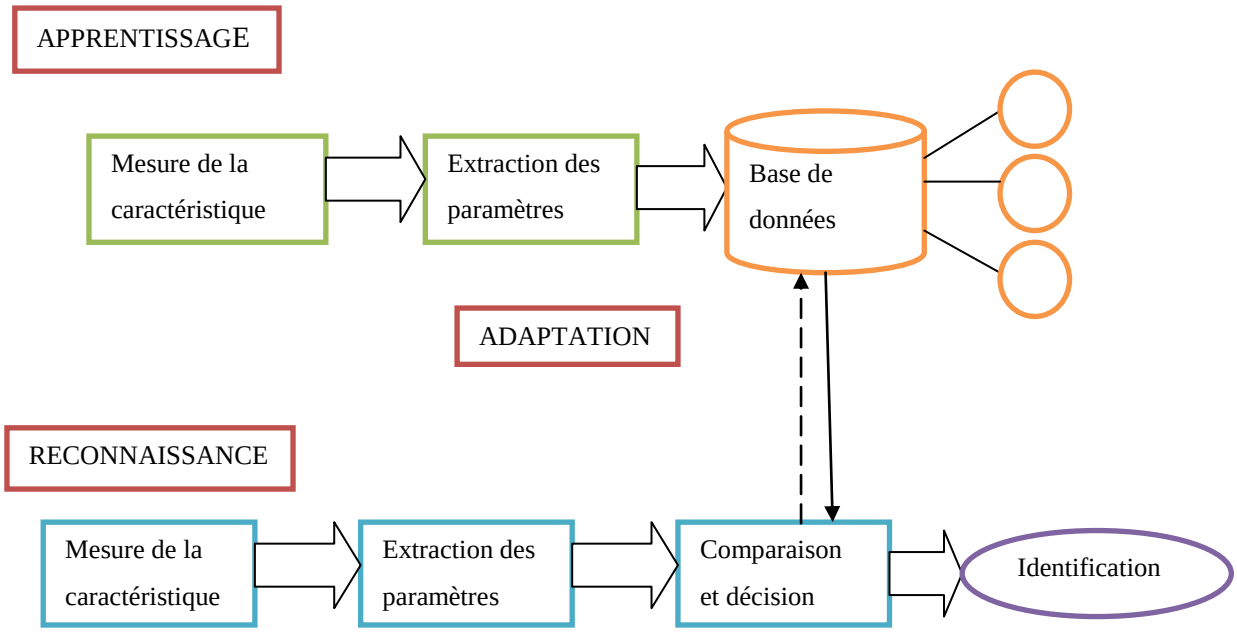


Figure 1.3 Architecture d'un système de reconnaissance biométrique

- **Le module d'apprentissage :**

Lors de la phase d'apprentissage, l'acquisition des caractéristiques se fait grâce au module de capture. En général, cette capture est enregistrée après un ensemble de transformations qu'on lui applique dans le module d'extraction de caractéristiques. Donc, on extrait seulement l'information pertinente afin de former une nouvelle présentation compacte dans le but de faciliter la reconnaissance et de diminuer aussi la quantité de stockage.

En fin, le rôle principal de ce module est de constituer une base de données où chaque modèle est obtenu à partir d'un ou de plusieurs enregistrements de la modalité considérée. Chaque personne a un modèle spécifique et unique dans la base de données biométriques. La plupart des modèles rencontrés sont des modèles statistiques qui permettent de prendre en compte une certaine variabilité dans les données individuelles.

- **Le module de reconnaissance :**

Au cours de ce module, l'ensemble des caractéristiques extraites sera comparé avec le modèle enregistré dans la base de données du système. L'étape de décision permet soit de vérifier l'identité affirmée par un utilisateur ou de déterminer l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et les modèles stockés.

Alors, ce module permet de prendre une décision. Si l'on est en mode identification, le système compare le signal mesuré avec les différents modèles contenus dans la base de données et sélectionne le plus proche. En mode vérification, le système compare le signal mesuré avec un seul des modèles de la base de données et autorise ainsi la personne ou la rejette.

- **Le module d'adaptation :**

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur.

Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir voir améliorer la performance d'un système utilisation après utilisation.

4. EVALUATION DES PERFORMANCES [1]

Les systèmes biométriques sont conçus pour être utilisés dans un grand nombre d'applications. Pour pouvoir envisager le déploiement de ces systèmes dans la vie courante, les systèmes ont besoin d'être évalués pour pouvoir estimer leurs performances en utilisation réelle. L'évaluation des performances comprend de nombreux aspects qui peuvent être plus ou moins importants à tester selon les applications [1]. Lors de la mise en œuvre d'un système biométrique, plusieurs facteurs interviennent comme la facilité d'usage et le confort d'utilisateur, la sécurité, le coût, les problèmes de protection de données, la fiabilité du système ou des capteurs, la vitesse d'acquisition et la rapidité du traitement, les nécessités de maintenance, les besoins humains de contrôle en mode opérationnel et bien sûr le taux

d'erreur de reconnaissance. Tandis que les évaluations des systèmes biométriques sont souvent réalisées uniquement en termes de performance des systèmes de reconnaissance.

Pour estimer les performances d'un système biométrique pour une application spécifique, on trouve trois types d'évaluation :

- L'évaluation technologique qui correspond aux performances des algorithmes du système.
- L'évaluation de scénario qui comprend tout le système, prenant en compte les capteurs, l'environnement et la population ciblée par l'application.
- L'évaluation opérationnelle qui concerne les conditions réelles d'utilisation du système biométrique global.

Dans ce qui suit, on abordera une évaluation de performances d'algorithmes. Pour cela on doit définir les taux d'erreurs engendrés dans un système biométrique.

En biométrie, nous sommes en face de deux populations. Les véritables clients, ceux qui sont dûment autorisés à pénétrer dans la zone protégée**.** Les imposteurs qui n'ont aucune autorisation mais qui vont quand même essayer de rentrer.

Les erreurs d'algorithmes sont des erreurs de décision. Ils sont de deux types : une fausse acceptation lorsque le système accepte un imposteur, et un faux rejet si le système rejette un client.

Dans le cas d'un système biométrique d'identification, on évalue ce dernier sur une base de données en mesurant les deux taux d'erreurs évoqués précédemment en fonction d'un seuil de décision fixé dans le module de décision :

- Le Taux de Fausse Acceptation (FAR : "False Acceptance Rate") qui est égal au nombre de fausses acceptations devisé par le nombre d'imposteurs testés par le système.
- Le Taux de Faux Rejet (FRR : "False Rejection Rate") qui est égal au nombre de faux rejets devisé par le nombre de clients testés par le système.

La performance est la fiabilité d'un système. Elle s'exprime par le taux de faux rejets (FRR) et le taux de fausses acceptations (FAR). Un système émet un faux rejet lorsqu'il rejette par erreur un vrai utilisateur. A l'inverse, un système émettra une fausse acceptation en donnant accès à quelqu'un qui n'a pas de droit. Le seuil de décision doit être estimé en fonction du niveau de sécurité souhaité.

On utilise aussi des courbes dites de performance. Ces courbes représentent chacune des taux d'erreur en fonction du seuil de décision lorsque celui-ci varie.

Lorsque le système est dans le *mode d'authentification*, on utilise la courbe ROC **(R**eceiver **O**perating **C**haracteristic). Cette courbe trace le taux de faux rejet FRR en fonction du taux de fausse acceptation FAR. 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 [3].

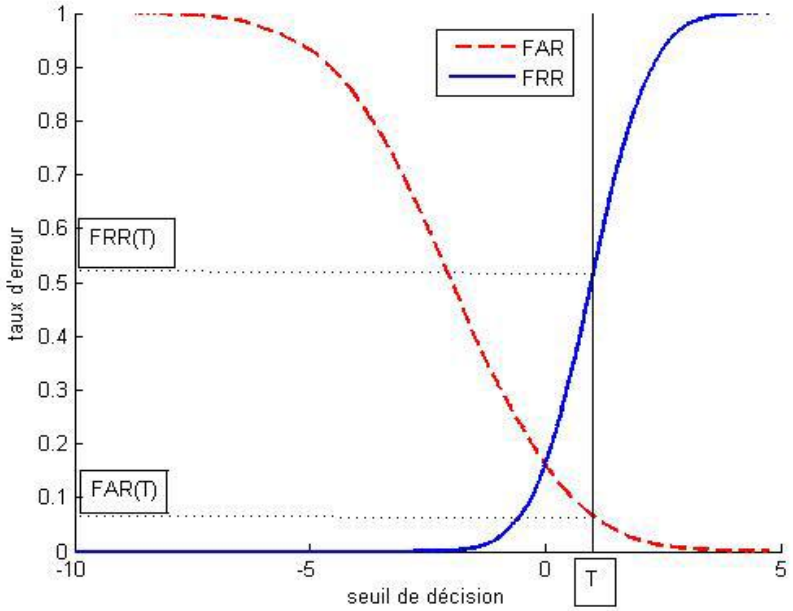


Figure 1.4 Variation des taux de Faux Rejets (FRR) et taux de Fausses Acceptations (FAR) en fonction du seuil de décision

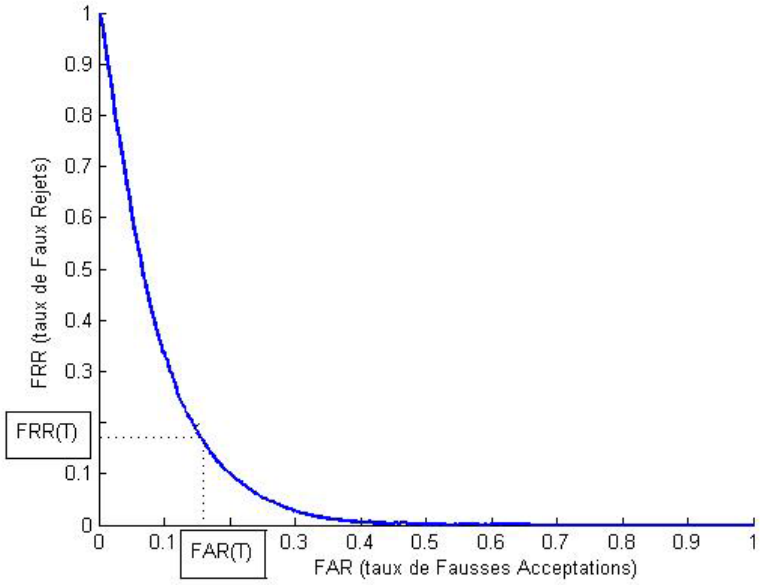


Figure 1.5 Courbe ROC : Variation du taux de Faux Rejets (FRR) en fonction du taux de Fausses Acceptations (FAR) lorsque le seuil de décision varie

La courbe DET (Detection Error Tradeoff) représente les mêmes variations que la courbe ROC pour des échelles logarithmiques.

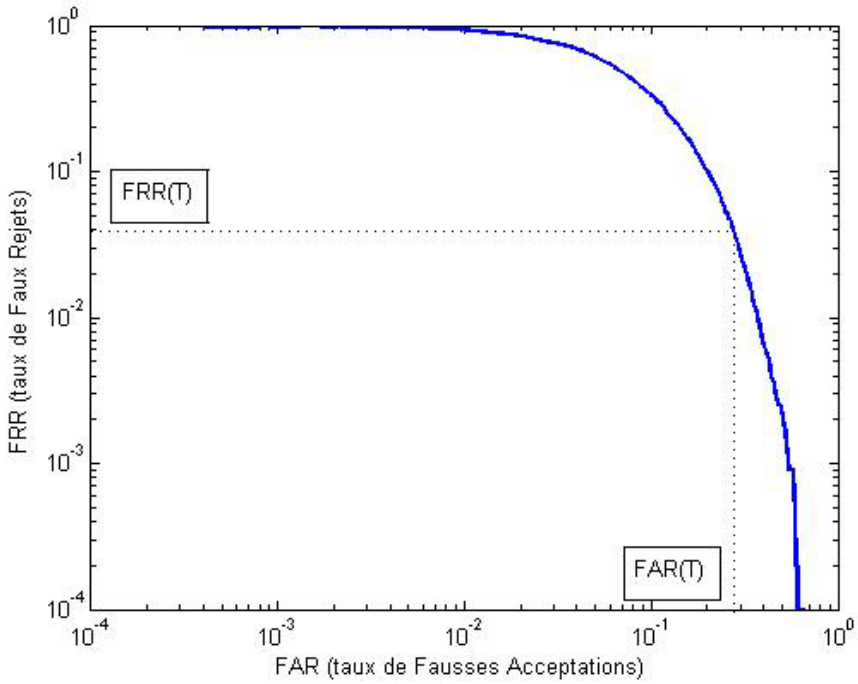


Figure 1.6 Courbe DET : Variation du taux de Faux Rejets (FRR) en fonction du taux de Fausses Acceptations (FAR) en échelle logarithmique lorsque le seuil de décision varie

Dans le cas d'un système utilisé en *mode identification*, on utilise la **courbe CMC** (**C**umulative **M**atch **C**haracteristic). Cette courbe représente le pourcentage de personnes reconnues en fonction du **rang**.

Le rang est une variable propriétaire au système de reconnaissance. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang n, lorsqu'il choisit, parmi n images, celle qui correspond le mieux à l'image d'entrée. Il est clair que le système devient plus performant lorsque le rang diminue.

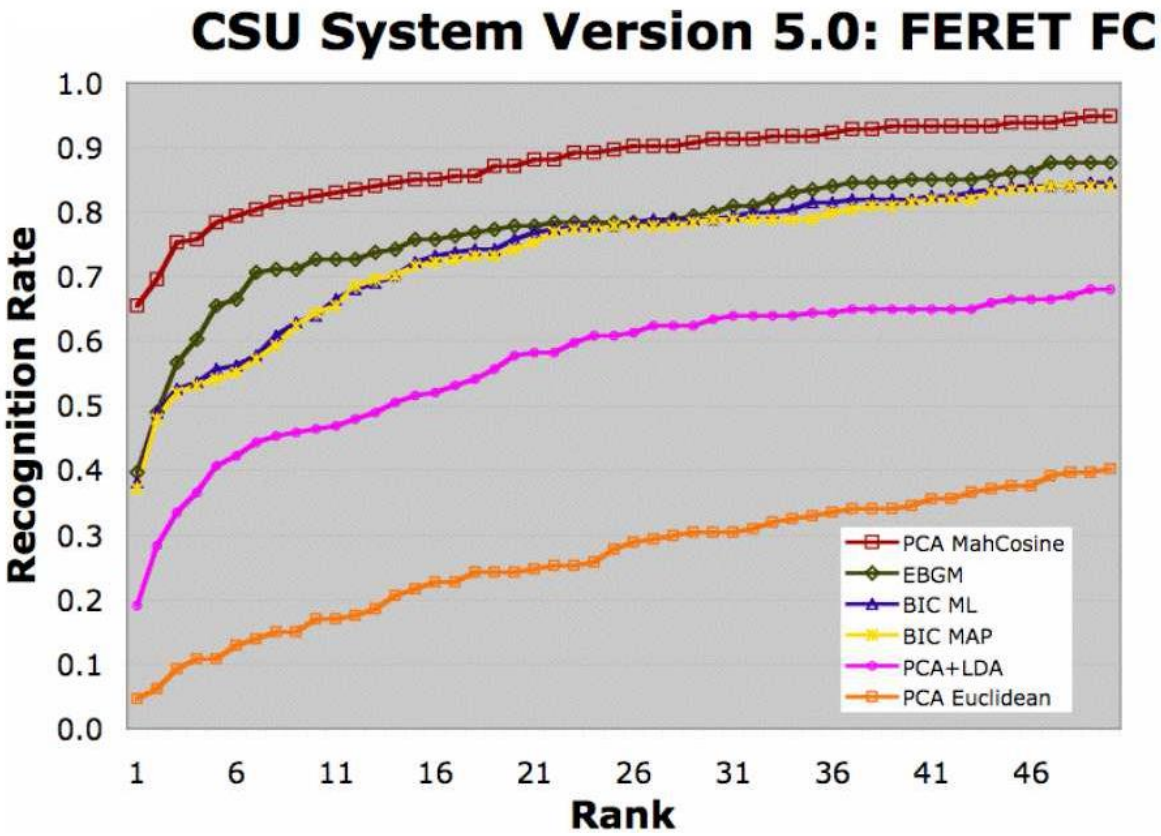


Figure 1.7 Courbes CMC du CSU System 5.0 pour le "FERET Probe Set FC" et pour différents algorithmes de reconnaissance faciale (PCA : Principal Component Analysis ; EBGM : Elastic Bunch Graph Matching ; BIC :Bayesian Information Criterion ; LDA : Linear Discriminant Analysis)

Un autre paramètre à ajouter lors de l'évaluation d'un système biométrique c'est le point de fonctionnement. Le choix de ce point consiste à fixer un seuil de décision et donc prendre les taux d'erreur FRR et FAR correspondants. Parmi les points de fonctionnement utilisés [1]:

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

WER : "Weighted Error Rate" ou taux d'erreur pondéré. Ce point de fonctionnement correspond au seuil tel que le FRR est proportionnel au FAR avec un coefficient qui dépend de l'application. On définit le taux d'erreur pondéré global WTER par la formule suivante :

$WTER = \alpha FAR + (1 - \alpha)FRR$ (Dans l'exemple de la figure 1.8, on a pris un α de 2/3)

FAR fixé : Ce point de fonctionnement correspond au seuil tel que le taux FAR est égal à un taux fixé par l'application (par exemple 1% ou 0:1%). La performance du système est donnée par le taux FRR pour cette valeur de FAR fixée.

FRR fixé : Ce point de fonctionnement correspond au seuil tel que le taux FRR est égal à un taux fixé par l'application (par exemple 1% ou 0:1%). La performance du système est donnée par le taux FAR pour le FRR fixé.

La figure suivante donne une représentation des différents types de points de fonctionnement sur une courbe de performance.

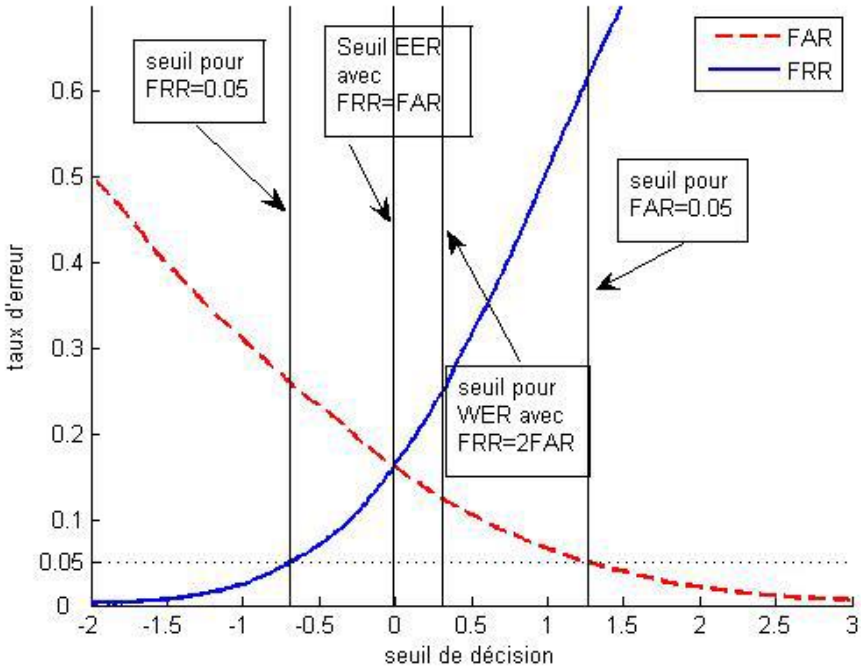


Figure 1.8 Les points de fonctionnement représentés sur une courbe des taux d'erreurs en fonction du seuil de décision

5. LES MODALITES BIOMETRIQUES

Avant de parler des différentes modalités, on parle d'abord des propriétés principales qui doivent les satisfaire. On peut citer :

- L'universalité : qui signifie que chaque personne possède des caractéristiques comparables. La caractéristique doit être possédée par tous les membres de la population.
- L'unicité : chaque individu a sa propre caractéristique qui doit être totalement différente des autres. Donc, deux personnes ne possèdent jamais deux signatures semblables.
- La stabilité : les caractéristiques ne doivent pas changer au cours du temps (permanence) et doivent avoir une résistance aux éléments extérieurs (conditions extérieures) et inférieures (conditions émotionnelles de la personne).
- Mesurabilité : qui justifie la possibilité de quantifier une caractéristique.
- La facilité d'usage : les caractéristiques doivent être accessibles et faciles à acquérir.
- La non reproductibilité (ou non vulnérabilité) : impossible à dupliquer (pirater) une caractéristique.

A cause du développement technologique, il existe de nos jours différents types de modalités biométriques qui sont en usage ou en cours de développement pour les prochaines années. Ces modalités sont classées en deux grandes catégories: les biométries morphologiques et physiologiques et les biométries comportementales.

5.1 Les modalités morphologiques et physiologiques

Ce sont des modalités qui sont basées sur l'analyse des caractéristiques physiologiques du corps humain comme :

5.1.1 L'empreinte digitale [5], [6]

C'est la technologie la plus ancienne et la plus répandue dans le monde. L'empreinte du pouce était comme une signature lors d'échanges commerciaux à Babylone dans l'Antiquité et en Chine au 7ème siècle. Et depuis que F.Galton découvrit la permanence et l'inaltérabilité du dessin papillaire de la naissance à la mort au 19ème siècle, elle est

utilisée pour l'identification criminelle et intervient actuellement pratiquement dans tous les domaines de la vie. La seule différence c'est qu'à l'époque, la vérification était humaine et maintenant elle est devenue numérique et automatique.

Une empreinte digitale se compose de beaucoup de rides et sillons. Ces rides et sillons présentent de bonnes similitudes dans chaque petite fenêtre locale, comme le parallélisme et la largeur moyenne. Cependant, il est montré que la distinction entre les différentes empreintes ne se fait pas par ces rides et sillons mais par des points anormaux sur les rides, nommés « minuties ». A ce jour, on considère qu'il faut huit à dix-sept de ces points sans discordance pour qu'on estime établie l'identification. On recense treize types différents de minuties permettant de classifier les empreintes digitales et d'en assurer leur unicité, dont les six plus fréquentes sont présentées sur la figure ci-dessous :

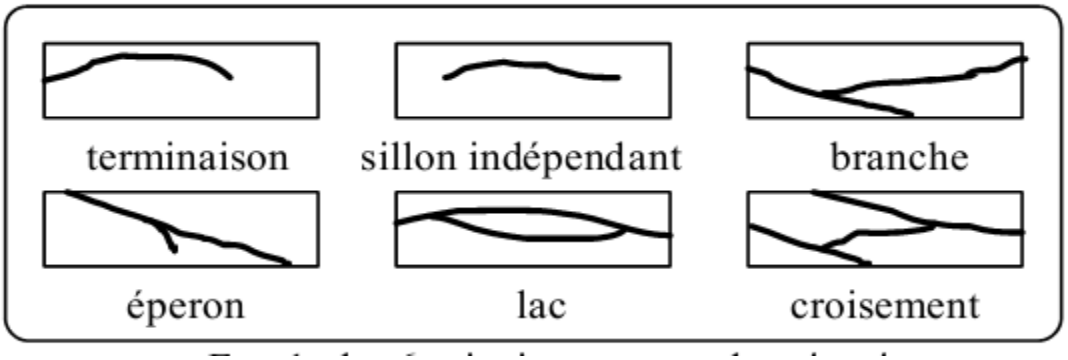


Figure 1.9 Les six principaux types de minuties

La capture de l'image d'une empreinte digitale qui se fait à l'aide de capteurs (optiques, capacitifs, thermiques ou à ultrason) consiste à trouver les lignes tracées par les crêtes (en contact avec le capteur) et les vallées (les creux). Après l'étape de l'acquisition, l'image passe par les étapes suivantes pour extraire les caractéristiques : Estimation d'orientation ; Segmentation ; Détection de rides ; Détection de minuties ; Post-traitement.

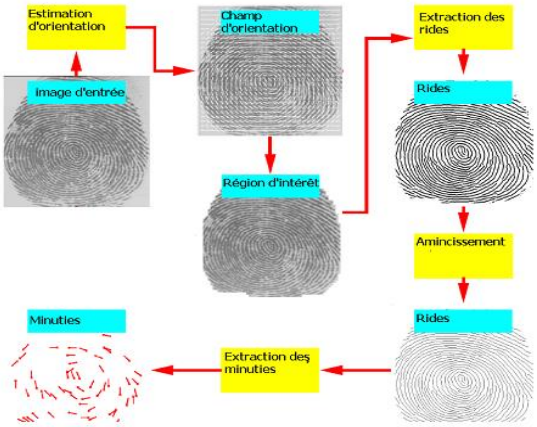


Figure 1.10 les différentes étapes d'extraction des caractéristiques d'une empreinte digitale

Pour la reconnaissance des empreintes, il existe deux catégories d'algorithmes dans la littérature, la première concerne les algorithmes qui s'appuient sur la position relative des minuties entre elles, alors que la seconde regroupe les algorithmes visant à extraire d'autres particularités de l'empreinte digitale telles que la direction locale des sillons, ou encore les composantes fréquentielles locales de la texture au cœur de l'image.

Cette modalité qui est la plus répandue dans le monde est une modalité très fiable qui a un « FAR = [0,005 ; 0,1%] » et un « FRR = [0,01 ; 0,2%] mais son problème est qu'elle laisse des traces.

5.1.2 L'iris [6, 2, 5]

L'identification par l'iris c'est une méthode récente qui a été développée grâce aux travaux de J. Daugman en 1980. L'iris est la zone colorée visible entre le blanc de l'œil et la pupille qui présente une quasi-infinité de points caractéristiques, qui ne varient pratiquement pas pendant la vie de la personne. Pour reconnaître un individu, on extrait ces points caractéristiques (les paramètres de l'image de l'œil), puis on compare ces paramètres avec tous les paramètres précédemment extraits et sauvegardés.

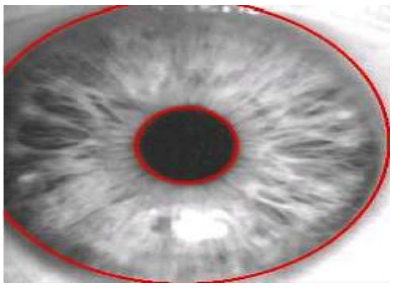


Figure 10.11 L'image de l'iris

A cause de son unicité (même entre jumeaux ou entre l'œil gauche et l'œil droit), son indépendance du code génétique de l'individu et très difficilement falsifiable ; elle est la modalité la plus exacte et la plus fiable qui a un « FAR = 0,0001% » et un « FRR entre 0,25 et 0,5% » mais elle présente différentes contraintes, comme par exemple **:** il faut également tenir compte des reflets ponctuels, de la non uniformité de l'éclairage et des images de l'environnement qui se reflètent sur l'iris.

5.1.3 La géométrie de la main [8]

Ce type de mesure biométrique est l'un des plus répandus, notamment aux Etats Unis. Cela consiste à mesurer plusieurs caractéristiques de la main (jusqu'à 90) telles que la forme de la main, la longueur et la largeur des doigts, les formes des articulations, les longueurs inter-articulations , la texture de la paumes …etc.

Cette modalité présente plusieurs avantages par rapport aux modalités précédentes. Par exemple son système de capture est moins coûteux par rapport à celui de l'iris. Aussi, à cause de multiplicité des caractéristiques de la main, cette méthode ne nécessite pas des images de bonne résolution (La technologie associée à cela est principalement l'imagerie infrarouge). De plus, ce système est bien accepté par les utilisateurs car la main laisse peu de traces contrairement au système basé sur l'empreinte digitale. Mais d'une façon générale, cette modalité présente un FAR assez élevé, surtout entre personnes de la même famille ou bien encore des jumeaux.

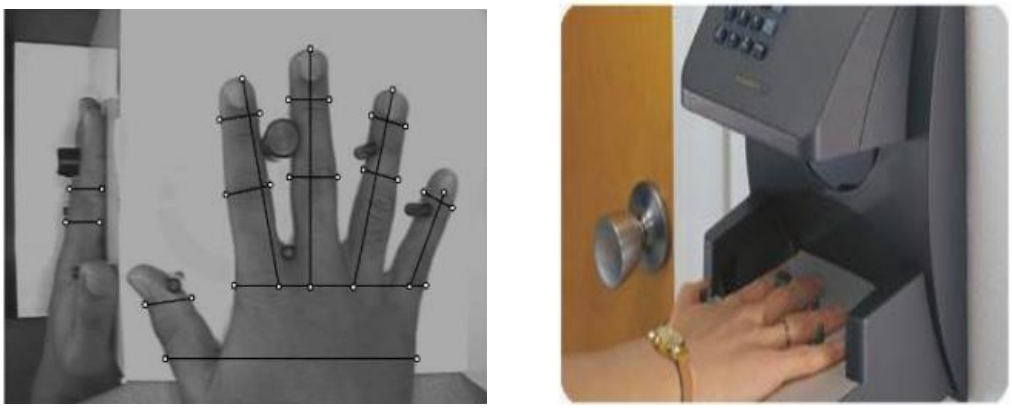


Figure 1.12 Les dispositifs de capture de la géométrie de la main

5.1.4 Le visage [5, 7]

la reconnaissance des visages est une technologie qui a vu un développement considérable ces dernières années, C'est une modalité très acceptée par les utilisateurs, car le visage est la caractéristique biométrique que les êtres humains utilisent le plus naturellement pour s'identifier entre eux.

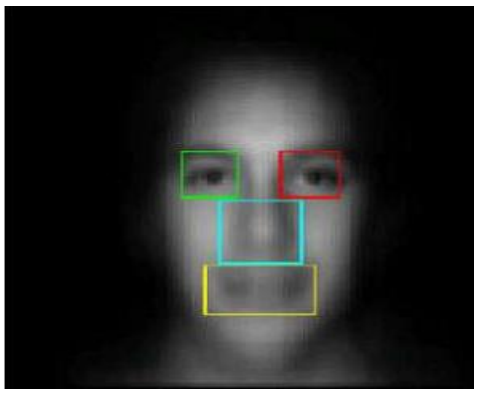


Figure 1.13 Reconnaissance de visage

Lors de la reconnaissance, une photo de visage de l'individu est capturée, volontairement ou involontairement, à l'aide d'une caméra ou d'un appareil photo. Les caractéristiques de l'individu (les yeux, la bouche, le tour du visage, le bout du nez, … etc.) sont extraites de l'image de visage et comparées à une base de données.

Grace à sa facilité d'utilisation et son faible coût, cette technique est la deuxième la plus utilisée après l'empreinte digitale. Mais elle est une modalité peu fiable qui a un FAR entre 0,3 et 5% et un FRR entre 5 et 45% car le problème de cette modalité vient des possibles perturbations pouvant transformer le visage comme le maquillage, la faible luminosité, la présence d'une barbe ou d'une lunette, une expression faciale inhabituelle, le changement avec l'âge…etc.

5.2 Les modalités comportementales

Les biométries comportementales sont celles utilisant un trait personnel du comportement (actions qu'on a effectuées).

5.2.1 La dynamique de la signature [7, 2]

La signature manuscrite est utilisée depuis longtemps pour authentifier des documents tels que des lettres, des chèques...etc. et elle est un geste naturel pour tout le monde donc son utilisation est bien acceptée par la population.

Pour faire l'authentification, la personne doit signer avec un stylo sur une tablette graphique (ou son équivalent) [fig.1.14], et le système de reconnaissance effectue la mesure et l'analyse de plusieurs caractéristiques lors de la signature, tel que la vitesse du stylo, l'ordre des frappes, la différence de pression sur la tablette, l'accélération, le temps total …etc. En d'autres termes, tout ce qui peut permettre d'identifier une personne de la façon la plus sûre possible quand on utilise une donnée aussi changeante que la signature.

Le problème de cette méthode est que l'individu ne signe pas de la même façon (elle dépond de l'état psychologique de la personne). Pour cela, il faut disposer de plusieurs exemplaires de la signature d'une personne (éventuellement recueillis dans un certain intervalle temporel) pour bâtir un modèle de la personne.

Figure 1.14 Capteur de signature

5.2.2 La démarche [9, 10]

Au début, l'analyse de la démarche humaine a été utilisée pour des raisons médicales comme le diagnostic des maladies. Après, des chercheurs ont constaté que comme l'empreinte, l'iris, le visage ... etc. presque chaque personne a son propre style de marche. Ils ont même pensé que la démarche pourrait également être utilisée comme une modalité biométrique pour identifier les personnes.

Comparées aux autres modalités (empreinte, iris ...) cette méthode ne nécessite pas l'interaction de l'utilisateur, et la reconnaissance se fait à distance (à condition que la démarche soit visible). De plus, il est difficile de la déguiser (l'empreinte digitale peut être masquée par un gant, l'iris peut être masqué par des lunettes). Mais le défaut de cette modalité, c'est son faible taux de reconnaissance à cause de sa large variété chez les personnes car plusieurs facteurs peuvent influencer sur la démarche comme « l'âge, l'humeur, la maladie, la fatigue, la drogue ou la consommation d'alcool… ».

5.2.3 La voix [11]

La reconnaissance du locuteur (reconnaissance vocale) est une technologie qui permet, après avoir capturé un modèle digitale de la voix d'une personne, d'utiliser les caractéristiques acoustiques de la parole pour différencier entre les personnes.

Ces caractéristiques acoustiques reflètent à la fois l'anatomie (taille et la forme de la gorge et de la bouche) et des modèles de comportement appris (pitch de la voix, façon de parler…etc.). Pour ces raisons, cette modalité biométrique est considérée comme une modalité physiologique et comportementale.

Pour les systèmes de reconnaissance, il faut distinguer entre les systèmes dépendant du texte et les systèmes indépendants du texte. Dans le premier mode «un mot de passe», est stocké dans une base de données et lorsque l'utilisateur se présente à l'identification, il lui suffit de dire son mot de passe. Le système biométrique analysera alors la voix de l'utilisateur pour déterminer son identité, puis comparera le mot de passe à celui qui est stocké dans la base de données. Par contre, dans le deuxième mode aucun mot de passe n'est requis. Le système analysera la voix et comparera ses caractéristiques avec les données stockées. Cela présente plusieurs avantages par rapport au système texte-dépendant. Tout d'abord, il n'y a pas de mots de passe à retenir (facilite la tâche aux utilisateurs). Deuxièmement, il aide à éliminer la fraude possible parce que la phrase n'est pas la même à chaque fois et ne peut pas être enregistrée et mise au point pour accorder l'accès frauduleux. Toutefois, les systèmes texte-indépendant ont beaucoup de problèmes avec les inadéquations et l'octroi d'accès aux personnes autorisées. C'est pourquoi ils restent principalement au stade expérimental.

Il existe deux différents types d'informations existant avec la reconnaissance vocale : les informations de haut niveau qui traitent les caractéristiques que les humains utilisent pour

la distinction d'une personne d'une autre, comme les accents, le style de parler, le contenu …etc. et les informations de bas niveau qui sont principalement utilisées dans les systèmes de reconnaissance vocale pour analyser la parole, comme la période de pitch, le rythme, le ton, l'amplitude du spectre, les fréquences et la bande passante …etc.

Cette modalité est bien accepter par les utilisateurs car elle n'exige aucun contact avec le système. De plus son système est moins coûteux mais elle est moins fiable à cause de la variabilité de ses caractéristiques comportementales, du fait de l'âge, les états émotionnels et de la santé. Ces systèmes sont sensibles au bruit de fond qui peut fausser l'opération.

Figure 1.15 : Le spectre d'un signal vocal

5.2.4 La dynamique de frappe [12, 13]

Comme la démarche, la manière de signer, chaque personne à sa façon d'écrire avec le clavier. Cette modalité biométrique n'est pas la même chez les individus, elle peut offrir suffisamment d'informations pour permettre de vérifier l'identité des personnes.

Comparée aux autres modalités biométriques, on peut considérer que cette modalité est la plus simple et la plus facile à mettre en œuvre car elle ne nécessite qu'un ordinateur et un clavier ordinaire dans lequel on installe un logiciel. Pour l'identification, l'utilisateur doit écrire un mot ou une phrase fixe (son nom ou un mot de passe) et ce logiciel fait l'extraction et l'analyse de certains paramètres qui déterminent la personne comme :

- la vitesse de frappe cumulant.
- le temps qui s'écoule entre les frappes consécutives.
- le temps pendant lequel chaque touche est maintenue enfoncée.
- la fréquence à laquelle les autres touches, tels que le pavé numérique ou les touches de fonction sont utilisés.
- la séquence utilisée pour taper une lettre majuscule (par exemple : si le shift ou une lettre est libérée en premier).

5.3 Comparaison

À partir des critères cités auparavant une première comparaison des principales technologies biométriques est proposée sur le Tableau 1.1.

Tableau 1.1 Comparaison de technologies biométriques

biométrie	universalité	unicité	permanence	mesurabilité	performance	acceptabilité	Vulnérabilité
DNA	Haute	Haute	Haute	Faible	Haute	Faible	Faible
Oreille	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Haute	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Faible	Haute	Haute
Thermo. Visage	Haute	Haute	Faible	Haute	Moyenne	Haute	Faible
Empreinte	Moyenne	Haute	Haute	Moyenne	Haute	Moyenne	Moyenne
Démarche	Moyenne	Faible	Faible	Haute	Faible	Haute	Moyenne
Géométrie Main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Moyenne
Veines Main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Faible
Iris	Haute	Haute	Haute	Moyenne	Haute	Faible	Faible
Frappe Clavier	Faible	Faible	Faible	Moyenne	Faible	Moyenne	Moyenne
Odeur	Haute	Haute	Haute	Faible	Faible	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Faible	Haute	Haute

Ce n'est pas nécessaire que chaque modalité possède toutes ces propriétés. Elles peuvent les posséder avec des degrés différents. Parmi les techniques les plus matures, on distingue le visage, l'empreinte digitale, la géométrie de la main, l'iris et la rétine, qui présentent de bonnes caractéristiques. Mais aucune d'entre elles n'est parfaite.

Lors du choix de la biométrie, on ne parle pas de modalité parfaite ou idéale mais de son adaptation à des applications ciblées. Donc, le compromis entre la présence ou l'absence de certaines de ces propriétés se fait selon les besoins de chaque application.

Chaque technique possède des avantages et des inconvénients, acceptables ou inacceptables suivant les applications en termes de niveau de sécurité et/ou de facilité

d'emploi, etc. Il faut motionné aussi que ces solutions biométriques ne sont pas systématiquement en concurrence.

6. LA MULTIMODALITE [1]

Les chercheurs ont trouvé que les systèmes de reconnaissance et d'identification basés sur une seule modalité présentent plusieurs problèmes et limites comme :

- la variabilité lors de la capture : qui est due à cause de la défiance du capteur ou du bruit d'acquisition.
- La variabilité temporelle ou intra-classe, ces variabilités d'une modalité pour un individu sont dues aux différences entre les caractéristiques acquises au moment de l'apprentissage et au moment de l'identification. Et la non-unicité « la variabilité interclasse » qui est la variabilité entre les modalités de plusieurs individus.
- La non-universalité qui signifie qu'il y a une catégorie de personnes dont on ne peut pas utiliser certaines caractéristiques biométriques pour leur identification.
- La dépendance aux conditions environnementales au moment de l'acquisition.
- Sensibilité aux attaques et à la fraude

Et pour augmenter la fiabilité de ses systèmes et améliorer ses performances, la multimodalité est souvent appliqué qui consiste en la combinaison de plusieurs systèmes biométriques différents afin de former un seul système plus performant et plus robuste au fraudes, ces systèmes peuvent être :

- Multi-capteur : c'est l'utilisation de plusieurs capteurs pour acquérir la même modalité.
- multi-algorithmes : lorsqu'ils utilisent plusieurs algorithmes pour traiter la même image acquise.
- multi-échantillons : lorsqu'ils récoltent plusieurs échantillons différents de la même modalité, par exemple deux empreintes digitales de doigts différents.
- multi-instances : lorsqu'ils assoient plusieurs instances de la même biométrie, comme par exemple l'acquisition de plusieurs images de visage avec des changements de pose. Dans ce cas les données sont traitées par le même algorithme et ne nécessitent

qu'une seule référence à l'enregistrement contrairement aux systèmes multi-échantillons qui nécessitent des références différentes.

- multi-biométries : lorsque on considère plusieurs biométries différentes.

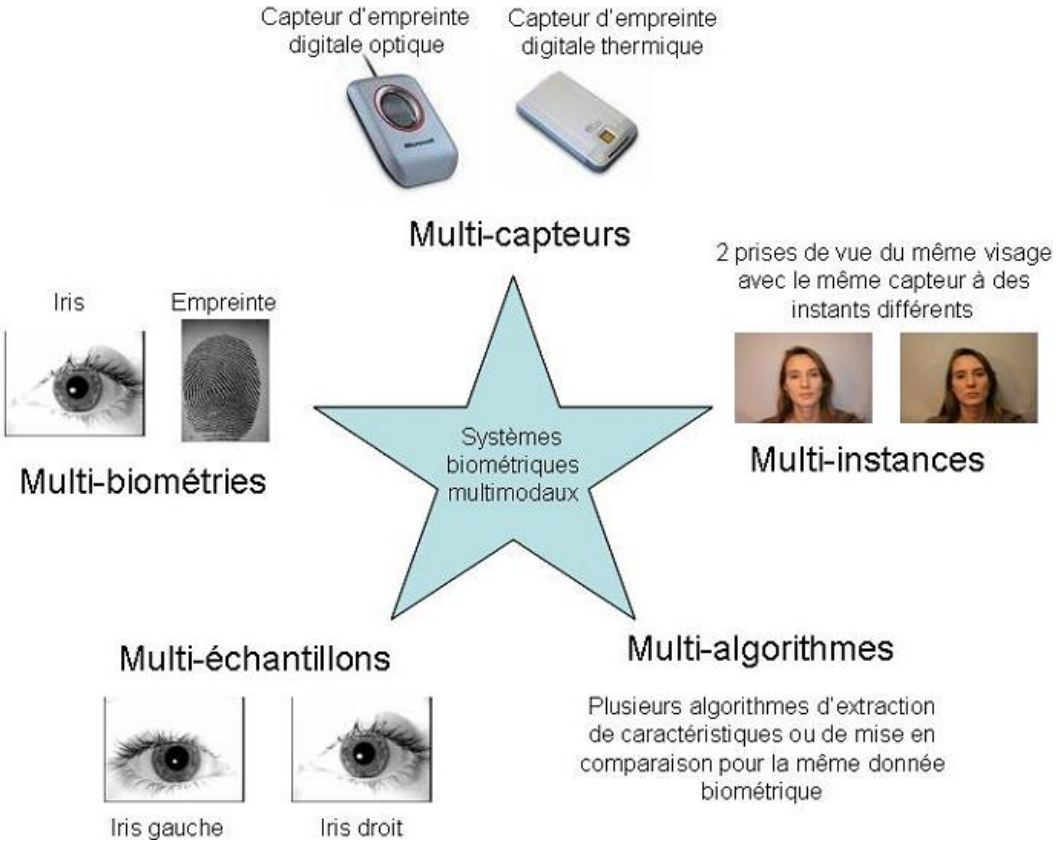


Figure 1.16 Les différents systèmes multimodaux

7. APPLICATION ET CONTRAINTES

L'industrie développe de plus en plus d'applications basées sur l'utilisation de la biométrie dans de nombreux domaines et à finalités diverses :

- Applications commerciales **:** telles que l'ouverture de réseau informatique, la sécurité de données électroniques, l'e-commerce, l'accès Internet, la carte de crédit, contrôles d'accès physique (à des installations, des locaux, des équipements spécifiques etc.), contrôles d'accès virtuel (des systèmes ou réseaux informatiques, commerce électronique etc.), contrôle du temps de travail, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance, etc.

- Applications gouvernementales **:** telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, sécurisation des voyages (contrôles aux frontières etc.), surveillance et identification de personnes ou de voyageurs (casinos, stades, aéroports, passeports biométriques etc.), etc.

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

Les solutions techniques qui s'offrent aux professionnels dans les secteurs les plus divers (dépassant le domaine pénal et celui de la sécurité publique) deviennent de plus en plus nombreuses et à bon marché de sorte que nombreux exploitants publics et privés sont conduits à envisager la mise en place de tels systèmes.

Néanmoins, les instances de protection des données continuent d'appeler à la prudence face à la multiplication de ces applications biométriques et surtout de systèmes basés sur la constitution de banques de données comprenant des informations biométriques des individus.

Il faut donc non seulement veiller à garder un juste équilibre notamment la finalité et la proportionnalité de l'application, mais également évaluer selon des critères pertinents les risques que présente la technique appliquée par rapport à la protection des données à caractère personnel. Ces critères sont les suivants :

- **Fiabilité** - taux d'erreurs important ou faible ? La reconnaissance faciale ou vocale, la géométrie du doigt et la dynamique de la signature sont jugés être d'une fiabilité moindre par rapport à l'empreinte digitale ou la reconnaissance de l'iris.
- **Transparence de l'exploitation** - application visible ou à l'insu des personnes concernées ? L'empreinte digitale, la géométrie de la main, la reconnaissance de la rétine ou encore la dynamique de la signature sont des techniques considérées comme transparentes puisqu'elles ne peuvent être mises en œuvre sans que la personne concernée ne soit au courant.
- **Acceptabilité par les utilisateurs** - l'acceptation de l'application dépend du caractère invasif ou non de la technique utilisée, la reconnaissance de la rétine étant ressentie comme plus dérangeante que la reconnaissance faciale.

- **Degré de stabilité de l'élément biométrique** - constance d'une caractéristique au cours du développement et vieillissement normal d'une personne.
- **Coût** - les technologies évoluent assez rapidement ; néanmoins la reconnaissance de l'iris ou de la rétine engendrent des coûts beaucoup plus importants que par exemple la reconnaissance vocale.
- **Facilité d'emploi** - il s'agit ici d'apprécier le degré d'interaction possible avec le système, en partant des techniques d'utilisation les plus faciles et en terminant avec les plus difficiles: la reconnaissance faciale, la dynamique de la signature, la frappe sur le clavier, la reconnaissance vocale, l'empreinte digitale, la géométrie de la main, et enfin la reconnaissance de la rétine.

Ainsi, la mise en place d'un système de contrôle d'accès doit prendre en compte des éléments propres au facteur humain pour que les contrôles fonctionnent efficacement. Il convient en particulier de prendre en compte les éléments suivants :

- Appareils communs à toute une population.
- Choix des paramètres : on parle alors du seuil d'acceptabilité. Quel que soit le procédé biométrique utilisé, la coïncidence à 100% entre les fichiers signatures, celui établi lors de l'enrôlement et celui établi lors de l'authentification est impossible.
- La durée du contrôle : Le temps d'utilisation du système doit être le plus court possible car il est généralement admis que le temps d'attente pour accéder à un lieu doit être de l'ordre de quelques secondes. En cas d'utilisation pour un contrôle d'accès logique, ce temps doit être révisé à la baisse par rapport aux contrôles d'accès physique. Un système biométrique est d'autant plus toléré qu'il est moins intrusif.
- Les personnes sont sensibles aux aspects « hygiène » dans l'utilisation des systèmes.

8. CONCLUSION

Dans ce premier chapitre qui concerne la biométrie et après la définition de ce terme, nous avons présenté quelques modalités qui sont les plus utilisées actuellement. On a vu aussi l'architecture d'un système biométrique et sur quels critères on se base pour évaluer les performances de ce dernier. En fin, ce chapitre se termine par les applications et les contraintes des systèmes biométriques.

Puisque la biométrie est un lien physique entre une personne et son identité, l'identification par cette méthode est plus sûre que par d'autres moyens comme les cartes ou les clés en termes de sécurité (perte, vol ou falsification) mais elles possèdent quelques problèmes et limites. Pour ces raison, les chercheurs ont pensé à la multi biométrie ou encore à trouver de nouvelles modalités biométriques comme la FKP «Finger Knuckle Print » qui traite une région texturée riche en informations et c'est ce qu'on va le détailler dans le chapitre suivant.

Chapitre 2 Etat de l'art sur la FKP

1. INTRODUCTION

De nombreux chercheurs ont bien exploré les différentes modalités biométriques comme l'empreinte digitale, le visage, l'iris, la main, la voix et la démarche… etc. Comme vu dans le chapitre précèdent.

Les traits à base de la main comme la texture de la paume, la géométrie de la main, les veines, l'empreinte digitale, l'articulation du doigt ont créé un centre d'attention car ils sont très accessibles et conviviaux. Parmi ces caractéristiques, l'empreinte d'articulation du doigt (la FKP) assure des performances meilleures à cause de sa richesse en texture et son acceptabilité. C'est ce qu'on va voir dans ce chapitre.

2. LA FKP [14, 15]

La FKP est une modalité récente qui se base sur l'extraction de la texture de la surface arrière du doigt. Ces inhérentes caractéristiques de la peau qui se trouvent autour de l'articulation phalangienne sont bien distinctives entre les individus.

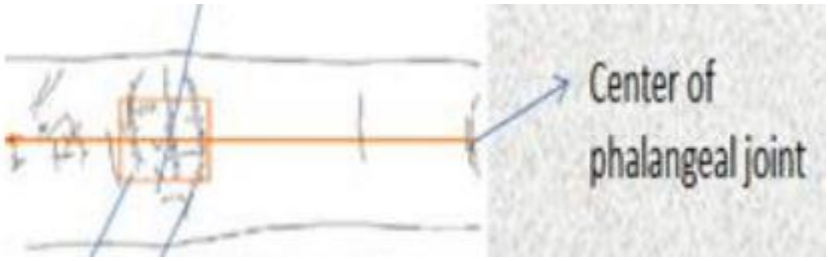


Figure 2.1 Caractéristique de l'articulation du doigt

Woodard et al [16], sont les premières qui ont pensé en 2005 à utiliser cette modalité pour l'authentification biométrique, ils ont proposé un algorithme de reconnaissance basé sur l'extraction de la surface du doigt en 3D prises par un capteur 3D. Mais ce capteur n'est pas acceptable pour une utilisation pratique en raison de sa taille, du coût, du poids, et du temps de traitement, etc. Après, Kumar et al [17] ont proposé en 2007 un algorithme appelé Coding-Based-Knuckle, code généré à l'aide de la transformation de Radon appliqué sur des images capturées en 2D de toute la main (tous les doigts en même temps). Ensuite, les travaux de Zhang et al [26] (en 2009) qui se sont

intéressés à la capture de l'image autour de la région d'intérêt, ont poussé les chercheurs à penser et proposer d'autres méthodes et algorithmes toujours dans le but d'améliorer les performances de reconnaissance.

3. ALGORITHMES DE TRAITEMENT DE LA FKP

Après la capture de l'image du doigt et spécialement autour de l'articulation, un prétraitement de l'image capturée est nécessaire pour l'extraction de la région d'intérêt [voir chapitre suivant]. Ensuite, on effectue l'extraction des caractéristiques et la classification des images pour trouver le résultat (vérification où identification). Plusieurs algorithmes sont appliqués dans cette étape comme :

3.1 BL-POC: Band-Limited Phase-Only Correlation

Zhang et al [14] ont proposé une méthode pour trouver le degré de similitude entre deux images FKP ROI. Le processus de comparaison se fait comme suit :

- POC : Phase-Only-Corelation :

Soient deux images f (m, n) et g (m, n) de résolution $M \times N$ et leurs transformées de Fourier discrètes en 2D $F(u,v)\ et\ G(u,v)$

$$F(u,v) = \sum_{m=-M_0}^{M_0} \sum_{n=-N_0}^{N_0} f(m,n) e^{j2\pi(\frac{mu}{M}+\frac{nv}{N})} = A_F(u,v) e^{j\varphi_F(u,v)} \quad (2.1)$$

$$G(u,v) = \sum_{m=-M_0}^{M_0} \sum_{n=-N_0}^{N_0} g(m,n) e^{j2\pi(\frac{mu}{M}+\frac{nv}{N})} = A_G(u,v) e^{j\varphi_G(u,v)} \quad (2.2)$$

Tel que : $n,v = \{-N_0, \dots, N_0\}\ et\ \ m,u = \{-M_0, \dots, M_0\}$; $M = 2M_0 + 1$ et $N = 2N_0 + 1$

La fonction POC : p_{gf} est la transformé de Fourier inverse de $R_{GF}(u,v)$

$$R_{GF}(u,v) = \frac{G(u,v)F^*(u,v)}{|G(u,v)F^*(u,v)|} = e^{j[\varphi_G(u,v)-\varphi_F(u,v)]} \quad (2.3)$$

Où R_{GF} (u, v) est le « Cross Phase Spectrum » de F(u, v) et G(u, v)

$$p_{gf}(m,n) = \frac{1}{MN}\sum_{u=-M_0}^{M_0}\sum_{v=-N_0}^{N_0} R_{GF}(u,v)\, e^{j2\pi(\frac{mu}{M}+\frac{nv}{N})} \quad (2.4)$$

Si les deux images sont similaires, leur fonction POC donne un pic distinctif au point (x_0,y_0) de la différence de déplacement entre les deux images, sinon la valeur de ce pic diminue et donc on peut mesurer la similitude entre deux images par le niveau de ce pic.

Cependant, les hautes fréquences s'occupent à souligner les détails de l'information et peuvent être sensibles au bruit. Pour éliminer ces composants fréquentiels, ils ont appliqué la BLPOC " Band-Limited Phase-Only-Correlation " qui limite le spectre des images FKP de telle sorte que : $v = -V_0, \dots, V_0 et\ u = -U_0, \dots, U_0$ tel que $0 \le V_0 \le N_0$ et $0 \le U_0 \le M_0$

Et la taille de spectre devient $L_1 = 2U_0 + 1$ $L_2 = 2V_0 + 1$ et la fonction BLPOC c'est :

$$p_{gf}^{U_0\,V_0}(m,n) = \frac{1}{L_1\,L_2}\sum_{u=-\,U_0}^{U_0}\sum_{v=-V_0}^{V_0} R_{GF}(u,v)\, e^{j2\pi(\frac{mu}{L_1}+\frac{nv}{L_2})} \quad (2.5)$$

Ainsi, ils ont fait deux expériences. La première expérience, qui est faite sur un seul doigt, a donné un EER de 1.68%. La deuxième, qui est basée sur la fusion de deux doigts, a donné des résultats meilleurs. Quelle que soit la combinaison, c'est encore plus performant par rapport aux travaux précédents, au niveau de la précision, la vitesse, la taille et le coût.

3.2 La DCT : Discret Cosin Transform

Mohammed Saigaa et al [18], ont utilisé la 2D-BDCT «C'est l'application de 1D-DCT une fois sur les colonnes et une autre sur les lignes, sur l'image f de dimensions $H \times W$ qui est divisée en $N \times N$ blocs», pour extraire le vecteur caractéristique :

$$\psi = [x_0 \quad x_1 \quad x_2 \dots \dots \quad x_{p-2} \quad x_{p-1}]^T \quad (2.6)$$

Où $p = \frac{H \times W}{N^2}$: est le nombre de blocs et x_i est le vecteur caractéristique du i^{ème} bloc qui se situe à (b, a).

Et puisque la DCT basique est sensible aux changements de la direction d'illumination, ils font l'application et la comparaison de différentes techniques de la DCT d'où ce vecteur x diffère d'une forme à une autre.

- La 2D-DCT basique :

$$x_i = [\, F_0^{(a,b)} \quad F_1^{(a,b)} \quad F_2^{(a,b)} \quad F_3^{(a,b)} \quad \dots\dots \quad F_{M-2}^{(a,b)} \quad F_{M-1}^{(a,b)} \,]^T \tag{2.7}$$

- La 2D-DCT-detla :

Ces caractéristiques sont basées sur les coefficients polynomiaux (coefficients deltas), ils ont été utilisés pour réduire les effets du bruit de fond et la disparité du canal.

Les n^{ième} coefficients delta horizontale et verticale pour un bloc situé à (b, a) sont donnés par les formules (2.8) et (2.9) suivantes :

$$\Delta^h F_n^{(b,a)} = \frac{\sum_{k=-K}^{K} k h_k F_n^{(b,a+k)}}{\sum_{k=-K}^{K} k^2 h_k} \tag{2.8}$$

$$\Delta^v F_n^{(b,a)} = \frac{\sum_{k=-K}^{K} k h_k F_n^{(b+k,a+)}}{\sum_{k=-K}^{K} k^2 h_k} \tag{2.9}$$

- La 2D-DCT mod :

$$x = [F_3 \quad F_4 \quad F_5 \quad F_6 \quad \dots\dots \quad F_{M-2} \quad F_{M-1}]^T \tag{2.10}$$

- La 2D-DCT mod2 :

$$x = [\Delta^h F_0 \quad \Delta^v F_0 \quad \Delta^h F_1 \quad \Delta^v F_1 \quad \Delta^h F_2 \quad \Delta^v F_2 \dots\dots \quad F_{M-2} \quad F_{M-1}]^T \tag{2.11}$$

- La 2D-DCT mod-delta :

$$x = [\Delta^h F_0 \quad \Delta^v F_0 \quad \Delta^h F_1 \quad \Delta^v F_1 \quad \Delta^h F_2 \quad \Delta^v F_2 \dots \quad \Delta^h F_{M-1} \quad \Delta^v F_{M-1}]^T \tag{2.12}$$

Tel que :

$$F_{ij}\ (u,v) = C(u)C(v)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1} f_{ij}(n,m)\psi(n,m,u,v) \qquad (2.13)$$

$les\ coeffecient\ de\ la\ DCT\ du\ bloc\ B_{ij}\ , et f_{ij}(n,m)\ la\ luminance\ de\ pixel\ (n,m)$

Ou $\psi(n,m,u,v) = \cos[\frac{(2n+1)u\pi}{2N}]\cos[\frac{(2m+1)v\pi}{2N}]$

$$C(u) = \begin{cases} \frac{1}{\sqrt{2}} & si\ u = 0 \\ 1 & si\ u \neq 0 \end{cases}$$

$$u,v = 0,1,\dots,N-1; i = 0,1,\dots,\frac{H}{N}-1; j = 0,1,\dots,\frac{W}{N}-1$$

Et pour l'étape de décision, ils ont calculé la somme d'erreurs entre chaque paire de points entre le vecteur caractéristique de l'image de test (ψ_t) et le vecteur caractéristique de l'image modèle (ψ_m), la plus petite valeur de E détermine l'image la plus proche.

$$E = \sum_{i=0}^{N-1}\sum_{j=0}^{N-1} |\psi_t(i,j) - \psi_m(i,j)| \qquad (2.14)$$

Dans le cas de l'identification, le score de similitude est calculé pour toutes les images de la base de données, donc une étape de normalisation est nécessaire et le vecteur de score normalisé devient :

$$E_i^{Nr} = \frac{E_i - \min(E_i)}{\max(E_i) - \min(E_i)} \qquad (2.15)$$

Tel que $E_i = [\,E_{i0} \quad E_{i1} \quad E_{i2} \dots\dots E_{iN_d}]$ (2.16)

Avec N_d : la taille de la base de données ; i l'ordre de l'image test ;

Et dans le cas de fusion des différents doigts, la règle de minima est appliquée.

$$E_f = \min(E_{LIF}, E_{LMF}, E_{RIF}, E_{RMF}) \qquad (2.17)$$

Les expériences de ces chercheurs [18] et l'évaluation des résultats qui sont basés sur la courbe ROC et la valeur d'EER ont montré que la meilleure forme, c'est la 2D-DCT-mod2

qui a donné un EER de 7.60% dans le mode de vérification et un EER de 3.33% dans le mode d'identification, et la fusion des différentes modalités (quatre doigts) donne des meilleurs résultats qu'une seule modalité.

3.3 SURF «Speeded-Up Robust Features »

L'algorithme *Speeded-Up Robust Features* est un algorithme très utilisé dans le domaine de traitement d'image et spécialement dans l'extraction de caractéristiques à cause de son invariante à l'échelle et à l'orientation.

L'étape d'extraction de caractéristiques proposée par ZHU Le-qing [19] se fait par cet algorithme comme suit :

- La détection des points clés par le calcul de la matrice de Henssian à chaque point p=(x, y) à l'échelle σ

$$H(p,\sigma) = \begin{bmatrix} L_{xx}(p,\sigma) & L_{xy}(p,\sigma) \\ L_{xy}(p,\sigma) & L_{yy}(p,\sigma) \end{bmatrix} \quad (2.18)$$

Où $L_{xx}(p,\sigma)$ c'est le produit de convolution entre l'image I et la dérivé seconde de la distribution de Gauss ($\frac{\partial^2}{\partial x^2}g(\sigma)$), même chose pour $L_{yy}(p,\sigma)$ et $L_{xy}(p,\sigma)$.

- L'extraction de descripteur SURF se fait en deux phases :

La première étape consiste à déterminer le domaine d'orientation pour chaque point d'intérêt, basée sur l'information d'une région circulaire autour de ce point à l'aide d'ondelette de Haar. Après, on construit une région carrée divisée en sous-régions alignées sur l'orientation choisie, et on extrait le descripteur SURF qui est la concaténation des vecteurs V_i de chaque sous-région :

$$V_i = \left\{ \sum d_x \ , \ \sum d_y \ , \ \sum |d_x| \ , \ \sum |d_y| \right\} \quad (2.19)$$

$\sum d_x$, $\sum d_y$ sont les réponses de la transformée en ondelettes sur une sous-région

Et pour la mise en conformité des caractéristiques, la meilleure façon pour accorder les points d'intérêt consiste à trouver son plus proche voisin des points d'intérêt des images

d'essai existant dans la base de données, en déterminant la plus petite distance euclidienne. Pour assurer de bons résultats et éliminer les erreurs de l'étape précédente, ils ont appliqué l'algorithme : RANSAC «random sample consensus».

Les expériences dans cette référence sont faites sur la base de données FKP de PolyU et l'évaluation des performances a été basée sur la précision qui est de : 90.63% en mode vérification et de 96.91% en mode identification et le temps moyen de l'opération est de 0.531s pour la vérification et 0.106s pour l'identification.

Michał Choraś et Rafał Kozik [20], font d'abord l'analyse par le PHT (Probabilistic Hough Transform) pour déterminer le domaine d'orientation et la construction du vecteur caractéristique de base qui décrit la texture de l'articulation « knuckle », ce vecteur contient un ensemble de descripteurs ligne représenté par la formule suivante :

$$LD_i(N) = \left[b_{xN}\,, b_{yN}\,, e_{xN}, e_{yN}\,, \theta_N\,, d_N\right] \qquad (2.20)$$

$DL_i(N)$: le descripteur pour la n-ième ligne de la i-ème image ; **(b_x, b_y)** : les coordonnées cartésiennes du point de départ de la ligne ; **(e_x, e_y)** : les coordonnées cartésiennes du point de la fin de ligne ; **θ** : l'angle entre la normale de la ligne et l'axe X, et **d** est la longueur de la ligne particulière exprimée en pixels, **N** : le nombre de lignes extraites.

Les descripteurs calculés pour des images tests et modèles entrent dans le bloc de correspondance pour trouver les 5 images modèles les plus proches de l'image de test par la détermination des distances euclidiennes minimales. Après, ils appliquent l'algorithme SURF pour trouver l'image désirée. Et pour bien comprendre la métrologie de classification, elle se compose de trois étapes consécutives :

a. Le choix de 50 images (ce nombre est déterminé empiriquement) pour la base du vecteur de base.
b. Après, on choisit 5 images pour la base du vecteur caractéristique de PHT.
c. Et finalement, le dispositif de SURF est employé.

Au cas où la classification par le SURF a échoué, ou on ne peut pas trouver l'image assortie, le premier plus proche voisin obtenu à partir de PHT est retourné avec les points assortis appropriés.

Ces expériences qui ont été appliqué sur la base de données IIT Delhi Knuckle, ont donné des résultats relativement bons (EER moyen = 1.02%) car la combinaison de la PHT avec le SURF donne des résultats beaucoup mieux que l'utilisation de PHT seul ou SURF seul.

3.4 Les ondelettes de Gabor

Hegde et al [21] ont proposé un système d'authentification basé sur l'image FKP d'une personne en utilisant l'ondelette de Gabor. Dans la technique proposée, ils ont appliqué la transformée en ondelettes de Gabor sur l'image FKP prétraitée. Ensuite, ils ont tracé un graphe d'odelettes de Gabor et des points pics ont été identifiés. L'algorithme proposé est simulé sur la base de données PolyU FKP.

Avoir la base de données d'images FKP de tous les membres d'une organisation consomme plus d'espace et la complexité du système augmente. Ainsi, ils ont proposé d'avoir le numéro d'identification d'utilisateur (UID) pour chaque personne.

Les caractéristiques de l'image FKP comme le nombre de pics dans le diagramme en ondelettes de Gabor et les distances successives entre ces pics sont stockées dans la base de données correspondant à un UID particulier. Lors de l'authentification, la personne doit fournir son UID et son image FKP est capturée. Si les caractéristiques de la nouvelle image conviennent aux caractéristiques correspondantes dans la base de données, la personne peut être authentifiée.

Dans un premier temps, un prétraitement est effectué. L'image acquise en RVB est convertie en niveaux de gris. Ensuite, la région d'intérêt (ROI) est extraite de l'image FKP. Les bords sont détectés par recherche de maxima locaux du gradient de l'image. Le gradient est calculé en utilisant la dérivée d'un filtre gaussien.

Le procédé utilise deux seuils pour détecter les bords forts et faibles, et inclut les bords faibles dans la sortie si elles sont reliées à des bords forts. Ensuite des filtres de rang sont utilisés, dont la réponse est basée sur la commande (classement) des pixels contenus dans la zone d'image englobées par le filtre. La réponse du filtre à un point quelconque est alors déterminée par le résultat de classement. L'algorithme actuel utilise le filtre médian.

L'Ouverture morphologique est appliquée pour lisser le contour des bords et éliminer des protubérances minces. L'image est ensuite dilatée pour élargir les bords obtenus. Ensuite, nous appliquons la transformée en ondelettes de Gabor sur l'image obtenue après traitement préalable. L'ondelette de Gabor est une onde plane complexe limitée par une enveloppe gaussienne bidimensionnelle. L'ondelette de Gabor contient deux composants à savoir réel et imaginaire. En dehors de l'échelle et l'orientation, la seule chose qui diffère deux ondelettes de Gabor est le rapport entre la longueur d'onde et la largeur de l'enveloppe gaussienne. Chaque ondelette de Gabor a une certaine longueur d'onde et une orientation, et peut être convoluée avec une image pour estimer l'amplitude des fréquences locales de cette longueur d'onde approchée et l'orientation dans l'image.

Pour authentifier la personne en question, nous comparons tout d'abord le nombre de points pics dans le graphe d'ondelettes de Gabor et celui dans la base de données pour un UID donné. S'ils ne correspondent pas à la valeur du seuil prédéfinie, la personne est refusée. Dans le cas contraire, les distances entre les sommets successifs stockées dans la base de données et celles de cette nouvelle image sont comparées. Chaque similarité pour un seuil donné est considérée comme le nombre de succès et une non-similarité comme un échec. La probabilité de succès est alors calculée. Si la probabilité calculée est supérieure à 0.60, la personne peut être acceptée. Sinon, elle sera rejetée.

La technique proposée est implémentée en utilisant MatLab 7.5. Les résultats de simulation montrent que le taux de fausses acceptations (FAR) pour l'algorithme proposé est de 1,24% et le taux de faux rejets (FRR) est d'environ 1,11%. Les résultats ont été obtenus lorsque pour un seuil fixé à 0,60. La technique proposée est facilement adaptable à des situations en temps réel car elle est basée sur des techniques simples de traitement d'image.

3.5 La fusion des caractéristiques de Gabor

Zahra et al [22] ont présenté une des modalités récentes dans la biométrie qui est la FKP « Finger-Knuckle-Print » en utilisant une nouvelle méthode de reconnaissance. Cette méthode inclut le filtre de Gabor, la combinaison des deux algorithmes PCA et LDA et la mesure de la distance euclidienne. Ces trois étapes sont utilisées pour la réduction de dimensionnalité, l'extraction de caractéristiques et l'étape de classification respectivement.

La fusion des informations est utilisée pour différentes combinaisons de doigts pour améliorer le taux de reconnaissance. Cet algorithme fonctionne comme une sorte de multimodalité avec une seule caractéristique biométrique mais plusieurs unités. Dans un premier temps, cette méthode a été appliquée sur chaque doigt séparément, puis sur les différentes combinaisons de doigts en utilisant quatre doigts.

Ils ont ainsi utilisé la base de données « Poly-U Finger-Knuckle-Print » pour évaluer les performances de cette méthode. L'algorithme de reconnaissance FKP est développé dans les deux modes d'identification et de vérification.

Il est nécessaire de construire un système de coordonnées locales pour chaque image FKP. Après avoir fait un tel système de coordonnées, une région d'intérêt (ROI) peut être recadrée de l'image originale pour l'extraction des caractéristiques.

Le filtre de Gabor est utilisé pour extraire la caractéristique à partir des images FKP(ROI). Ils ont utilisé un ensemble de filtres de Gabor pour extraire les différentes caractéristiques des images, partageant les mêmes paramètres, sauf les paramètres d'orientation et d'échelles. En fait, dans chaque expérience, ils utilisent 5 échelles et 8 orientations différentes.

Les caractéristiques extraites obtenus à partir de l'étape préalable, ont des dimensions élevées et il est difficile de les évaluer; alors ils ont utilisé l'algorithme PCA pour sélectionner les fonctions les plus importantes. Cette méthode est plus adaptée pour la reconstruction d'image mais elle ne considère pas la séparabilité des différentes classes. Pour une séparabilité optimale, l'algorithme LDA est combiné avec le PCA.

Ils ont utilisé la distance euclidienne comme règle de décision, en mesurant la distance euclidienne entre l'échantillon qu'on veut tester et celui (ceux) dans la base de donnés. Si cette distance est petite, on dit que ces vecteurs sont similaires.

Ils ont effectué deux expériences pour chaque mode, identification et vérification.

- Dans la première expérience, on évalue les performances de l'algorithme proposé pour chaque doigt séparément en utilisant la courbe CMC. Les résultats expérimentaux indiquent que le majeur droit est plus performant que les autres doigts. C'est

probablement parce que la majorité des gens de la base sont droitiers et aussi le doigt du milieu a une faible mobilité.

- Dans la deuxième expérience, en fusionnant les caractéristiques de chaque doigt, ils ont testé plusieurs combinaisons de doigts. En fait, le but de cette expérience est d'étudier les performances de l'algorithme lorsqu'on fusionne des informations de plus d'un doigt d'une personne. On peut dire que, par ce travail, l'algorithme fonctionne comme une sorte de multimodalité avec un seul trait biométrique, mais plusieurs unités.

D'après les résultats obtenus, on peut constater que par l'intégration des informations de plusieurs doigts, les performances de reconnaissance d'algorithme pourraient être améliorées, de sorte qu'en combinant les caractéristiques de quatre doigts, le plus haut taux de reconnaissance est obtenu.

Les résultats des expériences d'identification sont satisfaisants, mais la méthode proposée ne fonctionne pas bien sur le mode de vérification.

3.6 Les caractéristiques de Gabor avec OLDA, MMDA, OCLPP

Dans ces travaux, ils ont proposé une méthode qui utilise la représentation de la fonction de Gabor soit avec l'OLDA (Orthogonal Linear Discriminant Analysisre) ou bien la MMDA pour identifier les images FKP (finger-knuckle-print).

Premièrement, nous calculons la représentation de la fonction d'ondelette de Gabor de l'image. L'Ondelette de Gabor a été utilisée avec succès dans la reconnaissance des visages. Elle présente des caractéristiques souhaitables de localité spatiale et une sélectivité d'orientation, et elle est localisée de manière optimale dans l'espace et dans le domaine fréquentiel. L'ondelette de Gabor peut être définie comme suit :

$$\psi_{u,v}(z) = \frac{\left\| k_{u,v} \right\|^2}{\sigma^2} e^{\left(-\frac{\|k_{u,v}\|^2 \|z\|^2}{2\sigma^2}\right)} \left[e^{ik_{u,v} z} - e^{-\sigma^2/2} \right] \qquad (2.21)$$

Où u et v définissent l'orientation et l'échelle des noyaux de Gabor z(x,y), ‖ ‖ désigne la norme, et le vecteur d'onde $k_{u,v}$ est défini comme suit:

$$k_{u,v} = k_v \, e^{i\emptyset_u} \tag{2.22}$$

Ou $k_v = \frac{k_{max}}{2^{v/2}}$, $\emptyset_u = u\left(\frac{\pi}{8}\right)$, k_{max} est la fréquence maximale, et f est le facteur d'espacement entre les noyaux dans le domaine fréquentiel. Dans la plupart des cas, on devrait utiliser l'ondelette de Gabor de cinq échelles différentes, v = {0,…,4}, Et huit orientations, u = {0,…,7}.

La transformation de Gabor d'une image I (z) donnée est définie comme étant la convolution de celle-ci avec la fonction de Gabor :

$$G_{u,v}(z) = I(z) * \psi_{u,v}(z) \tag{2.23}$$

Où z(x, y) désigne la position de l'image, * désigne l'opérateur de convolution, $G_{u,v}(z)$ et est le résultat de convolution correspondant au noyau de Gabor à l'échelle v et l'orientation u. La transformée de Gabor est une fonction complexe, qui peut être réécrite sous la forme :

$$G_{u,v}(z) = A_{u,v}(z)e^{i\theta_{u,v}(z)} \tag{2.24}$$

Avec une amplitude $A_{u,v}(z)$ et une phase $\theta_{u,v}(z)$.

Nous choisissons l'amplitude comme la représentation des caractéristiques d'une image I(z). Par conséquent, l'ensemble S = $\{A_{u,v}(z)$: u = {0,… ,7}, v = {0,… ,4}$\}$ forme la représentation de la caractéristique de Gabor de l'image I(z).

Pour englober différentes fréquences spatiales (échelles), localités spatiales et sélectivités d'orientation, ils ont réunis tous ces résultats de représentation en créant un vecteur de caractéristique X de dimension élevée. Avant la concaténation, on sous-échantillonne chaque amplitude A par un facteur ρ pour réduire la dimension d'espace, et on la normalise à une moyenne nulle et variance unité. On construit alors un vecteur $A_{u,v}(z)$ en enchaînant ses lignes (ou colonnes).

Maintenant, supposons que $A_{u,v}(z)^{(p)}$ désigne le vecteur normalisé, construit à partir de $A_{u,v}(z)$. Le vecteur de caractéristiques de Gabor résultant $A^{(p)}$ est alors défini comme suit :

$$A^{(p)} = (A_{0,0}^{(p)t} A_{0,1}^{(p)t} \dots A_{4,7}^{(p)t}) \quad (2.25)$$

Ce vecteur est considéré comme information discriminante importante.

3.6.1 L'OLDA [23]

Maintenant, nous faisons la transformation OLDA dans un espace PCA transformé pour avoir la matrice de projection. Troisièmement, la représentation de la fonction de Gabor est projetée sur la matrice de projection et classée par la suite.

La représentation des caractéristiques de Gabor réside sur un espace de très grande dimension. Une représentation de faible dimension est très importante pour le stockage, le calcul et la classification. Ainsi, LDA est l'approche représentante pour apprendre le sous-espace discriminant.

Supposons qu'il existe C classes connues de signatures, la matrice de dispersion interclasse Sb, la matrice de dispersion intra-classes Sw et la matrice de dispersion totale St peuvent être notées :

$$S_b = \frac{1}{N} \sum_{i=1}^{C} N_i (m_i - m_o)(m_i - m_o)^T \quad (2.26)$$

$$S_w = \frac{1}{N} \sum_{i=1}^{C} \sum_{x_k \in X_i} (x_k - m_i)(x_k - m_i)^T \quad (2.27)$$

$$S_t = \frac{1}{N} \sum_{i=1}^{N} N_i (x_k - m_o)(x_k - m_o)^T \quad (2.28)$$

Où N est le nombre total d'échantillons d'apprentissage, et Ni est le nombre d'échantillons d'apprentissage de la classe i. En classe i, l'échantillon d'apprentissage j est noté par x_{ij}, le vecteur moyen d'échantillons d'apprentissage en classe i est représenté par m_i et le vecteur moyen de tous les échantillons d'apprentissage est m_o.

Si S_w est inversible, la projection optimale W_{opt}est choisie en tant que matrice avec des colonnes orthogonales qui maximisent le rapport entre le déterminant de la matrice de dispersion interclasse des échantillons projetés et le déterminant de la matrice de dispersion intra-classe des échantillons projetés,

$$W_{opt} = argmax_{\,w} \frac{W^T S_b W}{W^T S_w W} \tag{2.29}$$

Où w est l'ensemble des vecteurs propres généralisés de $S_w^{-1} * S_b$ correspondant aux m plus grandes valeurs propres généralisées. Dans le problème d'échantillon de petite taille, la matrice de dispersion intra-classe S_w est toujours singulière. Belhumeur et al ont proposé la méthode Fisherface (également appelée PCA + LDA) qui emploie en premier PCA pour réduire la dimension de l'espace des caractéristiques de N-C, puis applique LDA pour réduire la dimension de C-1, où N est le nombre d'échantillons et C le nombre de classes. Notez que cette méthode est sous-optimale parce que PCA doit garder N-1 composantes principales afin de ne pas perdre des informations. Cependant, la première étape de la PCA + LDA ne conserve que N-C composantes principales. On perdra beaucoup d'informations si le nombre de classes est grand. Et la matrice de dispersion intra-classe de Fisherface pourrait encore être singulière dans l'espace PCA transformé.

La LDA Orthogonale (OLDA) a été proposée par Wankou et al [23], comme une extension de la LDA classique. Les vecteurs discriminants en OLDA sont orthogonaux les uns aux autres. En outre, OLDA est applicable même lorsque toutes les matrices de dispersion sont singulières, surmontant ainsi le problème de singularité. La transformation optimale dans l'OLDA peut être calculée en résolvant le problème d'optimisation suivant :

$$W_{OLDA\_opt} = argmax_{\,(w^T w=1)} \frac{W^T S_b W}{W^T S_w W} \tag{2.30}$$

Ils ont utilisé la base de données PolyU FKP pour évaluer les performances de PCA, LDA, Gabor + PCA, Gabor + LDA et la méthode proposée. Dans toutes les expériences, ils faisaient des expériences sur l'index gauche, le majeur gauche, l'index droit et le majeur droit respectivement.

La méthode proposée a le meilleur taux de reconnaissance ; la LDA a de meilleures performances en comparaison avec la PCA ; la fusion de Gabor avec les méthodes globales a des performances meilleures que les méthodes globales correspondantes ; Le taux de reconnaissance du doigt du milieu est supérieur à celui de l'index.

3.6.2 La MMDA [24]

Wankou et al. [24] ont proposé une méthode qui utilise la fonction de Gabor avec la MMDA (multi-manifold discriminant analysis) pour identifier des images FKP.

En LDA, la matrice de dispersion interclasse est déterminée par les grandes distances entre les moyennes de classe, alors que, l'influence des distances entre les moyennes de classe est ignorée. En outre, chaque échantillon dans chaque classe a une contribution différente dans la matrice de dispersion intra-classe, qui est également ignorée dans la LDA. Pour pallier ces inconvénients, ils ont proposé une méthode MMDA pour l'extraction des caractéristiques et la reconnaissance de visage.

L'idée de MMDA est de garder l'étiquetage de classe après intégration ou apprentissage des sous-espaces. En d'autres termes, dans la dérivé du sous-espace de faible dimension MMDA, nous nous attendons à ce que les points soient encore proches si elles sont de la même classe, et les points de différentes classes soient aussi loin que possible les uns des autres.

À cette fin, nous définissons deux types de graphes en MMDA : un graphe Gw intra-classe et un autre graphe Gb interclasse, avec N nœuds et C nœuds respectivement. Le graphe intra-classe caractérise l'information sous-collecteur de chaque catégorie et le graphe interclasse caractérise l'information multi-collecteur de différentes classes.

Dans la première expérience, ils comparent uniquement certaines méthodes globales sur la base d'images FKP d'index gauche. Selon le protocole de cette base de données, les images capturées à la première session sont utilisées pour l'apprentissage et les images capturées à la deuxième session pour les tests. Ainsi, pour chaque classe, il y a six échantillons d'apprentissage et six échantillons de test. La PCA, LDA, LPP, locale PCA (LPCA), et MMDA sont utilisées pour l'extraction de caractéristiques FKP. Après extraction de caractéristiques, un classificateur du plus proche voisin qui utilise la distance en cosinus est

appliqué comme module de décision. De cette expérience, nous constatons que la MMDA a le taux de reconnaissance le plus élevé.

Dans la deuxième expérience, ils utilisent les quatre doigts. D'après les résultats, nous pouvons constater que le taux de reconnaissance du doigt du milieu est plus élevé que l'index.

3.6.3 L'OCLPP [25]

Afin de mettre en évidence les distinctions entre les angles et les différentes données, et d'améliorer l'information complémentaire des angles par rapport à la distance, Xiaoyuan et al. ont proposé un nouveau type de mesure d'angle d'image dans un espace d'image décalée qui est centré sur les données signifiantes. L'angle et la distance sont fusionnés en utilisant la stratégie de fusion parallèle, en se basant sur la CLPP (Complex Locality Preserving Projections) pour extraire des caractéristiques de faibles dimensions qui peuvent mieux préserver la structure du collecteur de l'ensemble de données d'entrée. Afin d'éliminer les informations redondantes parmi les caractéristiques, ils étendent davantage de la CLPP à l'approche OCLPP, qui produit des fonctions de base orthogonales.

Sur la base de données PolyU FKP, ils ont comparé leur projet « OCLPP » et CLPP avec LPP traditionnelle, PCA et CPCA.

D'après les résultats, nous pouvons constater que la méthode proposée OCLPP dispose d'un taux de reconnaissance supérieur, la LPP a de meilleures performances que la PCA et les méthodes LPP complexes dispose de meilleures performances que les méthodes LPP traditionnelles.

4. COMPARAISON

Tableau 2.1 Comparaison entre les différents algorithmes utilisés en reconnaissance de la FKP

N° de Référence	La base de données utilisée	L'algorithme utilisé	Performance
[14]	PolyU	BL-POC	EER de 1.68%
[18]	PolyU	La DCT-2	Mode vérification EER=7.60% Mode d'identification EER= 3.33%
[19]	PolyU	SURF	Précision de : 90.63% (vérification) et de 96.91%(l'identification) Et un « average matching time » qui est de 0.531s (vérification) et 0.106s (l'identification)
[20]	IIT Delhi	PHT+SURF	EER = 1.02%
[22]	PolyU	Gabor feature fusion (PCA + LDA)	Taux de reconnaissance (LM)=61.92
[21]	PolyU	Les ondelettes de Gabor	FAR = 1.24, FFR =1.11
[25]	PolyU	OCLPP	Taux de reconnaissance moy(LM)= 87.49
[23]	PolyU	Gabor + OLDA	Taux de reconnaissance (LM)=95.88
[24]	PolyU	Gabor + MMDA	Taux de reconnaissance moy(LM)=95.26

D'après le tableau de comparaison ci-dessus, on constate que chacune des méthodes proposées par les chercheurs a un avantage. Il y a celle qui est plus rapide que les autres comme la SURF. Donc, elle présente un temps de calcul relativement petit pour les deux modes de vérification et d'identification «**0.531s** et **0.106s** respectivement » et une précision importante de "**90.63%**". En comparant les "EER" obtenus par les méthodes PHT+SURF, BL-POC et la DCT-2, on voit que la fusion de la PHT avec la SURF donne le meilleur EER (à mentionner qu'ils ont travaillé avec une autre base de données). Plusieurs chercheurs qui ont été intéressés par cette modalité ont utilisé la fonction de Gabor avec d'autres méthodes globales comme la PCA, LDA, OLDA, MMDA. Parmi tous ces travaux, la fusion de la fonction de Gabor avec la MMDA donne le meilleur taux de reconnaissance «**T= 95.88%**».

5. CONCLUSION

Dans ce chapitre, nous avons présenté une nouvelle méthode de reconnaissance qui se base sur la modalité récente « FKP ». On a présenté aussi quelques algorithmes utilisés dans cette méthode pour l'extraction des caractéristiques des images FKP (filtre de Gabor, ondelette de Gabor, SURF, DCT, BL-POC) et une com0paraison entre ces algorithmes est faite. Il existe aussi d'autres algorithmes qui ont été développés pour améliorer les performances du système de reconnaissance (EER, la vitesse de traitement, la robustesse … etc.) comme les méthodes basées codage «coding-based methods». On va aborder deux parmi ces algorithmes dans le chapitre suivant de notre travail.

Chapitre 3 Système de reconnaissance FKP

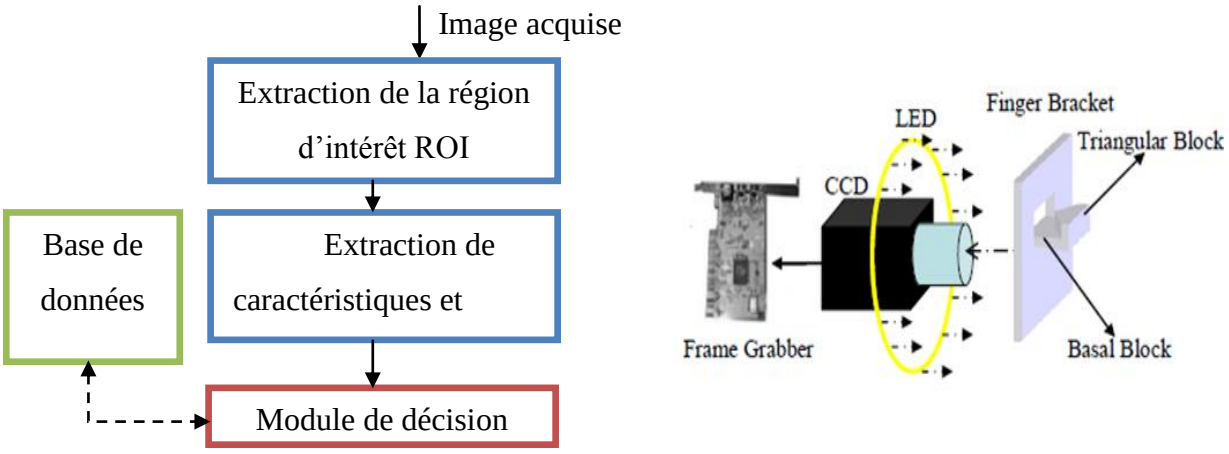
1. INTRODUCTION

Comme on a vu dans le chapitre précédant, il existe plusieurs méthodes d'extraction des caractéristiques utilisées. Parmi celles-ci il y a les méthodes de codage à base qui ont été largement utilisées et avec succès surtout après les bonnes performances de l'IrisCode inventé par Daugman dans la reconnaissance de l'iris. Par rapport aux autres méthodes, les méthodes de codage à base présentent de nombreux avantages comme la haute précision, la robustesse aux variations d'éclairage et la rapidité de l'extraction de caractéristiques et d'appariement.

Dans ce chapitre, on va faire une brève étude des méthodes de codage de base. On présente par la suite le système de reconnaissance de la FKP, la base de données utilisée, l'étape d'extraction de la région d'intérêt ainsi que les deux codes proposés pour l'extraction de caractéristiques et l'appariement.

2. DESCRIPTION GLOBALE DU SYSTEME DE RECONNAISSANCE

Le schéma de principe du système d'authentification personnelle basé sur la FKP est représenté sur la figure 1. Il est composé d'un module d'acquisition de données et un module de traitement de données. Ce système est proposé par Zhang et al. [26].



(a) Module de traitement de données **(b) Module d'acquisition de données**

Figure 3.1 Structure du système d'authentification personnelle basé sur la FKP

3. BASE DE DONNEES ET SYSTEME D'ACQUISITION [28]

Les images utilisées dans notre étude sont celles de la base de données PolyU (Université polytechnique de Hong Kong), cette base de données est disponible dans la référence [29].

Ces images FKP ont été recueillies en deux sessions distinctes à partir de 165 volontaires, dont 125 hommes et 40 femmes. Parmi eux, 143 avaient entre 20 et 30 ans et les autres entre 30 et 50 ans. Pendant chaque séance, il est demandé aux sujets (individus) de fournir 6 images pour chacun des doigts de la main : l'index gauche, le majeur gauche, l'index droit et le majeur droit, donc 48 images des 4 doigts ont été prélevés pour chaque sujet. Au total, la base contient 7920 images à partir de 660 doigts différents. L'intervalle du temps moyen entre la première et la deuxième session était d'environ 25 jours. L'intervalle maximal et minimal de temps était de 96 jours et 14 jours respectivement.

Le module d'acquisition utilisé pour capturer les images de cette base de données est composé d'un support de doigt, un anneau de source de lumière LED, une lentille, une caméra CCD et une carte d'acquisition.

Le problème qui se pose est de savoir comment faire le geste du doigt pour qu'il soit à peu près constant, de sorte que les images FKP capturées du même doigt seront cohérentes. Dans ce système, le support du doigt est conçu à cet effet.

En se reportant sur la figure 02 et la figure 01 (b), on peut voir un bloc de base et un bloc triangulaire qui sont utilisés pour fixer la position de l'articulation du doigt. Dans l'acquisition des données, l'utilisateur peut facilement mettre son doigt sur le bloc de base avec la phalange moyenne et la phalange proximale, il touche les deux versants du bloc triangulaire. Une telle conception a pour but de réduire les variations de la position spatiale du doigt de capture dans des sessions différentes. Le bloc triangulaire est aussi utilisé pour limiter l'angle entre la phalange proximale et la phalange moyenne, dans une certaine amplitude de sorte que les caractéristiques de la ligne de la surface d'articulation doigt peuvent être clairement imagées.

Figure 3.2 Appareil d'acquisition des images FKP

4. MODULE DE TRAITEMENT

L'image FKP capturée est entrée dans le module de traitement de données, qui comprend trois étapes de base: l'extraction de la région d'intérêt « ROI », l'extraction de caractéristiques et le codage, et le module de décision.

4.1 Extraction de la région d'intérêt

La phase d'extraction de la région d'intérêt est très nécessaire pour réduire considérablement les variations causées par les différentes poses du doigt dans la collecte des données. Par l'alignement des différentes images FKP et la normalisation des zones d'extraction de caractéristiques, des images de région d'intérêt ROI peuvent être rangées à partir de l'image originale en vue d'avoir des modules d'extraction de caractéristiques et de décision plus fiables. Donc, seule la région qui contient les caractéristiques va être traitée. Cette phase consiste à déterminer un système de coordonnées qui contient les étapes suivantes :

4.1.1 Prétraitements

Cette étape est déjà faite pour les images de la base de données. Ils ont appliqué un filtre de lissage gaussien sur l'image d'origine après un sous-échantillonnage de l'image lissée pour diminuer sa résolution (au début étant de 400 dpi) car le traitement suivant ne nécessite pas une grande résolution. Et pour trouver la résolution optimale qui satisfait les

performances désirées, ils ont fait des expériences sur une partie de la base de données pour différentes résolutions (200 dpi ,170 dpi, 150 dpi, 120 dpi, 100 dpi) et ils ont trouvé que la résolution 150 dpi donne les meilleurs résultats. Cette opération à deux avantages :

- Elle permet de réduire considérablement le coût du calcul par la réduction de la quantité des données.
- Le lissage gaussien supprime le bruit dans l'image d'origine, ce qui peut faciliter les étapes qui suivent (comme l'extraction de caractéristiques). Figure 3(a)

4.1.2 Détermination de l'axe X du système de coordonnées

On peut considérer que l'axe X du système de coordonnées comme la limite inférieure du doigt car elle est stable pour toutes les images FKP (le doigt est toujours mis sur le bloc de base lorsque l'image est capturée), et cette limite peut être facilement extraite par un détecteur de contour de Canny. Figure 3(b)

4.1.3 Coupage d'une sous-image IS de l'image I_D

Pour faciliter le traitement de l'image dans les étapes suivantes, on doit diminuer la taille de nos images. Les limites inferieures et supérieures de l'image découpée sont estimées selon la largeur des vrais doigts et les limites droite et gauche sont des valeurs fixes évaluées empiriquement. Figure 3(c)

4.1.4 Détection de contour

On applique le détecteur de contour de Canny une autre fois sur l'image coupée. Figure 3(d)

4.1.5 Codage de la direction de convexité

En se basant sur l'observation, on constate que les lignes caractéristiques autour de l'articulation phalangienne ont deux types de convexité (généralement les lignes droites ont une convexité droite et lignes gauches ont une convexité gauche) et pour faciliter la détermination de l'axe Y, on fait un codage de direction de convexité pour chaque pixel. Le principe de ce codage est de donner la valeur « 1 » au pixel de convexité gauche, la valeur « -1 » au pixel de convexité droite et la valeur « 0 » au pixel qui n'a aucune convexité. Figure 3(e)

L'algorithme de ce code est donné comme suit :

$entrées : I_E$

$sorties : I_{CD}$

$Début :$

$y_{mid} = \frac{height\ of\ I_E}{2}$;

$pour\ tout\ I_E(i,j) faire$

$si\ I_E(i,j) = 0$

$I_{CD}(i,j) = 0;$

$sinon\ si\ I_E(i+1,j-1) = 1\ et\ I_E(i+1,j+1) = 1$

$I_{CD}(i,j) = 0;$

$sinon\ \ si\ I_E(i+1,j-1) = 1\ et\ i \leq y_{mid}\ où\ \ I_E(i+1,j+1) = 1\ et\ i > y_{mid}$

$I_{CD}(i,j) = 1;$

$sinon\ si\ I_E(i+1,j+1) = 1\ et\ i \leq y_{mid}\ où\ \ I_E(i+1,j-1) = 1\ et\ i > y_{mid}$

$I_{CD}(i,j) = -1;$

$fin\ si$

$fin\ pour$

$fin\ programme$

4.1.6 Détermination de l'axe Y du système de coordonnées

Comme on a déjà dit que la plupart des lignes (courbes) de la partie gauche ont une convexité gauche et les lignes de la partie droite ont une convexité droite, il existe une petite zone autour de l'articulation phalangienne qui n'a pas de convexité. Donc, après le codage de direction de convexité, on peut définir l'amplitude de convexité qui nous permet de mesurer la force de la direction de convexité dominante dans une région locale comme :

$$conMag(x) = abs(\sum_W I_{CD}) \qquad (3.1)$$

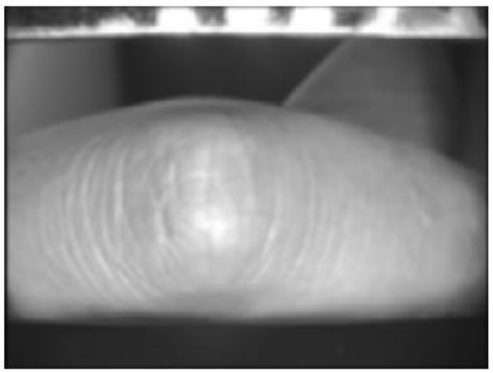
Tel que $W = d \times h$ est une fenêtre symétrique autour de la colonne d'absice x,

Où h est l'hauteur de l'mage I_s, et d est choisi empiriquement comme égale à 35. D'après les caractéristiques précédemment citées des images FKP, cette fonction

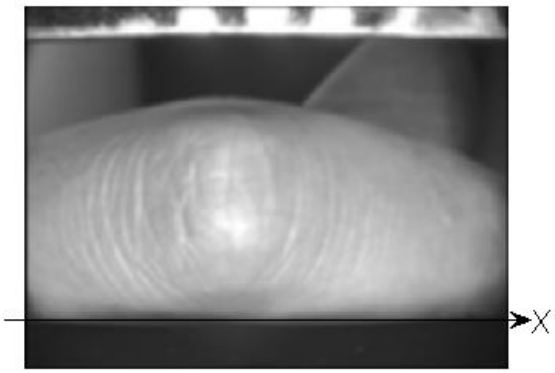
« $conMag(x)$ » possède un minimum autour du centre de l'articulation phalangienne. On peut donc facilement définir l'axe Y du système de coordonnées qui correspond à la position de ce minimum « x_0 » : $x_0 = argmin(conMag(x))$

4.1.7 L'image de la région d'intérêt ROI

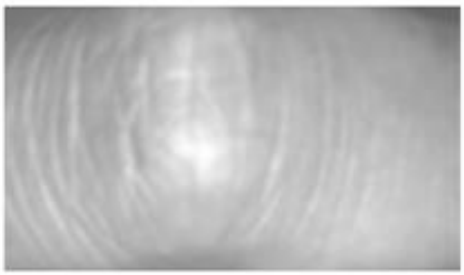
Maintenant que nous avons fixé les axes X et Y, le système de coordonnées local peut alors être déterminé. En se reportant sur la figure 3(h), on remarque que l'image ROI peut être extraite à partir de l'image Id avec une taille qui est fixée de manière empirique à 110 × 220 dans notre système.



(a) L'image après prétraitement

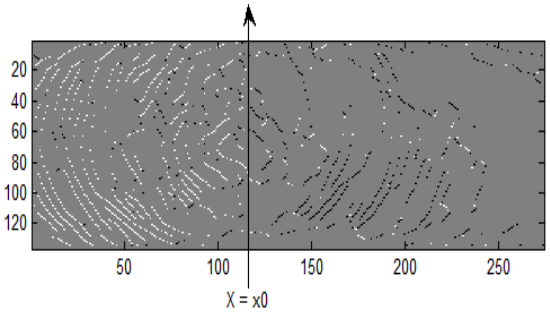


(b) Localisation de l'axe X

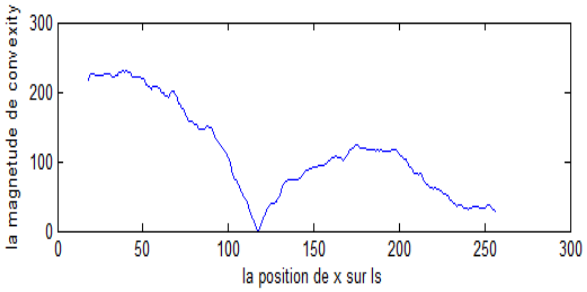


(c) La sous-image I_S

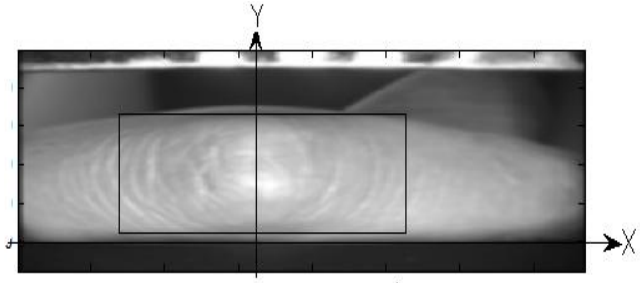
(d) Application du détecteur de contour de Canny sur I_S



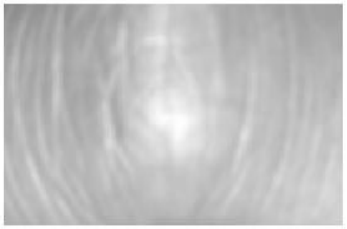
(e) Le codage de l'image I_S



(f) Le graphe de la fonction « conMag »



(g) La partie à rogner de l'image I_D



(h) L'image ROI

Figure 3.3 Les différentes étapes de l'extraction de la région d'intérêt ROI

4.2 Extraction des caractéristiques [27, 28]

Dans cette étape « l'extraction des caractéristiques », on va pratiquer l'un des algorithmes les plus utilisées « méthodes de codage à base », ces méthodes consistent à donner un code pour chaque pixel de l'image après filtrage. Le filtre que l'on va appliquer est celui de Gabor.

La technique de filtrage de Gabor peut extraire simultanément les données de fréquence spatiale du signal d'origine. Depuis les années 1980, il a été largement utilisé comme un outil efficace pour réaliser le module d'extraction de caractéristiques dans les systèmes biométriques tels que: le visage, l'iris et les empreintes digitales…etc. A l'aide du filtre de Gabor, on peut générer trois types de caractéristiques: phase, amplitude et orientation, que l'on peut utiliser séparément ou combinées dans des systèmes différents.

La fonction de Gabor a plusieurs formes dans la littérature. La forme qu'on va adopter est celle qui est utilisée dans la référence [28] :

$$G(x,y) = \exp\left(-\frac{1}{2}\left(\frac{x'^2}{\sigma_x^2}+\frac{y'^2}{\sigma_y^2}\right)\right).\exp(i2\pi f x) \qquad (3.2)$$

Où : $x' = xcos\theta + ysin\theta$; $y' = -xsin\theta + ycos\theta$

f: La fréquence du facteur sinusoïdale

θ: L'orientation de la normale

$\sigma_x et\ \sigma_y$: Sigma de l'enveloppe gaussienne des deux dimensions x et y.

4.2.1 Code compétitif (CompCode)

L'idée de base du Code Compétitif est d'extraire le domaine d'orientation pour chaque pixel comme caractéristique et la codé par un code binaire. par la convolution de l'image avec la partie réelle de « J » filtres de Gabor qui diffèrent par leurs paramètres d'orientation θ= jπ/J tel que j={0, 1, 2, 3, 4, J-1} où « J » représente le nombre des différents orientations, l'information d'orientation locale de l'image pour chaque pixel peut être extraite et codée mathématiquement comme suit :

Et basant sur les résultats de Lin [] l'utilisation de 6 filtre de Gabor (J=6) sa suffi

$$CompCode(x,y) = arg_J \ min\{I_{ROI}(x,y) * G_R(x,y,\theta_J)\} \quad (3.3)$$

Où * désigne l'opération de convolution et θ_J = jπ/6, j = {0, ..., 5}, G_R c'est la partie réelle du filtre de Gabor.

Ensuite, l'orientation dominante {0, π/ 6 , π / 3 , π/ 2 , 2π / 3, 5 π/ 6 } sera encodé avec trois bits {000,001, 011, 111, 110, 100} pour une représentation efficace.

4.2.2 ImCompCode et MagCode

Dans cet algorithme, nous proposons une méthode combinant l'orientation et l'amplitude pour la reconnaissance des images FKP.

- Codage compétitifs améliorée (ImCompCode) pour l'extraction des caractéristiques d'orientation

Ce code une amélioration du code compétitif « CompCode » original. Car souvent sur une image FKP, il y a quelques pixels qui se trouvent sur des zones relativement "planes", c'est à dire que ces pixels ne résident pas dans toutes les lignes et par conséquent on ne peut pas avoir une orientation dominante. En conséquence, les réponses du filtre de Gabor pour ces pixels n'ont pas beaucoup de variations. Si, de plus, nous attribuons un code d'orientation, ce code peut ne pas être stable et sera sensible au bruit, ce qui rend la performance des modules d'extraction de caractéristiques et de décision faible. Par conséquent, ces pixels "planes" devraient être retirés du codage d'orientation. Nous définissons « l'amplitude d'orientation» à un pixel comme:

$$oriMag(x,y) = \frac{abs(\max(R) - \min(R))}{\max(abs(\max(R), abs(\min(R))} \quad (3.4)$$

Où R =$\{R_j = I_{ROI}(x,y) * G_R(x,y,\theta_j)\}$, j = {0, ..., 6} sont le filtrage des réponses à ce pixel Gabor.

L'amplitude d'orientation OriMag (x, y) peut mesurer la façon dont le pixel (x, y) a une orientation dominante. Si elle est inférieure à un seuil, nous estimons que le pixel n'a pas d'orientation dominante et le code compétitif correspondant est affecté à 6.

$entrées : I_{ROI}\ (m \times n)$

$sorties : ImCompCode$

$Début :$

$pour\ tout\ I_{ROI}(x,y) faire$

$R = R_j\ \{I_{ROI}(x,y) * G_R(x,y,\theta j)\}$ Tel que $\theta_j = \frac{j\pi}{6}, j = \{0,1, \dots 5\}$

$$oriMag(x,y) = \frac{abs(\max(R) - \min(R))}{\max(abs(\max(R), abs(\min(R))}$$

$si\ oriMag < T$ T : un seuil choisi expérimentalement

$ImCompCode(x,y) = 6;$

$sinon$

$ImCompCode(x,y) = arg_j\ min\ (R_j);$

$fin\ si$

$fin\ pour$

$fin\ programme$

- Codage d'amplitude (MagCode) pour l'extraction de caractéristiques d'amplitude

Outre des informations d'orientation, nous voulons aussi exploiter les informations d'amplitude des réponses des filtres de Gabor. L'amplitude de la réponse du filtre de Gabor appliquée au pixel IROI (x, y) est :

$$\sqrt{\left(I_{ROI}(x,y) * G_R(x,y,\omega,\theta_j)\right)^2 + \left(I_{ROI}(x,y) * G_I(x,y,\omega,\theta_j)\right)^2} \quad (3.5)$$

Où GR et GI représente la partie réelle et la partie imaginaire de la fonction de Gabor G respectivement. Nous utilisons encore la partie réelle du filtre de Gabor et définissons l'amplitude au pixel IROI (x, y) comme suit:

$$mag(x,y) = \max_j \left(abs\left(I_{ROI}(x,y) * G_R(x,y,\theta_j)\right)\right) \quad (3.6)$$

Ensuite, une quantification localisée est appliquée à mag (x, y) pour obtenir le code d'amplitude. Ce processus peut être exprimé comme suit:

$$magCode(x,y) = ceil\left(\frac{mag(x,y) - lmin}{\frac{lmax - lmin}{N}}\right) \quad (3.7)$$

Où N est le nombre de niveaux de quantification, $lmin = min_{(x,y)\in Wm}(mag(x,y))$ et $lmax = max_{(x,y)\in Wm}(mag(x,y)$

Wm est une fenêtre w * w centré à (x, y). Le code d'amplitude qui en résulte est un entier entre 1 et N. W et N peuvent être réglés par des expériences sur un sous-ensemble de données et ils sont expérimentalement définis comme 31 et 8 dans le présent travail, respectivement.

5. MODULE DE DECISION

Cette étape consiste à calculer la distance entre l'image teste et les images de la base de données pour qu'on puisse décider de l'existence ou non de la personne et l'identifier dans le cas où il est accepté.

5.1 CompCode

L'appariement pour ce code se fait par le calcul de la distance de Hamming normalisée pour mesurer la similitude entre deux images codées.

Soit P et Q deux cartes de codes de deux images, leur distance de Hamming normalisée est donnée par la formule suivante :

$$d(P,Q) = \frac{\sum_{y=1}^{m}\sum_{x=1}^{n}\sum_{i=0}^{2}(P_i^b(x,y) \otimes Q_i^b(x,y)}{3S} \quad (3.8)$$

Où : m, n, S sont le nombre de lignes, le nombre de colonnes et la surface de carte des codes respectivement.

P_i^b et Q_i^b sont les valeurs du i^{ème} bit de P et Q.

$\otimes$ le ou exclusif.

5.2 ImCompCode et MagCode

Supposons que nous comparons les deux images FKP ROI, P et Q. Soient Po et Qo les deux codes d'orientation, Pm et Qm les deux codes d'amplitude. Dans un premier temps, nous calculons la distance de correspondance entre Po et Qo et la distance de correspondance entre Pm et Qm respectivement, puis nous fusionnons les deux distances pour avoir la distance de correspondance finale entre P et Q.

Lors du calcul de la distance de correspondance entre Po et Qo, nous adoptons la distance angulaire proposée dans [12], qui est définie comme suit:

$$angD(P,Q) = \frac{\sum_{y=1}^{Rows}\sum_{x=1}^{cols} G(P_0(x,y),Q_0(x,y))}{\left(\frac{J}{2}\right).S} \quad (3.9)$$

Où S est la surface du code, et

$$G\big(P_0(x,y),Q_0(x,y)\big) = \{\ 1, \quad si\ \ P_o(x,y) = 6\ et\ Q_0(x,y) \neq 6$$

$$1, \quad si\ \ P_o(x,y) \neq 6\ et\ Q_0(x,y) = 6$$

$$0, \quad si \quad P_0(x,y) = Q_0(x,y)$$

$$\mathrm{Min}\big(P_0(x,y) - Q_0(x,y), Q_0(x,y) - (P_0(x,y) - 6)\big),$$

$$si\ \ P_0(x,y) > Q_0(x,y)\ et\ P_o(x,y) \neq 6$$

$$\mathrm{Min}\big(Q_0(x,y) - P_0(x,y), P_0(x,y) - (Q_0(x,y) - 6)\big),$$

$$si\ P_0(x,y) < Q_0(x,y)\ et\ Q_o(x,y) \neq 6\ \} \qquad (3.10)$$

La distance de correspondance entre Pm et Qm est définie comme suit:

$$magD(P,Q) = \frac{\sum_{y=1}^{Rows}\sum_{x=1}^{cols} abs\big(P_m(x,y) - Q_m(x,y)\big)}{(N-1).s} \qquad (3.11)$$

Ensuite, la distance de correspondance finale entre P et Q peut être fusionnée à partir de angD et magD comme :

$$dist(P,Q) = (1-\lambda).angD(P,Q) + \lambda.\mathrm{magD(P,Q)} \qquad (3.12)$$

Où λ est utilisé pour contrôler la contribution de magD, il est expérimentalement fixé à 0,15 dans notre système.

6. CONCLUSION

En accord avec les étapes du flot de conception d'un système biométrique, nous avons d'abord fait l'étude du système d'authentification proposé. On a expliqué ainsi ces différents modules commençant par l'extraction de la région d'intérêt des images FKP acquises. Ensuite, le module de traitement où on a présenté deux méthodes de codages différentes pour l'extraction de caractéristiques avec leurs algorithmes de comparaison.

Dans le chapitre suivant, on s'intéressera aux résultats expérimentaux pour s'assurer par la simulation du bon fonctionnement de notre système.

Chapitre 4 Simulation et résultats du système de reconnaissance réalisé

1. INTRODUCTION

Ce chapitre est dédié à la partie programmation des deux algorithmes CompCode et ImCompCode & MagCode sur MATLAB. Le recours à ce langage, est essentiellement fait pour la validation et la vérification des deux algorithmes déjà vus dans le chapitre 3.

On commence par une présentation de la base de données utilisée. Puis, on donnera une description des étapes suivies pour la programmation des algorithmes CompCode et ImCompCode & MagCode en donnant aussi quelques résultats obtenus lors de la simulation.

On terminera par une évaluation des performances en termes d'EER, de taux de reconnaissance et de temps de calcul.

2. PRESENTATION DE LA BASE DE DONNEES UTILISEE

Nos expériences ont été faites sur des images de la base de données PolyU [26]. Il n'est pas suffisant d'utiliser la même base de données pour pouvoir honnêtement comparer des résultats. Il est nécessaire également de définir un protocole de test. La base de données est scindée en deux ensembles : ensemble d'apprentissage, ensemble de test. L'ensemble d'apprentissage est utilisé comme ensemble de référence, il contient 6 images pour chacun des quatre doigts pour 50 personnes. Il sert d'ensemble de base. L'ensemble de test permet de tester le système en utilisant 4 images de test pour chacun des quatre doigts pour 75 personnes. L'ensemble de test est divisé en deux classes : clients (50 personnes) et imposteurs (25 personnes).

3. CONCEPTION DU SYSTEME

Le système de reconnaissance FKP réalisé utilise l'algorithme CompCode pour la reconnaissance. Il va faire une mesure de similarité après l'extraction des caractéristiques FKP de test à partir de l'image présentée à l'entrée.

D'abord, le système doit identifier la personne, c.-à-d. que le système doit décider laquelle des images stockées dans la base de données ressemble plus à l'image à identifier.

Puis, il doit vérifier si elle appartient à la base de données ou non. En d'autres termes, le système doit décider si la personne est un client ou non.

Ensuite, nous avons essayé d'améliorer les résultats de la méthode CompCode en faisant une combinaison de l'ImCompCode (CompCode amélioré) avec le MagCode.

L'organigramme du système de reconnaissance réalisé est illustré sur la figure 4.1 et l'interface représentative du système est illustrée sur la figure 4.2.

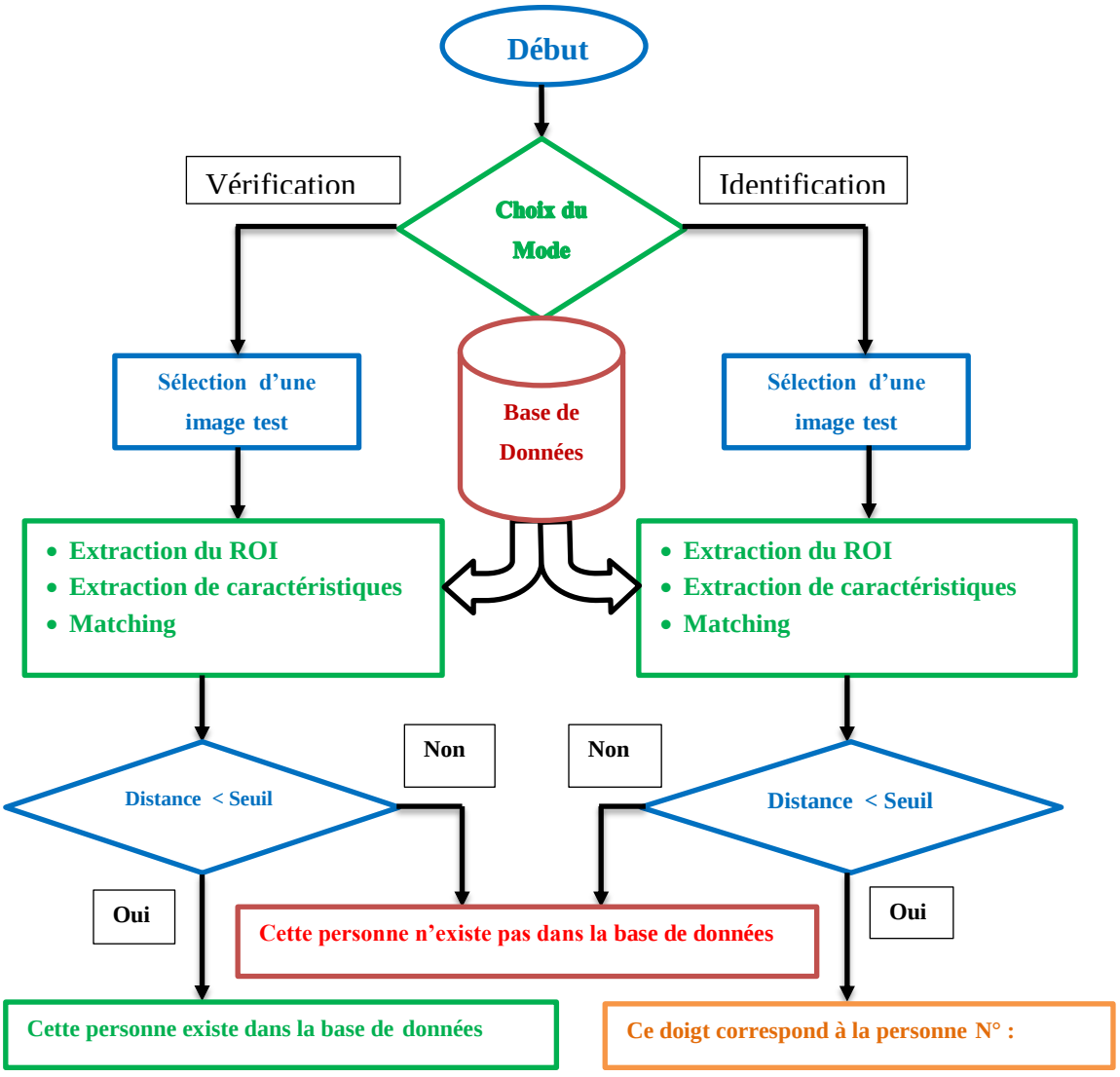


Figure 4.1 Le système de reconnaissance FKP réalisé

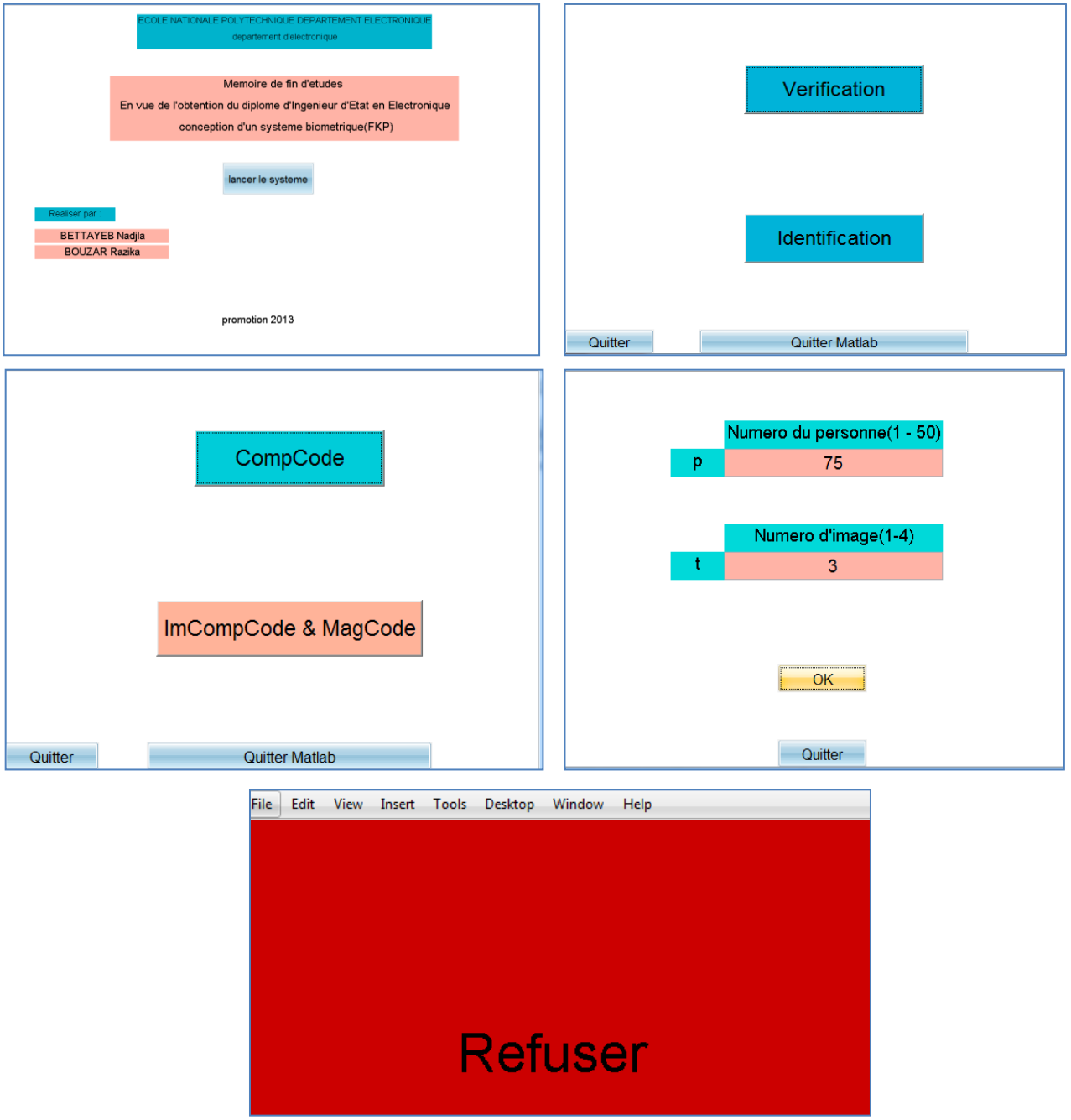


Figure 4.2 Interface graphique du système de reconnaissance FKP

4. ÉVALUATION DES PERFORMANCESES

Pour déterminer les performances du système de reconnaissance des images FKP se basant sur l'un des algorithmes vus précédemment, et pour les quatre doigts, plusieurs paramètres doivent être déterminés, comme :

FAR : le taux de fausses acceptations, c'est le nombre des imposteurs acceptés par le système sur le nombre total d'imposteurs.

FRR : le taux de faux rejets, c'est le nombre de clients légitimes refusés par le système sur le nombre total de clients légitimes.

ERR : le taux d'égale erreur qui est le point d'intersection entre le FAR et le FRR.

Taux d'identifications correctes (le taux de reconnaissance): le pourcentage des reconnaissances justes, c'est le nombre des tests correspondant à une identification correcte sur le nombre total de tests effectués.

Un autre paramètre qui peut être une bonne mesure de performance pour un système de reconnaissance, c'est le temps d'exécution. Car, le coût du système peut être un temps d'exécution, un nombre de cycles ou d'instructions ou une consommation.

On va commencer cette section par une présentation des résultats obtenus pour les taux de reconnaissance FAR, FFR pour différents seuil afin de tracer les courbes ROC (les taux de fausses acceptations (FAR) et de faux rejets (FRR) en fonction du seuil de décision) en déterminant ainsi l'ERR. Par la suite on exposera les taux d'identifications correctes obtenus. Et finalement, on évalue notre système en termes de temps de calcul et rapidité.

4.1 Taux de fausses acceptations FAR et Taux de faux rejets FRR

Pour mesurer le taux de fausses acceptations, on injecte au système de reconnaissance, des images de visage de personnes inconnues. Ce qui mène à enlever certaines personnes de la base de données lors de la phase de l'apprentissage pour pouvoir les utiliser lors des tests.

Ces personnes sont appelées imposteurs. Pour ce qui est du taux de faux rejets, on injecte au système de reconnaissance, des images de visage de personnes connues, c'est-à-

dire, les images de tests doivent appartenir aux personnes présentes dans l'ensemble d'apprentissage.

Ces personnes sont appelées clients. La mesure de FAR et FRR se fait en fonction d'un seuil de décision. Le seuil de décision permet au système d'accepter ou de rejeter une personne. Soit S ce seuil de décision; lors de la reconnaissance quand la distance minimale d entre l'image de test et celles de la base de données est déterminée, elle sera comparée à ce seuil S. Si d est inférieure à S, la personne sera acceptée et dans le cas contraire elle sera rejetée. Dans un système biométrique, on cherche toujours le seuil optimal permettant de donner FAR=FRR, dans le but d'équilibrer les erreurs dues aux fausses acceptations et aux faux rejets. Car, si le FAR est grand, le nombre d'imposteurs acceptés par le système sera élevé. Dans le cas où c'est le FRR qui est grand on aura un nombre élevé de clients rejetés par le système. On a procédé à deux expériences pour cela.

Dans ce qui suit, on cherche à comparer les deux algorithmes entre eux afin de déterminer lequel d'eux donne le plus faible ERR.

Dans la première expérience, on a utilisé la première méthode CompCode pour comparer entre les quatre doigts. Le tableau suivant résume les différents résultats obtenus lors de la recherche du seuil idéal donnant un FRR = FAR.

Tableau 4.1 Mesure du FAR et du FRR pour les quatre doigts

Seuil		0,15	0,151	0,152	0,153	0,154	0,155	0,156
FAR	**RI**	2,2	7	14	28	48	85	97
	RM	2,0	3	4,5	10	27	52	94
	LI	2,3	5	15	23	50	60,2	88
	LM	2,1	4,5	10	19	46	68,75	82
FRR	**RI**	85	55	20	14	12	9	7,0
	RM	75	54	19	11	8	6,5	3,5
	LI	92	78	26	19	14	12	8
	LM	77	56	18	13	10	7	5

Le Tableau 4.1 montre que le choix du seuil n'est pas une chose très facile, car si le seuil est très faible, on rejettera plusieurs utilisateurs légitimes ; même si on choisit un seuil élevé on aura un autre problème qui est l'acceptation de plusieurs imposteurs, la solution

idéale est d'essayer d'avoir un seuil qui donne un FAR = FRR. En se basant sur les courbes ROC (figure 4.3), le tableau 4.2 indique les EER obtenus pour les quatre doigts.

Tableau 4.2 EER (%) obtenus pour les quatre doigts (méthode 1 CompCode)

RI	RM	LI	LM
18	11	20	16

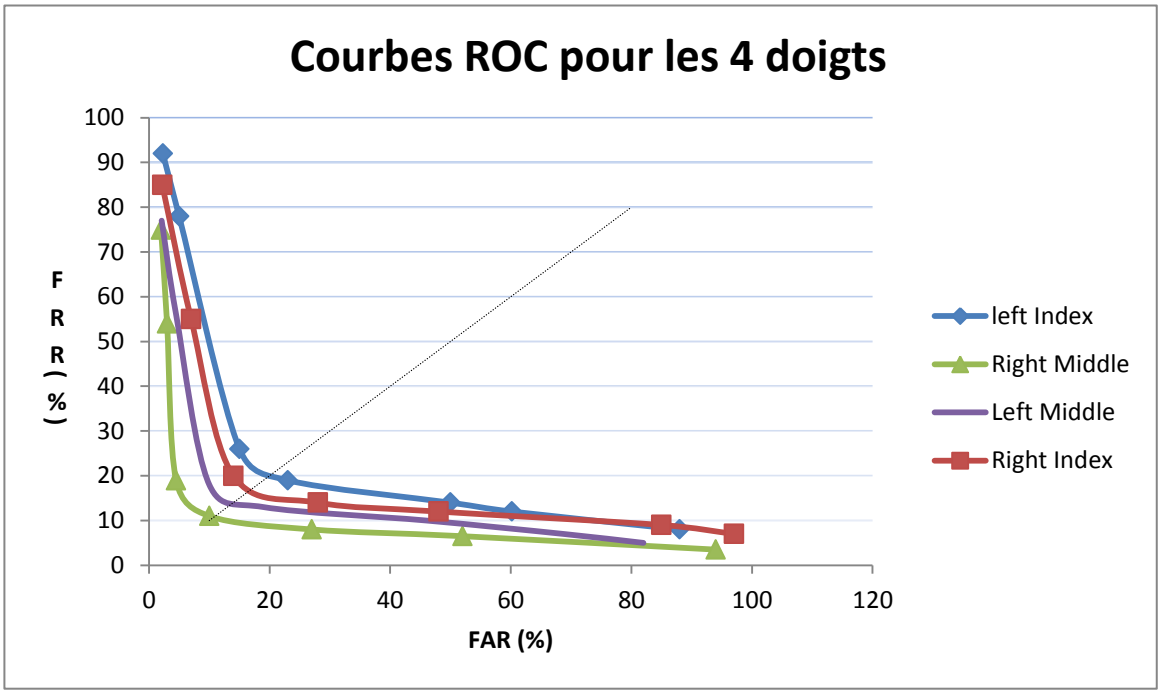


Figure 4.3 Courbes ROC pour les quatre doigts (méthode 1 CompCode)

- D'après les résultats obtenus, on peut constater que le majeur droit (RM) a le plus petit EER de **11%.** C'est probablement parce que la majorité des gens de la base sont droitiers et aussi le doigt du milieu a une faible mobilité.

Dans la deuxième expérience, on a comparé entre les deux méthodes implémentées CompCode et ImCompCode & MagCode. La comparaison se fait par le doigt qui a donné de bons résultats, le majeur droit. Le tableau ci-dessous résume les différents résultats obtenus lors de la recherche du seuil idéal donnant un FRR = FAR.

Tableau 4.3 Mesure du FAR et du FRR pour les deux méthodes

Seuil	0,29	0,3	0,31	0,32	0,33	0,34	0,345	0,35
FAR	0	0,09	0,5	1	2,46	8	40	90
FRR	88	72	60	55	28	9	5	3

En se basant sur les courbes ROC obtenues pour les deux méthodes (figure 4.3), on déduit un EER de **11%** pour la première méthode CompCode et un EER de **9%** pour la deuxième ImCompCode & MagCode.

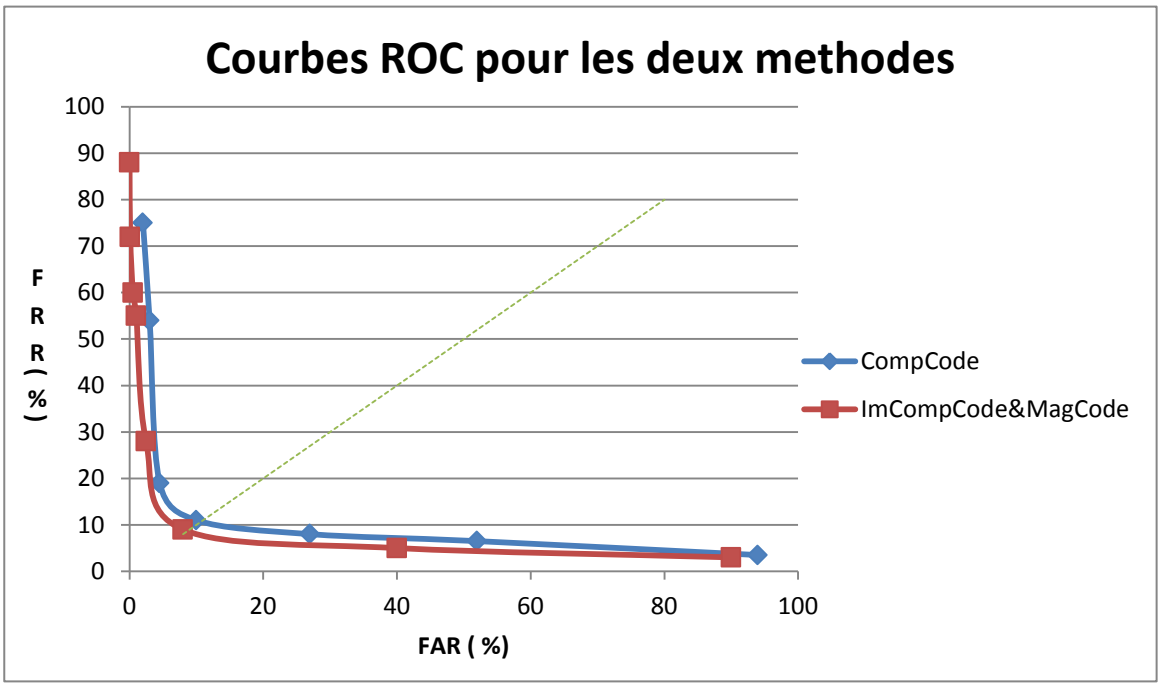


Figure 4.4 courbes ROC pour les deux méthodes

CompCode et ImCompCode & MagCode

- D'après les résultats obtenus, on peut constater que la deuxième méthode donne de bonnes performances en termes d'EER. Donc, il est clair que la méthode basée codage ImCompCode & MagCode est meilleure.

4.2 Taux d'identification

Pour déterminer le taux d'identifications correctes, les images de tests utilisées doivent appartenir aux personnes présentes dans l'ensemble d'apprentissage, autrement dit, on ne va pas utiliser pour le test des images de personnes inconnues.

Le taux d'identification nous indique le nombre de fois où le système a bien reconnu la personne de test. Pour le mesurer on utilise la totalité de la base de données, il est alors égal à la moyenne des taux d'identifications correctes obtenus lors de chaque calcul, c'est-à-dire lors de chaque test.

Tableau 4.4 Les taux d'identification des deux méthodes

Méthode	**CompCode**				**ImCompCode & CompCode**
Doigts	**LI**	**LM**	**RI**	**RM**	**RM**
TI (%)	**56**	**90**	**72**	**92**	**94**

Le tableau ci-dessus montre que le taux d'identification obtenu par la méthode ImCompCode & MagCode est relativement élevé par rapport à la méthode CompCode. Le doigt majeur droit donne toujours de meilleures performances en termes de taux d'identification.

4.3 Rapidité du système et temps de calcul

Dans une seconde étape, le temps d'exécution (ou temps de calcul) est une bonne mesure de performance pour un système de reconnaissance qui a été simulé par un logiciel de traitement.

Pour déterminer le temps de processeur utilisé dans certaines fonctions, on peut manuellement ajouter dans le code des instructions de chronométrage du temps consommé existant dans MATLAB.

Première méthode : CompCode

Temps Minimum : 2.4744 s, temps Maximum : 316.2120 s = 5°16',

Temps moyen du système de vérification : 159.3432 s

Temps du système d'identification : 348.9893 s =5°48'

Deuxième méthode : ImCompCode & MagCode

Temps du système d'identification : 494.7960 s = 8°14'

Temps Minimum : 6.8s, temps Maximum : 500.944 s = 8°20',

Temps moyen du système de vérification : 253.8931 s = 4°13'

5. CONCLUSION

Les résultats obtenus concernant les différents taux de reconnaissance avec l'algorithme CompCode sont moyens et peuvent être améliorés pour atteindre de meilleurs résultats par l'algorithme ImCompCode & MagCode. Mais ce dernier a un temps de calcul important. Il existe d'autres techniques qui pourraient aussi améliorer la performance du système biométrique comme l'utilisation de la multimodalité.

Conclusion générale

La biométrie est une technologie en plein essor. Elle est de plus en plus utilisée dans les applications en relation avec la sécurité, vu les avantages qu'elle offre contrairement aux anciennes méthodes.

Après avoir introduit les principes fondamentaux de la biométrie et présenté les systèmes biométriques ainsi que les différentes modalités existantes, nous nous sommes intéressés aux différents algorithmes utilisés dans la reconnaissance FKP en présentant un état de l'art sur cette modalité. Par la suite, nous avons étudié en détail les méthodes basées codage.

L'objectif principal du travail effectué est de tester la fiabilité de cette modalité en faisant une comparaison entre deux algorithmes CompCode et ImCompCode & MagCode. La comparaison a été basée sur leurs performances. Ces performances sont traduites par le taux d'identifications correctes, le taux d'égale erreur (ERR) et le temps de reconnaissance.

Après comparaison, nous avons constaté que le meilleur algorithme, parmi ceux utilisés, est la fusion de l'ImCompCode « CompCode amélioré » avec le MagCode. Cet algorithme assure un taux d'identifications correctes de 94%. Cependant, Le taux d'égale erreur n'est pas suffisamment faible (EER = 9%).

Comme amélioration à ce travail, nous proposons l'utilisation de la multimodalité, en combinant cette modalité « FKP » avec d'autres techniques biométriques (La géométrie de la main, l'empreinte digitale …), car les systèmes multimodaux assurent des bonnes performances.

Et dans le but d'améliorer le temps de reconnaissance tout en gardant les mêmes performances, il est souhaitable de penser à une architecture matérielle travaillant en parallèle telle que les cartes FPGA. L'utilisation de ce genre de matériel est prise essentiellement pour leur flexibilité et le temps de traitement réduit qu'ils offrent.

Bibliographie

[1] Lorène ALLANO. La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles. Thèse de doctorat, INSTITUT NATIONAL DES TELECOMMUNICATIONS. France (2009)

[2] Bernadette DORIZZI, Jean LEROUX LES JARDINS, Philippe LAMADELAINE, Claudine GUERRIER. La biométrie - Techniques et usages. Technique de l'ingénieur, 2004.

[3] Nicolas MORIZET. Reconnaissance biométrique par fusion multimodale du visage et de l'iris. Thèse de doctorat, Ecole Nationale Supérieure des Télécommunications, 2009.

[4] Florent PERRONNIN, Jean-Luc DUGELAY. Introduction à la biométrie, Authentification des individus par traitement audio-vidéo. Technique de l'ingénieur, 2002.

[5] Bernadette DORIZZI. Techniques et usages biométriques. Cour Institut national des télécommunications, France 2004.

[6] Christel-Loïc TISSE, Lionel MARTIN, Lionel TORRES, Michel ROBERT. Système automatique de reconnaissance d'empreintes digitales, Sécurisation de l'authentification sur carte à puce, France.

[7] DANG Hoang Vu. Biométrie pour l'identification, Rapport final du tipe. Institut de la Francophonie pour l'Informatique Vietnam, 2005.

[8] Julien Doublet, Marinette Revenu, Olivier Lepetit. Reconnaissance biométrique sans contact de la main intégrant des informations de forme et de texture, France.

[9] Shermin Bazazian, Marina Gavrilova. Context based gait recognition. SPIE Vol. 8407 84070J-2, Canada, 2012.

[10] Jinyan Chen, Rongteng Wu. Two-dimensional PCA based human gait identification SPIE Vol. 8558 85580D-1, China, 2012.

[11] John R. Vacca. Biometric technologies and verification systems. BH Elsevier, 2007.

[12] Anil K. Jain, Patrick Flynn, Arun A. Ross. Handbook of Biometrics, Springer 2008.

[13] Ravi Das. Keystroke recognition, Keesing Journal of Documents & Identity, issue 26, 2008.

[14] Lin Zhang, Lei Zhang, and David Zhang. Finger-Knuckle-Print Verification Based on Band-Limited Phase-Only Correlation. CAIP 2009.LNCS 5702,pp.141-148, Springer-Verlag Berlin Heidelberg, 2009.

[15] Mrs. S.S. Kulkarni1, Dr.Mrs.R.D.Rout. Secure Biometrics: Finger Knuckle Print. International Journal of Advanced Research in Computer and Communication EngineeringVol. 1, Issue 10, 2012.

[16] D.L. Woodard, PJ. Flynn. Finger surface as a biometric identifier, Computer Vision and Image Understanding, vol. 100, pp. 357-384, 2005.

[17] A Kumar and Y. Zhou. Human identification using knuckle codes, Proc. IEEE. Biometrics: Theory, Applications and Systems, pp. 1-6, 2009.

[18] Mohammed Saigaa, Abdallah Meraoumia, Salim Chitroub, Ahmed Bouridane. Efficient Person Recognition by Finger-Knuckle-Print Based on 2D Discrete Cosine Transform. International Conference on Information Technology and e-Services, IEEE, 2012.

[19] ZHU Le-qing. Finger knuckle print recognition based on SURF algorithm. Eighth International Conference on Fuzzy Systems and Knowledge Discovery, IEEE, 2011.

[20] Michał Choraś, Rafał Kozik. Knuckle Biometrics for Human Identification. Image Processing & Communications Challenges 2, AISC 84, pp. 91–98. Springer-Verlag Berlin Heidelberg, 2010.

[21] Chetana Hegde, P Deepa Shenoy, Venugopal K R, L M Patnaik. FKP Biometrics for Human Authentication Using Gabor Wavelets, IEEE, 2011.

[22] Zahra S. Shariatmadar, Karim Faez. A Novel Approach for Finger-Knuckle-Print Recognition Based on Gabor Feature Fusion. 4th International Congress on Image and Signal Processing, IEEE, 2011.

[23] YANG Wankou, SUN Changyin, SUN Zhongxi. Finger-Knuckle-Print Recognition Using Gabor Feature and OLDA. 30th Chinese Control Conference, China, 2011.

[24] Wankou YANG, Changyin SUN, Zhenyu WANG. Finger-knuckle-print recognition using Gabor feature and MMDA. Front Electr Electron Eng China, Higher Education Press and Springer-Verlag Berlin Heidelberg, 2011.

[25] Xiaoyuan Jing, Wenqian Li, Chao Lan, Yongfang Yao, Xi Cheng, Lu Han. Orthogonal Complex Locality Preserving Projections based on Image Space Metric for Finger-Knuckle-Print Recognition, 978-1-4577-0490-1 IEEE, 2011.

[26] Lin Zhang, Lei Zhang, David Zhang. FINGER-KNUCKLE-PRINT: A NEW BIOMETRIC IDENTIFIER. Biometrics Research Center, Department of Computing, The Hong Kong Polytechnic University, Hong Kong, China. 978-1-4244-5654-3IEEE, 2009.

[27] Jing Wei, Wei Jia, Hong Wang, and Dan-Feng Zhu. Improved Competitive Code for Palmprint Recognition Using Simplified Gabor Filter, Springer-Verlag Berlin Heidelberg, 2009

[28] http://www.comp.polyu.edu.hk/~biometrics/FKP.htm

[29] Lin ZHANG. Personal Authentication Using Finger-Knuckle-Print. Thèse de doctorat. Université Polytechnique de Hong Kong. 2011.

Annexes

1. Filtre de Canny

La détection de contour est une étape préliminaire dans le traitement d'image qui consiste à trouver les variations brusques d'intensité lumineuse dans une image. Le filtre de Canny est l'une des techniques les plus utilisée dans la détection de contours. Elle a été développée par John F. Canny en 1986, pour être optimale aux critères suivants :

- Bonne détection : faible taux d'erreur dans la signalisation des contours et maximisation du rapport signal sur bruit.

- Bonne localisation : des distances minimales entre les contours détectés et les contours réels.

- Unicité de la réponse : un contour doit être détecté une seul fois.

La détection de contour d'après Canny se fait suivant les étapes suivantes :

Lissage : Cette étape se fait à l'aide d'un filtre Gaussien en 2D pour réduire le bruit de l'image initiale (et surtout quand elle est capturée à l'aide d'une caméra).

Calcul du gradient : Après le lissage de l'image et pour bien décrire les zones de changement brusque d'intensité dans une image en niveau de gris, on doit calculer l'amplitude et l'angle du gradient, ces dernier sont calculés comme suit :

$$|G| = \sqrt{G_x^2 + G_y^2} \text{ où pour simplifie } |G| = G_x + |G_y| \quad \text{(A.1)}$$

$$\theta = \arctan\left(\frac{|G_y|}{|G_x|}\right) \quad \text{(A.2)}$$

Tel que : G_x et G_y sont les gradients suivant la direction des X et Y respectivement.

Suppression des non maxima : Le calcul du module du gradient pour une image nous donne une intensité pour chaque pixel de cette image. Une forte intensité signifie une forte probabilité de présence d'un contour mais il ne suffit pas pour décider si c'est un point de contour ou pas, seuls les points correspondant à des maxima locaux sont considérés. Dans cette étape, on fait la suppression des points qui ne correspondent pas à des maxima locaux à l'aide de l'orientation du gradient.

Seuillage par hystérésis : La différenciation entre les points réels du contour et les points causés par le bruit se fait par un seuillage d'hystérésis, cela nécessite deux seuils (un seuil bas et un autre haut). Après comparaison entre l'intensité du gradient et le seuil, la décision s'effectue comme suit : si l'intensité du gradient est :

- Inférieure au seuil bas, le point est rejeté ;
- Supérieure au seuil haut, le point est accepté comme formant un contour ;
- Entre le seuil bas et le seuil haut, le point est accepté s'il est connecté à un point déjà accepté.

2. Filtre de Gabor

Les filtres de Gabor sont une classe particulière des filtres linéaires orientés. Ce sont des discriminateurs de texture et sont sensibles à différentes fréquences et échelles. Ces faits ont soulevé un intérêt considérable et ont motivé les chercheurs à exploiter largement les propriétés des fonctions de Gabor.

Le filtre de Gabor n'est qu'une fréquence pure modulée par une gaussienne, c'est-à-dire, un filtre passe bande avec une enveloppe gaussienne. Ce filtre est très répandu du fait de sa propriété de résolution optimale conjointe en fréquence et en temps. En plus, des études physiologiques sur les mammifères ont montré qu'on peut assimiler le fonctionnement de certains neurones du cortex visuel à ce type de filtre.

- Formule Complexe du filtre de Gabor :

$$g(x,y;\lambda,\theta,\psi,\sigma,\gamma) = \exp\left(-\frac{x'^2+\gamma^2y'^2}{2\sigma^2}\right)\exp\left(i\left(2\pi\frac{x'}{\lambda}+\psi\right)\right)$$

- Partie Réelle

$$g(x,y;\lambda,\theta,\psi,\sigma,\gamma) = \exp\left(-\frac{x'^2+\gamma^2y'^2}{2\sigma^2}\right)\cos\left(2\pi\frac{x'}{\lambda}+\psi\right) \quad \text{(A.3)}$$

- Partie Imaginaire

$$g(x,y;\lambda,\theta,\psi,\sigma,\gamma) = \exp\left(-\frac{x'^2+\gamma^2y'^2}{2\sigma^2}\right)\sin\left(2\pi\frac{x'}{\lambda}+\psi\right) \quad \text{(A.4)}$$

Ou

$$x' = x\cos\theta + y\sin\theta \quad y' = -x\sin\theta + y\cos\theta$$

Dans cette équation, λ représente la longueur d'onde du facteur sinusoïdal, θ représente l'orientation de la normale à des bandes parallèles d'une fonction de Gabor, ψ est le décalage de phase, σ est le sigma de l'enveloppe gaussienne et γ est le rapport d'aspect spatial, détermine le taux d'ellipticité du support de la fonction de Gabor.

Les filtres de Gabor sont directement liés aux ondelettes de Gabor, car ils peuvent être conçus pour un certain nombre de dilatations et rotations. Cependant, en général, l'expansion n'est pas appliquée pour ondelettes de Gabor, puisque ce calcul nécessite des ondelettes bi-orthogonales, qui peuvent être très chronophage. C'est pourquoi, en général, un ensemble composé de filtres de Gabor avec différentes échelles et rotations est créé. Les filtres sont convolués avec le signal, ce qui entraîne un espace que l'on appelle espace de Gabor.

L'espace de Gabor est très utile dans les applications de traitement d'image telles que la reconnaissance optique de caractères, reconnaissance de l'iris et la reconnaissance d'empreintes digitales. Il peut aussi servir dans la détection des contours.

Ils permettent de mettre en évidence des textures ainsi que des zones homogènes d'une image. Grâce à la forme gaussienne des filtres, les enveloppes des images filtrées apportent une information spectrale locale en chaque pixel. De plus, elles renseignent sur le contenu énergétique de l'image dans la direction du filtre choisi.