République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université de Larbi Tébessi –Tébessa
Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie
Département : Mathématiques et Informatique

MEMOIRE DE MASTER
Domaine : Mathématiques et Informatique
Filière : Informatique
Option : Systèmes et MultiMedia

Thème :

Combinaison de multiple classifieurs pour la reconnaissance biométriques des personnes

Présenté par :

SALHA Saoussen
KAKICHE Mayssa

Devant le jury :

T.NOUIOUA	M.A.A	Université de Tébessa	Président
C.DJEDDI	M.C.B	Université de Tébessa	Examinateur
L.LAIMECHE	M.A.A	Université de Tébessa	Rapporteur
A.MERAOUMIA	M.C.B	Université de Ouargla	Co-encadreur

Date de soutenance : 30/05/2016

Note : Mention :

Résumé

La biométrie se réfère à la reconnaissance automatique des individus basée sur leurs caractéristiques physiologiques et/ou comportementales. Les systèmes biométriques unimodaux permettent de reconnaître une personne en utilisant une seule modalité biométrique, mais ne peuvent pas garantir avec certitude une bonne identification. La plupart des problèmes des systèmes unimodaux peuvent être réduits par la mise en place de systèmes biométriques multimodaux utilisant plusieurs modalités ou signatures biométriques d'une même personne. Dans ce travail nous introduisons tout d'abord la notion de biométrie. Nous décrivons l'architecture d'un système biométrique ainsi que les métriques utilisées pour évaluer leur performance. Nous donnons un bref aperçu des technologies biométriques les plus courantes et des moyens de les fusionner pour obtenir des systèmes multimodaux. Nous présentons enfin nos résultats expérimentaux pour plusieurs systèmes biométriques multimodaux basés sur deux modalités biométriques liées à la main (l'empreinte palmaire et l'empreinte de l'articulation du doigt) et deux classifieur a savoir le classifieur à distance minimale (1-PPV) et la fonction à base radiale (RBF).

Mots clés : Sécurité, Biométries, Empreinte palmaire, empreinte des articulations des doigts, Multi-modalité, Fusion des données.

Abstract

Biometrics refers to automatic recognition of individuals based on their physiological and/or behavioral characteristics. Unimodal biometric systems allow person recognition based on a single source of biometric information but cannot guaranty a perfect identification. Most of the unimodal systems problems can be alleviated by using multimodal biometric systems that combine several biometric modalities or signatures of the same person. In this works, we first introduce the notion of biometrics. Then, we describe the architecture of biometric systems and the metrics used to evaluate their performances. We briefly discuss the most common biometrics and the different ways to combine them to obtain multimodal systems. Finally, we present our experimental results for several multimodal systems based on two biometrics related to hand (palmprint and finger-knuckle-print) and two classifier namely minimal distance classifier (1-NN) and Radial basis function classifier (RBF).

Index term: Security, Biometrics, palmprint, Finger-Knuckle-Print, Multimodality, Data fusion.

ملخص

البيموتري، يشير إلى التعرف على الأفراد بطريقة تلقائية بالاعتماد على خصائصه الفزيائية أو السلوكية. أنظمة التحقق من الهوية الأحادية تسمح بالتعرف على الأفراد باستعمال مصدر واحد فقط، ولكن لا يمكن أن تضمن على وجه اليقين التحديد السليم للأفراد. يمكن التقليل من معظم المشاكل المتعلقة بالأنظمة الأحادية باستعمال أنظمة التحقق من الهوية متعددة البصمات لنفس الشخص. في هذا العمل قمنا بتعريف مفهوم البيومتري ثم وصف بنية النظام البيومتري والمقاييس المستعملة لتقييم نتائجه القياسية. بعد ذلك قمنا بإعطاء لمحة حول مختلف التكنولوجيات البيومترية الشائعة والوسائل المستعملة لإدماجها وحللنا على أنظمة متعددة الأشكال. أخيرا قدمنا نتائج التجريبية الخاصة بنظام بيومتري يعتمد على صور لبصمة كف اليد وبصمة أصابع اليد.

الكلمات المفتاحية: الأمن البيومتري، بصمة راحة اليد، بصمة المفاصل، تعدد التمثيل، دمج المعطيات.

REMERCIMENTS

En préambule à ce mémoire nous remercions ALLAH de nous avoir permis d'arriver à ce niveau d'études et nous donne la patience et le courage durant ces langues années.

Nous souhaitant adresser nos remerciements les plus sincères à notre directeurs de mémoire Monsieur, Laimech Lakhdar, qui c'est montrés toujours à l'écoute et très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration, l'aide et le temps qu'ils ont bien voulu nous consacrer et sans qui ce mémoire n'aurait jamais vu le jour.

Nous adressons nos vifs remerciements à M. Abdallah MERAOUMIA, Docteur à l'université de Kasdi Merbah, Ouargla pour nous avoir diligentés tout au long de ce travail, pour son aide, sa compréhension, sa patience, sa compétence, et ses remarques qui nous ont été précieuses.

Nous tenons à remercier aussi sincèrement le corps professoral et administratif du département d'informatique, pour la richesse et la qualité de leur enseignement et qui déploient de grands efforts pour assurer à leurs étudiants une information actualisée et à toutes personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année universitaire.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous ont toujours soutenue et encouragée au cours de la réalisation de ce mémoire.

Merci à tous et à toutes.

Dédicace

Merci Allah (mon dieu) de m'avoir donné la capacité d'écrire et de réfléchir, la force d'y croire, la patience d'aller

jusqu'au bout du rêve.

Je dédie ce modeste travail à celle qui m'a donné la vie, le symbole de tendresse, qui s'est Sacrifié pour mon bonheur et ma réussite à ma mère.
A mon père, école de mon enfance, qui a été mon ombre durant
toutes les années d'études, et qui a veillé tout au long de ma vie
à m'encourager, à me donner l'aide et à me protéger.
Que dieu les garde et les protège.

A mes chers frères et sœurs, à mes amies
A tous ceux qui me sont chers.

KAKICH Mayssa

Dédicace

A mon très cher père
Je vous dois ce que je suis aujourd'hui grâce à votre patience et vos innombrables sacrifices.
Qu'A, le tout puissant, vous préserve et vous procure santé et longue vie afin que je puisse à mon tour vous combler.
A ma très chère mère
Je ferai de mon mieux pour rester un sujet de fierté à vos yeux avec l'espoir de ne jamais vous décevoir.
A mes très chères sœur et frères
Aucune dédicace ne serait exprimer assez profondément ce que je ressens envers vous, un grand merci, je vous aime.
A tous mes amis pour leurs soutiens et leurs encouragements.
A toute ma famille.

En témoignage de l'amitié sincère qui nous a liées et des bons moments passés ensemble. Je vous dédie ce travail en vous souhaitant un avenir plein de bonnes promesses.

SALHA Saoussene.

Page

1-PPV	:	1 plus proche voisin
ADN	:	Acide Désoxyribonucléique
CMC	:	Cumulative Match Curve
DCT	:	Discrete Cosine Transform
DET	:	Detection Error Trade-off
DFT	:	Discrete Fourier Transform
DWT	:	Discrete Wavelet Transform
EER	:	Equal Error Rate
FAR	:	False Acceptance Rate
FKP	:	Finger Knuckle Print
FRR	:	False Rejection Rate
GAR	:	Genuine Acceptance Rate
HMM	:	Hidden Markov Models
HOG	:	Histogramme de gradient orienté
LIF	:	Left Index Fingers
LP	:	Laplacian Pyramid
MVN	:	Multivariate Normal density
PCA	:	Principal Component Analysis
PLM	:	Palm print
PLV	:	PALM-Vein
RBF	:	Radial Basis Function
ROC	:	Receiver Operating Curve
ROI	:	Region Of Interest
ROR	:	Rank One Recognition
RPR	:	Rank of Perfect Recognition

Introduction Générale

L'identification fiable des individus est un service en pleine croissance. Il est très demandé dans beaucoup de domaine, pas seulement dans les environnements militaires ou de police, mais dans beaucoup d'applications civiles, à titre d'exemple, le contrôle d'accès aux systèmes de transactions financières (banques, trésorerie,…etc.). Les systèmes traditionnels de sécurité sont basés sur la possession d'un élément physique comme par exemple un badge, une carte à puce ou sur une connaissance comme un mot de passe, un code confidentiel ou d'un code PIN. Ces systèmes ont atteint leurs limites, par exemple les mots de passe peuvent être oubliés, pensés, divulgués ou cassés par force algorithmique brute. La solution de ces problèmes a été trouvée dans les technologies d'authentification basées sur la biométrie. La biométrie recouvre l'ensemble des procédés tendant à identifier un individu à partir de la mesure de l'une ou de plusieurs de ses caractéristiques physiques, comportementales ou biologiques. Ces caractéristiques doivent répondre à un certain nombre d'exigences : universelles, mesurable, unique, et permanentes, ce qui signifie qu'elles doivent être invariantes au cours du temps.

Plusieurs méthodes de reconnaissance biométriques ont été proposées, reconnaissance du locuteur, reconnaissance faciale, empreinte digitale, reconnaissance de l'iris et de la forme de la main. Malgré les avantages des méthodes biométriques par rapport aux systèmes traditionnels, ces méthodes souffrent de plusieurs limitations comme la non-universalité des biométries, la variabilité lors de la capture et la non-unicité des biométries. De plus les systèmes qui reposent sur une seule modalité biométrique sont vulnérables aux attaques et dépends,

généralement, de certains applications ce qui a donné la naissance à la fusion des modalités biométriques. Les résultats de plusieurs travaux ont montrés la performance des systèmes biométriques multimodaux par rapport aux systèmes unimodaux est une raison forte qui nous a conduit à travailler sur ce sujet.

Dans notre travail, nous avons proposés des systèmes biométriques basés sur deux modalités biométriques liées à la main (l'empreinte palmaire (PLM) et l'empreinte des articulations des doigts (LIF)) et deux classifieurs a savoir le classifieur à distance minimale (1-ppv) et la fonction à base radiale (RBF). Des systèmes unimodaux sont proposés dont les caractéristiques de chaque modalité sont extraites, séparément, via la méthode basée sur l'histogramme de gradient orienté (HOG), ensuite ces derniers sont utilisés dans les deux classifieurs. Quant aux systèmes multimodaux, dans une première série des tests, les deux modalités (PLM et LIF) sont fusionnées au niveau des images via l'utilisation de trois méthodes de fusion (DWT, PCA et LP). L'image résultante est utilisée comme une nouvelle modalité biométrique et le reste de système est similaire au système unimodal. Dans la deuxième série de tests, la fusion au niveau des scores est examinée. Dans cette série, plusieurs systèmes multimodaux, à savoir systèmes multi-biométriques, systèmes multi-algorithmiques et système hybrides sont évalués.

Le reste de ce mémoire est structuré comme suit :

- Le premier chapitre présente les notions de base de la biométrie, les différentes techniques biométriques et leurs applications. Ensuite, l'architecture d'un système biométrique unimodal est présentée ainsi les différentes phases de son fonctionnement.
- Le second chapitre décrit les limitations liées aux systèmes unimodaux, le principe de la multi-modalité et les différents niveaux des fusions ainsi que les différentes méthodes de fusion existantes.
- Le dernier chapitre présente l'algorithme HOG utilisé afin d'extraire un vecteur présentant efficacement les caractéristiques discriminantes des différentes modalités. Afin de concevoir un système robuste et efficace, dans une deuxième étape, plusieurs systèmes biométriques unimodaux et multimodaux sont testés. Des bases de données types sont utilisées pour évaluer les performances des systèmes proposés.

Enfin, une conclusion générale avec les perspectives visées que nous envisagerons sont données à la fin de ce mémoire.

Sécurité d'information et la biométrie

I.1 Introduction

De nos jours, la reconnaissance biométrique des individus est devenu une approche primordiale dans le domaine de la sécurité et de contrôle d'accès au sein des infrastructures et des systèmes informatiques telles que la protection de l'accès à un ordinateur, un téléphone portable, un établissement, des cartes bancaires... etc. De nombreuses technologies biométriques ont été développées, toutes basées sur les identificateurs biométriques (iris, voix, empreintes digitales, face, signature...). Dans ce chapitre nous allons présenter les notions de base de la biométrie, les différentes techniques biométriques et leurs applications. Ensuite, nous allons présenter l'architecture d'un système biométrique ainsi les différentes phases de son fonctionnement.

I.2. Nécessité de la biométrie

La sécurité des informations dans les différents domaines d'applications comme le secteur bancaire, la surveillance des frontières, le contrôle d'accès … etc., consiste à protéger la vie privée des individus, et éviter les tentatives de fraudes et de crimes. Pour assurer ces informations, elle exige une reconnaissance de l'identité de chaque personne. Dans la pratique en distingue deux modes d'identification ou de vérification : le premier basé sur la connaissance et le deuxième sur la possession [1] :

 Utiliser une connaissance : l'identification ou la vérification de l'identité d'un individu est basée généralement sur la connaissance d'un mot de passe, un code confidentiel ou d'un code PIN (Personal Identification Number). Elle est utilisée pour l'accès à des services en ligne, à

l'utilisation d'un ordinateur, à un immeuble, ou même à un réseau d'entreprise. Mais cette approche n'est pas sure parce que les mots de passe peuvent être oubliés, divulgués, pensés, ou cassés par force algorithmique brute.

 Utiliser un identifiant : Méthode basée sur la possession d'un élément physique [2]comme par exemple un badge, une carte à puce, un document écrit ou une clé. Malheureusement ces éléments aussi peuvent être volés, perdus ou falsifiés. Afin d'améliorer l'identification ou la vérification des individus, une autre technique de sécurité a été développé basée sur les caractéristiques physiques ou comportementales d'un individu [3], et qui sont unique et propre à chaque individu [4].

I.3. Définition de la biométrie

Le terme de biométrie est originaire d'une contraction des deux anciens termes grecs : « bios » qui signifie : la vie et « metron » qui se traduit par mesure [5].

Définition 1 : La biométrie recouvre l'ensemble des procédés tendant à identifier un individu à partir de la mesure de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques ou comportementales[1].

Définition 2 : À l'origine, le mot « biométrie » désigne l'application au domaine de la biologie des mesures utilisées en mathématiques. Il renvoie maintenant à un éventail de techniques, d'appareils et de systèmes permettant aux machines de reconnaître des personnes ou de confirmer ou d'authentifier leur identité[2].

La biométrie est une technologie d'identification et de vérification qui consiste à transformer une caractéristique biologique, morphologique ou comportementale en une empreinte numérique.

I.4. Intérêt biométrique

L'intérêt principal de la biométrie est de reconnaitre et d'identifier automatiquement les identités des individus en utilisant leurs caractéristiques physiologiques ou comportementales illustrées dans la figure I.1.

L'usage de la biométrie est motivé par plusieurs raisons comme [6]:

[1] Commission nationale de l'informatique et des libertés : http://www.cnil.fr/.

[2] Commissariat à la protection de la vie privée du Canada : https://www.priv.gc.ca.

1) La haute sécurité : en l'associant à des technologies comme le cryptage ou la carte à puce, pour éviter toutes tentatives de fraudes.

2) Le confort : la biométrie remplace les méthodes traditionnelle a risques tel que :

- L'oublie de mot de passe.
- La désactivation de l'écran de veille dans le but d'éviter la saisie fréquente du mot de passe.

Elle permet une identification sur et confortable de l'utilisateur.

3) Sécurité/psychologie : afin de mettre l'usager en confiance, il est indispensable pour les acteurs de commerce électronique d'encourager les transactions d'authentification biométrique pour changer le comportement des consommateurs. Vu qu'il est presque impossible de modifier, voler ou copier une caractéristique physiologique ou comportementale humaine.

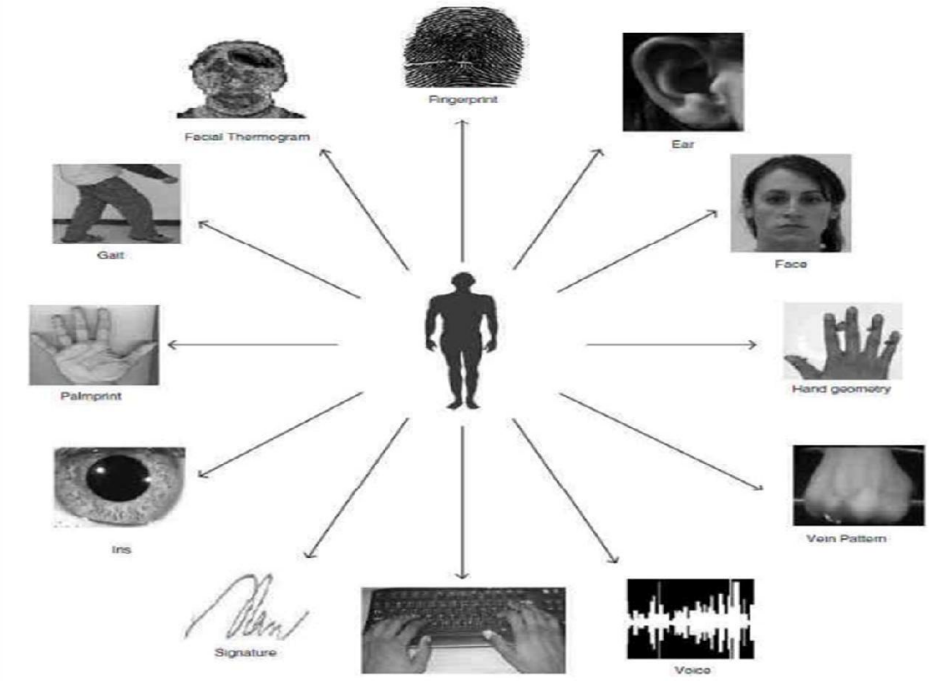


Fig. I.1: Exemple des traits biométriques utilisé pour l'identification .

I.5. Modalités biométriques

Il existe trois catégories de modalités biométriques :

- Biométries morphologiques (physiques) : sont les biométries utilisant une partie du corps humain comme l'empreinte palmaire, le visage, l'empreinte digitale, l'iris… .
- Biométries comportementales : sont celles qui utilisent un trait personnel du comportement comme la signature, la dynamique de frappe, la voix… .

- Biométries biologiques : elle regroupe des caractéristiques biométriques comme l'ADN, l'odeur, l'urine, la salive…etc.

La figure I.2 présente les différents traits biométriques classées dans trois catégories.

Fig. I.2: Exemple des traits biométriques classés en catégories.

Les trais physiologiques, comportementales et biologiques de l'être humain doivent répondre à un certain nombre d'exigences biométriques [7]afin de permettre le développement d'un système biométrique sure est fiable.

- L'universalité : tout le monde devrait l'avoir.
- L'unicité : les caractéristiques doivent être unique, en ne doit pas avoir deux personnes portant les même caractéristiques.
- La permanence / la robustesse : elle doit être invariante sur une période de temps.
- Le recouvrement : elle devrait mesurable et enregistrable.

I.6. Techniques biométriques

Différentes techniques biométriques existes dans la littérature et qui sont basées sur l'analyse des caractéristiques morphologiques, comportementales ou biologiques d'un individu afin d'extraire un vecteur de caractéristiques utilisé pour l'identification ou la vérification des individus. Ces techniques peuvent être regroupées dans trois grandes catégories selon le type de la biométrie utilisée.

I.6.1. Biométrie morphologique (physique)

1) Géométrie de la main : Les techniques biométriques basées sue la géométrie de la main consistes à déterminer les caractéristiques de la main : les dimensions des doigts, les caractéristiques des articulations la paume et la forme de la main [8].

Les systèmes de reconnaissance de la géométrie de la main sont simple à utiliser (voir figure I.3). Dans une première étape, une personne doit poser sa main sur une platine, les doigts doivent être correctement placés. Une caméra à infrarouge prend alors une image sous deux angles différents de sorte à obtenir une reproduction en trois dimensions de la main. Cette biométrie est toutefois sujette aux modifications de la forme de la main liées au vieillissement.

Fig. I.3 : Géométrie de la main.

Avantages :

- Très simple à utiliser.
- Espace de stockage faible.
- Le résultat est indépendant de l'humidité et de l'état de propreté des doigts.
- Bonne acceptation des usagés.
- Une fiabilité élevée et un temps de traitement rapide.

Inconvénients :

- Risque de faute pour des jumeaux ou des membres d'une même famille, technique peu discriminante.
- Sensible aux modifications ou altérations naturelles de la main (accident, vieillissement, arthrose), précision restreinte, difficile à utiliser pour les personnes souffrant d'arthrite.

Applications :

Contrôle d'accès à des locaux, parloirs de prison et accès à des bâtiments privés non stratégiques tels que les entreprises et toutes sortes d'établissements.

2) Empreinte digitale : D'autres techniques biométriques basées sur l'empreinte digitale sont proposées. L'empreinte digitale est la caractéristique d'un doigt, c'est-à-dire le dessin formée par les lignes de la peau des doigts (voir figure I.4). Chaque empreinte digitale est unique et chaque personne a ses propres empreintes digitales avec l'unicité permanente.

Le système de classification biométrique doit connaitre certains types de traits, Francis Galton [10] les classées en trois grandes catégories principales : boucle, delta et spires ou tourbillon. Quand a Edward Henry [9], il les subdivisées en sous-classes : boucle à gauche, boucle à droite, arche, arche penchée, spires et spires imbriquées ou boucles jumelles.

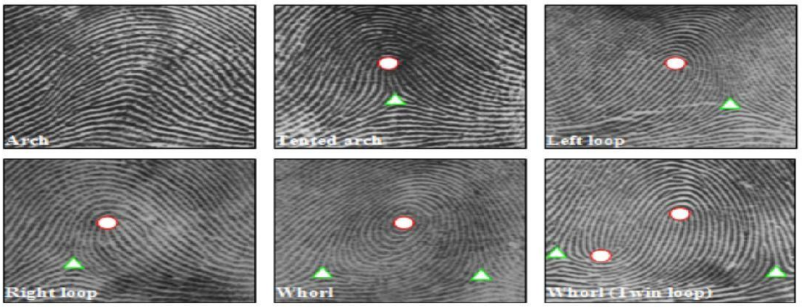


Fig. I.4: Principales classes d'empreintes digitales.

Avantages :

- Très discriminante.
- Petite taille du lecteur facilitant son intégration dans la majorité des applications (téléphones portables, PC).
- La technologie la plus éprouvée techniquement et la plus connue du grand public.
- Facile à mettre en œuvre.
- Technique pas chère, et peu vulnérable.
- Grande précision et peuvent être installée dans divers milieux.

Inconvénients :

- Exige un environnement propre.
- Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur).
- L'enregistrement se fait par contact, ce qui peut entraîner des réticences d'ordre psychologique ou hygiénique.

Applications :

- le contrôle d'accès physique (locaux, machines).
- le contrôle d'accès logique (systèmes d'information).

3) Empreinte palmaire : Est une empreinte biométrique situer sur la paume de la main, elle contient plus de caractéristiques discriminatives comme les lignes principales et les ridules. On distingue trois zones sur une empreinte palmaire (voir figure I.5) : la zone interdigitale, la zone thénar et la zone hypothénar[3].

[3]Police scientifique : http://www.police-scientifique.com/.

Fig. I.5 : Empreinte palmaire.

Avantages :

- Elles sont plus discriminantes, et peuvent être extraites à partir des images à basse résolution
- Elles sont beaucoup moins chères que celles de capture des iris.
- La combinaison des caractéristiques de la paume, telles que les caractéristiques des ridules ou des plis, et des lignes principales, nous permet d'établir un système biométrique robuste.

Inconvenients :

- exécution plus lente que celle d'empreinte digitale.

Applications:

- utilisée typiquement dans des applications légales criminelles.
- Plusieurs études montrent que l'identification d'empreinte palmaire est sans doute le prochain grand domaine d'investigation dans le cadre des lois sur la sécurité.

4) Empreinte des articulations des doigts : Chaque doigt possède trois articulations : La phalange proximale, la phalange médiane et la phalange distale. Les articulations des doigts possèdes des caractéristiques distinctives sur ça face extérieur tel que les lignes principales, les lignes secondaires et les crêtes appeler aussi empreinte d'articulation des doigts (voir figure I.6), qui y'en une grande capacité discriminative des individus [10].

Fig. I.6 : Empriente articulations des doigts.

Avantages :

- très simple à utiliser.

- La combinaison de tous les doigts de la main, nous permet une possibilité d'établir un système biométrique robuste et précise.
- Bonne acceptation.

Inconvénients :

- Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur).
- Risque de fausse acceptation pour des jumeaux.

Applications :

- Ce système reste expérimental.

5) Visage : C'est la première technique biométrique utilisée pour l'identification des personnes [11]. Le visage est certainement la caractéristique biométrique que les humains utilisent le plus naturellement pour s'identifier entre eux, ce qui peut expliquer pourquoi elle est en générale très bien acceptée par les utilisateurs.

Fig. I.7: Visage.

Dans un système de classification biométrique, une caméra est utilisée afin d'acquérir la forme du visage d'un individu, ensuite retirer certaines caractéristiques telles que : la forme, la couleur des yeux, la forme de la bouche, le tour du visage et la position des oreilles … etc. (voir figure I.7). Commeil existe beaucoup de changement dans la vie quotidienne des personnes (la barbe, les moustaches, le maquillage, l'expression d'une émotion, le vieillissement) cette technique est moins robuste [12].

Avantages :

- Très bien acceptée par le public.
- Simple et capable de fonctionner sans la collaboration de la personne (ne demande aucune action de l'utilisateur).
- Technique peu couteuse.
- Technique peut s'appuyer sur l'équipement d'acquisition des images actuel.

Inconvénients :

- Les vrais jumeaux ne sont pas différenciés.
- Cette technique est trop sensible au changement d'éclairage et aux fortes préoccupations relatives au respect de la vie privée.
- Les changements physiques peuvent tromper le système.

Applications :

- Technique appliquée dans les aéroports et certains grands magasins.
- Technologie pouvant être associée avec une autre technologie pour la compléter.

6) Rétine: La rétine est la paroi interne et opposée de l'œil sur laquelle se projettent les images que nous voyons. Cette paroi est tapissée par un réseau de vaisseaux sanguins (voir figure I.8), qui forment un motif unique pour chaque individu[4].

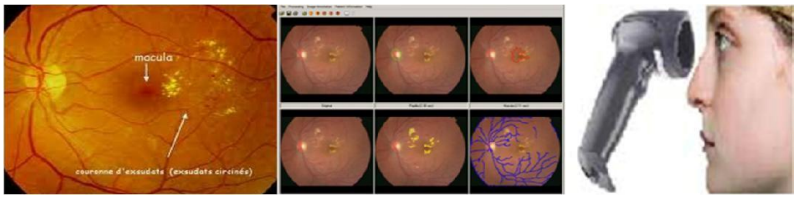


Fig. I.8 : Rétine.

Récemment la reconnaissance basée sur la rétine est considéré comme la méthode la plus sure dans le domaine de la biométrie. L'utilisateur doit placer son œil à quelques centimètres d'un orifice de capture situé sur le lecteur de rétine. Il ne doit pas bouger et doit fixer un point vert lumineux qui effectue des rotations. A ce moment, un faisceau lumineux traverse l'œil jusqu'aux vaisseaux sanguins capillaires de la rétine.

Avantages :

- Faible taux d'erreur (1 sur 10 millions).
- Grande fiabilité.
- Risques de fraude sont quasi nuls.

Inconvénients :

- Le danger du rayon lumineux envoyé dans l'œil.
- La mesure doit s'effectuer à très faible distance du capteur (quelques centimètres).
- Une forte alcoolémie ou un diabète modifie le réseau veineux rétinien.

Applications :

- Technique issue du milieu médical.

[4] L'internaute : http://www.linternaute.com/.

- depuis les années 70, elle a été utilisée par l'armée américaine.
- La CIA (Central Intelligence Agency) et le FBI (Federal Bureau of Investigation) ont adopté l'identification rétinienne, et aussi certaines prisons américaines.

7) Iris : L'iris est la zone colorée visible entre le blanc de l'œil et la pupille (voir figure I.9) [13]. C'est un réseau de tubes fins vus du dessus et dont le diamètre est inférieur à celui d'un cheveu. L'enchevêtrement des tubes est fixe et ne varie que très peu durant la vie de l'individu[5].

Fig. I.9 : Iris.

L'image de l'iris comporte de nombreuses caractéristiques physiques différentes. Ce sont les caractéristiques recherchées lorsqu'une personne utilise ce type de système biométrique. Cetteimage est lue par un appareil qui contient une caméra infrarouge, lorsque la personne se place à une courte distance de l'appareil. La reconnaissance de l'iris est une technologie plus récente puis qu'elle ne s'est véritablement développée que dans les années 80.

Avantages :

- Structures de l'iris restent stables durant toute la vie.
- La texture de l'iris est parfaitement stable au cours du temps.
- Les vrais jumeaux non confondus.
- Potentiel de très grande précision.

Inconvénients :

- Le matériel est plus couteux avec exigences sur l'éclairage.
- L'acquisition des images exige une certaine formation et de la pratique.
- La fiabilité diminue proportionnellement à la distance entre l'œil et la caméra.
- L'enregistrement assez contraignant car il impose de ne pas bouger pendant quelques secondes face à la caméra, ce qui rebute certains utilisateurs.
- L'acquisition des images crée un certain inconfort chez l'utilisateur, ce qui peut empêcher l'enrôlement de certaines personnes.

Applications:

- Contrôle d'accès physique et logique.

[5]Biométrie on ligne : http://www.biometrie-online.net/.

- Distributeurs de billets de banque.

I.6.2. Biométrie comportementale

Les modalités biométriques comportementales ce diffèrent selon l'analyse de certains comportements d'une personne à une autre, et à titre d'exemple on peut citer :

1) Signature manuscrite : Chaque personne à sa signature manuscrite unique [14], cette technique contient deux modes :

- Mode statique : qui utilise juste l'information géométrique de la signature.
- Mode dynamique : dans ce mode une tablette graphique est utilisée pour capturer la signature, ce mode dépend de la vitesse du stylo qui contient les informations dynamiques et géométriques.

Le point faible de cette technique est que, si un individu ne signe pas toujours de la même façon il va être sujette au refus automatique du système.

Fig. I.10: Signature manuscrite.

Avantages :

- La signature écrite peut être conservée des certains documents.
- Acceptation forte par l'utilisateur.

Inconvénients :

- La stabilité de cette technologie est qualifiée de moyenne à faible.
- Notre signature ayant tendance à évoluer au fil du temps.
- Les utilisateurs n'ont pas l'habitude de signer sur une tablette graphique (mode dynamique).
- Pas utilisable pour du contrôle d'accès.

Applications :

Les banques, les hôpitaux et les compagnies d'assurances utilisent cette technologie pour authentifier des documents électroniques.

2) Voix : La voix une autre technique pilote qui peut contenir des composantes physiologiques et comportementales (voir figure I.11). La reconnaissance vocale est utilisée

pour déterminer des caractéristiques uniques de la voix de chaque individu comme le débit, la force, la dynamique et la formes des ondes produites… etc. [15].

La voix nécessite l'application d'une méthode qui élimine certaines variations issue d'un changement bien entendu avec l'âge et peut être aussi affectée temporairement par l'état de la santé ou émotionnel du locuteur.

Fig. I.11: Voix.

Avantages :

- Cette biométrie est en général très bien acceptée car la voix est un signal nature à produire.
- Peut exploiter l'infrastructure téléphonique.
- Elle est facile de mise en œuvre.

Inconvénients :

- sensible à l'état physique et émotionnel de l'individu.
- Sensible au bruit.
- Possibilité de la modifier avec un échantillon vocal préenregistré.

Applications:

- Les corps policiers.
- Les agencies d'espionnage.
- Les services d'immigration.
- Les hôpitaux et en téléphonie.

3) Démarche : C'est la manière particulière de marche et c'est la complexité de la biométrie spatio-temporelle [16]. La reconnaissance de démarche consiste à identifier un individu à distance, une caméra capte les différentes articulations de mouvement de l'individu lors de sa marche et les envoie à un ordinateur qui les analyse comme illustré dans la figure I.12.

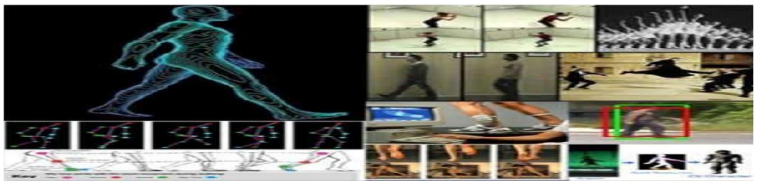


Fig. I.12: Démarche

Cette méthode dépend de la vitesse et l'accélération dont il a besoin pour reconnaitre chaque personne.

Avantages :

Elle peut être repérée à grande distance à l'aide d'une caméra à faible résolution et observée ainsi de n'importe quel angle.

Inconvénients:

Ne pas rester invariant en particulier sur une grande période de temps, en raison de grandes fluctuations de poids, changement majeur dans le poids du corps ou à cause d'ébriété. Il est sensible aux changements d'habits, chaussures et surface.

Applications :

Installations militaires.

4) Dynamique de frappe sur clavier : C'est une méthode qui utilise un logiciel de calcule de la vitesse de frappe qui dépend sur la situe de lettres [17], le temps de pression sur une touche, la pause entre chaque mot (figure I.13).

Fig. I.13 : Dynamique de frappe

Avantages :

- Acceptation forte par l'utilisateur.
- Elle conserve bien les défauts de l'authentification par mot de passe.
- Renforce la sécurité, mais n'est pas plus pratique.
- C'est un geste naturel pour un individu qui exploite le matériel existant.

Inconvénients :

- Elle dépend de l'état physique de personne (Age, émotion, fatigue).

Applications :

- Les banques.
- Les assurances.
- Les documents administratifs.

I.6.3. Biométrie biologique

C'est une catégorie biométrique importante dans le domaine de la sécurité criminaliste, elle contient des caractéristiques spécifiques à chaque individu et à titre d'exemple on peut citer :

1) ADN: Signifie acidedésoxyribonucléique qui constitue la molécule support de l'information génétique héréditaire[6] (figure I.14). C'est la méthode biologique la plus sure du monde, mais ses analyses nécessitent des délais de plusieurs semaines, ce qui interdit toutes les applications d'identification en temps réel.

Fig. I.14: ADN.

Avantages :

- Elle facilite largement la désignation du coupable.
- Différencier des personnes avec une grande fiabilité, c'est une technique très distinctive.

Inconvénients :

- Cout élevé.
- Analyse trop lente pour donner les résultats et en particulier en temps réel.

Applications :

- Domaine de lasécurité.

2) Veines de la main : Le réseau veineux palmaire est propre à chaque individu, même dans le cas de vrais jumeaux. Cette technique utilise un «scanner du réseau veineux palmaire»: il s'agit d'un capteur optique capable de "photographier" les veines de la paume à l'aide de «rayons proches de l'infrarouge», les veines palmaires absorbe ces rayons, réduisant ainsi le coefficient de réflexion, ce qui donne aux veines l'aspect d'un réseau de couleur noire», figure I.15. Les veines, ainsi dessinées, servent de repère pour les analyses. Pour être identifié, il faut placer la paume de la main au-dessus du lecteur. Le réseau veineux repéré est alors comparé avec les réseaux enregistrés afin d'authentifier la personne[7].

Fig. I.15: Veines de la main.

[6]Futura santé par futura science : http://www.futura-sciences.com/.
[7]ZDnet : http://www.zdnet.fr/

Avantages :

- Réseau interne difficile pour un imposteur de le copier.
- Technique très fiable.

Inconvénients :

- Très couteuse à mettre en œuvre.

Applications :

- Les cartes bancaires des clients.

I.7. Système biométrique

C'est un système de reconnaissance de formes [18, 19]qui acquiert des données biométriques d'identification d'un individu, puis extrait un vecteur de caractéristiques physiologique ou comportementale à partir de ces données, ce vecteur est généralement stocké dans une base de données (ou enregistrer sur une carte à puce donnée à l'individu après avoir été extrait) pour pouvoir exécuter une action ou prendre une décision à partir du résultat de comparaison.

I.7.1. Fonctionnement d'un système biométrique

Chaque système biométrique comporte deux phases principales comme illustré dans la figure I.16 : la phase d'enrôlement et la phase de reconnaissance.

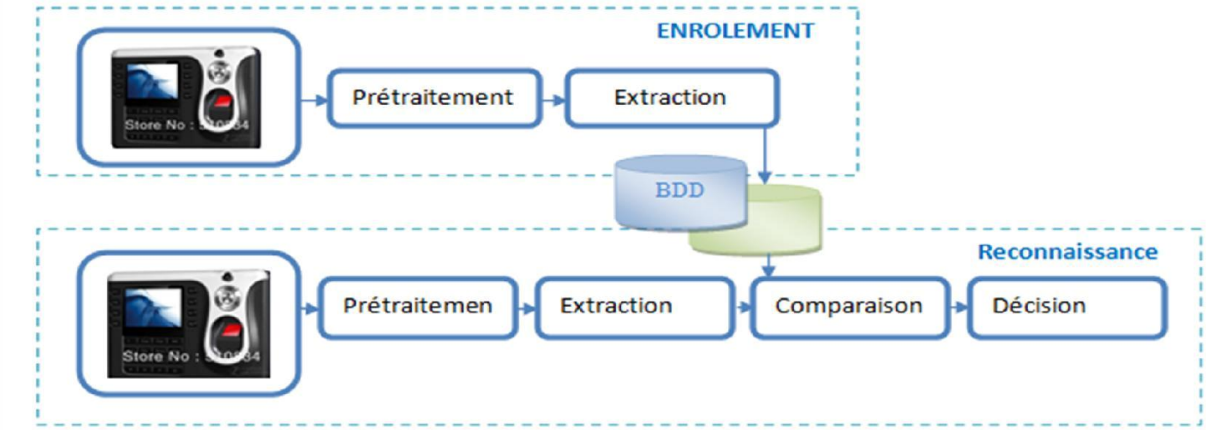


Fig. I.16 : Système de reconnaissance biométrique

1) Phase d'enrôlement : C'est la phase d'enregistrement des signatures biométriques (gabarit biométrique) de chaque individu dans la base de données, Ce gabarit de référence servira comme point de comparaison lors de la reconnaissance. Cet enregistrement peut s'accompagner de l'ajout d'information biographique dans la base de données comme le nom, le prénom, l'adresse… etc., ces données serviront plus tard dans la phase d'identification.

2) Phase de reconnaissance : C'est la phase de vérification ou d'identification d'identité de la personne qui veut accéder au système, elle est primordiale dans le fonctionnement de la biométrie, Au cours de cette phase le système effectue une saisie de la donnée biométrique puis un ensemble de paramètres sera extrait comme dans la phase de l'enrôlement. Le capteur utilisé dans la phase de reconnaissance doit être aussi proche de celui utilisé dans la phase d'enrôlement. Selon le fonctionnement du système, il existe deux modes de reconnaissance [20]:

 Mode de vérification : nommée aussi mode d'authentification, le système agit par vérification que l'identité de la personne est bien celle proposée par l'utilisateur, et ceci par comparaison entre le gabarit d'enrôlement et celui proposé par l'utilisateur. Il s'agit donc d'une comparaison avec un seul des modèles présent dans la base de données (comparaison un à un).

 Mode d'identification : son but est de deviner l'identité de la personne, il agit par comparaison entre le signal mesuré et les différents modèles de la base de données lors de la phase d'enrôlement (1 : N), si l'utilisateur a un modèle dans la base de données il va être accepté, dans le cas contraire il va être rejeté. L'identification peut décomposer en deux modes opératoires :

- Identification en mode ensemble fermé : L'identité de la personne (modèle possédant le degré de similitude le plus élevé avec l'échantillon présenté en entrée) constitue la sortie du système biométrique.
- Identification en mode ensemble ouvert : Dans le cas où l'utilisateur n'est pas accepté (rejeté) cela implique qu'il n'est pas enrôlé dans le système biométrique, et que la plus grande similarité entre l'échantillon et tous les modèles inférieur ou supérieur n'est pas conforme au seuil de sécurité fixé.

I.7.2. Modules principaux d'un système biométrique:

Un système biométrique est essentiellement un système de reconnaissance des formes. L'objectif de ces types des systèmes est de classifier des entités (modalités) en catégories (personnes) à partir d'observations (vecteur des caractéristiques) effectuées sur celles-ci. Ce dernier comporte quatre modules [21] :

1) Acquisition des données : L'acquisition des données biométriques d'une personne s'effectue par une interface utilisateurs telle qu'un appareil photo, caméra, microphone… etc.

2) Extraction des caractéristiques : Pour éviter les informations inutiles qui existent dans une image originale de là quelle on va extraire des caractéristiques biométriques, généralement on applique un processus de prétraitement dans une première étape. Ensuite, on prend l'image prétraitée et extrait les caractéristiques pertinente afin de former un gabarit biométriques unique et discriminatif.

3) Comparaison : Dans le but de déterminer le degré de similitude, en applique une comparaison entre l'ensemble des caractéristiques biométriques extraites et les modèles enregistrés dans la base de données du système.

4) Décision : Cette étape est basée sur un seuil de décision afin de pouvoir accepter ou rejeter une donnée biométrique tout dépend du passage du score de correspondance au-dessus ou au-dessous de ce seuil.

Seuil de rejet : score en dessous duquel un algorithme biométrique rejettera une authentification/identification.

Seuil d'acceptation : score au-dessus duquel un algorithme biométrique acceptera une authentification/identification.

En générale c'est l'étape où le système vérifier l'identité de l'utilisateur et décide s'il peut accéder au système ou non.

I.7.3. Système en ligne et système hors ligne

En distingue deux types de systèmes de reconnaissance biométrique [22]: système de reconnaissance en ligne et système de reconnaissance hors ligne.

1) Système en ligne : C'est un système qui acquit et traite les images numériques en temps réel, comme le déverrouillage de téléphone portable par empreinte digitale.

2) Système hors ligne : Un système biométrique hors ligne traite les images (modalités biométriques) capturées précédemment. Par exemple, des images obtenues à partir des doigts des mains encrées digitalisées par un scanner numérique. Ces approches peuvent fournir des images à haute résolution et conviennent aux méthodes qui exigent des images de résolution fine pour extraire des lignes, des points caractéristiques et des minuties. Cependant, ces méthodes ne sont pas appropriées aux systèmes de sécurité en ligne car deux étapes sont nécessaires : encrer les doigts pour obtenir les images de modalité sur des papiers et puis les scanner pour obtenir des images numériques.

I.8. Domaines d'application de la biométrie

La biométrie aujourd'hui est la méthode la plus utilisé dans les systèmes de vérification et d'identification des individus. De nos jours les principales applications de la biométrie sont : les systèmes d'informations, les stations de travail, le contrôle des frontières, le paiement électronique, l'accès aux réseaux, et le chiffrement des données. On distingue quatre groupes principaux d'application de la biométrie [23].

I.8.1 Service public

La biométrie est généralement utilisée dans tous les services publics d'ordre gouvernemental tel que le contrôle des frontières et la sécurité des aéroports par l'intermédiaire d'iris, de visage et d'empreinte digitale. Et de même dans le domaine de la santé pour mieux gérer l'utilisation des cartes d'assurance sociale en identifiant leur propriétaire.

I.8.2 Identification judiciaire

Dans ce domaine ont distingué deux techniques biométriques : l'empreinte digitale, qui par sa détection prouve la présence des criminels sur les lieux du crime et les objets qu'il a touché et ceci ne peut être réalisé que par la création d'une base de données internationale. L'ADN qui est une technique basée sur l'analyse de sang, des cheveux ou des cellules buccales déposé par la salive, par les qu'elles on peut identifier le suspect.

I.8.3 Transactions bancaires

En utilisant des cartes à puce qui incorporeraient la reconnaissance des empreintes digitale on estime limiter l'utilisation frauduleuse de carte de crédit ou le retrait d'argent au guichet des banques, les paiements par cartes bancaires, les transferts de fonds, les paiements effectuée à distance par téléphone ou sur internet.

I.8.4 Accès physique et logique

On fait allusion à un contrôle d'accès physique lorsqu'on cherche à sécuriser l'accès à un lieu par exemple entré à un bâtiment ou une salle, alors que le contrôle d'accès logique concerne l'accès informatique à un terminal, réseau informatique ou de télécommunications comme l'ordinateur, le téléphone portable, la base de données privée.

I.9. Conclusion

La biométrie est devenue le moyen de sécurité le plus utilisé grâce à la variabilité des modalités biométriques et ses avantages multiples. Dans ce chapitre, nous avons présenté les différentes modalités biométriques et les différentes caractéristiques qu'on peut l'extraire, ainsi la structure générale d'un système biométriques et le fonctionnement de chaque phase. Finalement, nous avons présenté les différentes applications de la biométrie.

La multi-modalité et la fusion des données

II.1 Introduction

Dans les systèmes biométriques uni-modaux (c'est-à-dire une seule modalité), les taux d'erreurs associés à ces systèmes restent relativement élevés. Ce qui les rend inacceptables pour des applications critiques de sécurité [24]. Ce problème peut être résolu par la mise en place d'un système biométrique multimodal utilisant plusieurs modalités biométriques d'une même personne.

Dans ce chapitre, nous allons présenter les différents types de fusion appliquée à la biométrie afin d'améliorer les performances de la reconnaissance. Ensuite, nous allons détailler les différents niveaux de fusion ainsi la notion de normalisation des scores.

II.2 Limitation des systèmes uni-modaux

Malgré les avantages des systèmes biométriques uni-modaux par rapport aux systèmes traditionnels, ils possèdent des inconvénients qui les rendent moins robuste et moins performant. Les systèmes biométriques uni-modaux souffrent de plusieurs limitations, ils sont affectés par les problèmes suivants :

II.2.1 La non-universalité des biométries

Le choix de la modalité biométrique dans un système de reconnaissance biométrique uni - modale dépend du critère de l'universalité, c'est que signifié que tout le monde devrait avoir cette modalité. En revanche, la non-universalité veut dire que certaines personnes ne possèdent pas certaines modalités, ou il existe un manque d'informations d'une modalité précise par le système de reconnaissance de l'identité, comme par exemple : les personnes qui ne peuvent pas

réaliser une identification par signature à cause d'un handicape physique, une personne muette ne peut pas utiliser la reconnaissance par la voix, aussi des personnes ayant des maladies oculaires (glaucomes ou cataractes) ne peuvent pas fournir une identification d'iris ou de rétine. De la même manière, des gens accidenté (par exemple : ils ont des brûlures), ils ne peuvent pas réaliser une identification d'empreinte digitale, palmaire ou d'articulation des doigts. Pour ces raisons, toutes ces personnes risquent d'être refusées par certains systèmes biométriques, c'est que signifié qu'ils peuvent être exclus de certaines utilisations si aucune alternative ne leur proposé.

II.2.2 La variabilité lors de la capture

La variabilité lors de la capture ou bien l'acquisition est le résultat de plusieurs facteurs différents, tel que :

- Le changement inhérent de la modalité biométrique.
- L'utilisation de différents capteurs lors de l'enrôlement et de la vérification, à des changements de conditions d'environnement ambiant (changement d'éclairage).
- La déformation physique lors de la capture (variabilité du capteur).
- Le bruit d'acquisition, par exemple : l'accumulation de poussière sur un capteur d'empreintes digitales.
- La mauvaise interaction de l'utilisateur avec le capteur.

II.2.3 La sensibilité aux attaques

La sensibilité aux attaques touche beaucoup plus les modalités biométriques comportementales, car ils sont très sensibles à ce genre d'attaques comme par exemple : imiter une voix ou reproduire une signature. Par contre il est très difficile de reproduire une modalité biométrique physiologique comme les empreintes palmaires, empreintes digitales iris… etc. Mais malheureusement certaines études ont prouvé qu'il était possible de fabriquer des fausses empreintes digitales en gomme et de les utiliser pour la contrefaçon.

II.2.4 La non-unicité des biométries

La non-unicité des biométries signifie que les caractéristiques extraites à partir des modalités biométriques de différentes personnes peuvent être relativement similaires, comme par exemple : la variabilité de la géométrie de la main à travers le temps (le vieillissement,

l'arthrose, grossir ou bien devenir svelte… etc.) rend certaines géométries des mains des individus différents identique (exemple : vrais jumeaux).

Donc le taux d'erreur d'un système de reconnaissance biométrique augmente dans ce cas, et risque d'accepter des personnes non enregistrées dans la base de données (imposteur).

II.3 Systèmes biométriques multimodaux

Le système biométrique multimodal consiste à combiner plusieurs modalités biométriques différentes ainsi que la consolidation d'informations présentées par les différentes modalités peut permettre une authentification précise de l'identité e améliorer les performances de reconnaissance [25] afin de diminuer les tentatives de fraudes.

Lors de l'augmentation de la quantité d'informations discriminantes de chaque personne, on souhaite augmenter le pouvoir de reconnaissance du système (vérification ou identification), et diminuer le taux d'erreur.

II.3.1 Fusion des données

La fusion des données est une méthode qui consiste a combiné plusieurs données issues de plusieurs sources différentes afin d'avoir la meilleur décision.

Dans les systèmes biométriques multimodaux, il existe deux architectures de fusion différentes qui sont : l'architecture en série et l'architecture en parallèle.

1. Architecture de fusion en série

L'architecture de fusion en série consiste à obtenir un score de similarité issue de chaque acquisition comme illustré dans la figure II.1.

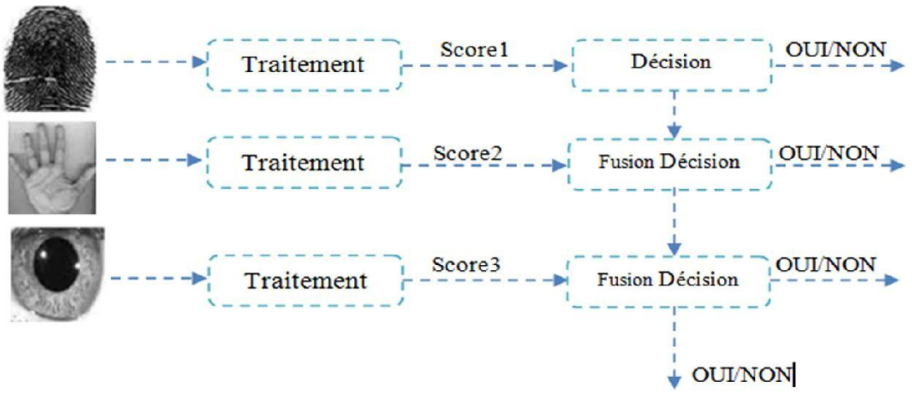


Fig. II.1 : Architecture de fusion en série.

L'architecture en série peut être privilégiée dans certaines applications, par exemple le cas d'un individu atteint de cataracte, il est incapable de réaliser une identification d'iris, l'architecture de multi-modalité représente pour lui une solution alternative de secours comme l'empreinte digitale ou palmaire.

2. Architecture de fusion en parallèle

Elle procède un ensemble des acquisitions avant de prendre une décision [26]. L'architecture en parallèle, figure II.2, nous permet d'utiliser toutes les informations disponibles qui nous aide à améliorer les performances du système, mais, lors de l'acquisition et le traitement d'un grand nombre de données biométrique le temps et le matériel devient couteux, et réduit le confort d'utilisation.

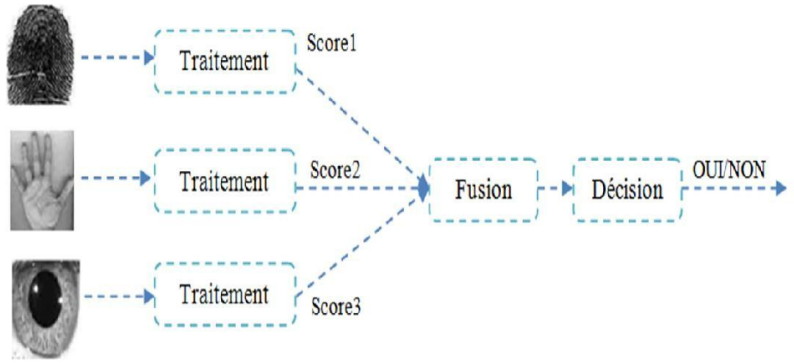


Figure II.2 : Architecture de fusion en parallèle.

II.3.2 Sources des fusions

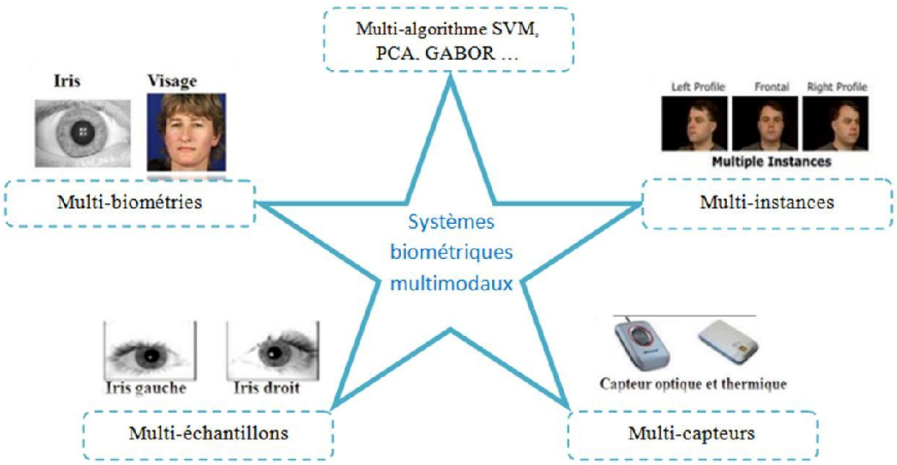


Fig. II.3 : Les différents systèmes multimodaux.

Il existe plusieurs méthodes pour effectuer une fusion biométrique (systèmes biométriques multimodaux) indiqué dans la figure III.3.

II.3.3 Systèmes Multi-biométriques

Ce système dépend de la combinaison des différents traits biométriques d'un individu, par exemple : la fusion de l'empreinte palmaire et l'articulation des doigts. Cette approche devient plus précise en reconnaissance et plus forte en sécurité si en utilise un nombre croissant de traits biométriques. Elle nécessite différents capteurs et algorithmes dédiés à chaque caractère biométrique.

1. Systèmes Multi-capteurs

Le fonctionnement de ce système est d'obtenir la même modalité à partir de plusieurs capteurs afin d'extraire diverses informations provenant de l'enregistrement des images, par exemple l'acquisition de l'empreinte digitale par deux capteurs différents le premier optique et l'autre capacitif.
L'utilisation de plusieurs capteurs permet d'acquérir des informations complémentaires pour accroitre les performances des systèmes uni-modaux, et la fusion dans ce type de système ce termine au niveau capteur.

2. Systèmes Multi-instances

Ce système dépend de la capture de plusieurs instances du même trait biométrique, par exemple la capture de plusieurs images du visage avec des changements de pose (profil frontal, profils gauche et droit), Ces systèmes n'entraînent pas généralement de surcoût de capteurs, ni le développement de nouveaux algorithmes d'extraction de caractéristiques. À ne pas confondre avec les systèmes multi échantillons.

3. Systèmes Multi-échantillons :

Dans ce système on peut utiliser un seul capteur pour capturer plusieurs échantillons du même trait biométrique afin de prendre en compte les variations qui peuvent se produire au sein de ce trait, ou bien pour avoir la représentation plus complète du caractère sous-jacent. Par exemple capturer l'iris gauche et l'iris droit d'un individu pour vérifier son identité.

4. Systèmes Multi-algorithmes

Ce système dépend du traitement de la même donnée biométrique par plusieurs algorithmes, on peut appliquer cette approche lors de la phase d'extraction de caractéristiques et/ou de comparaison. Par exemple l'application des algorithmes d'analyse de minuties et de texture pour traiter la même image d'empreinte digitale dans le but d'extraire diverses caractéristiques qui peuvent améliorer la performance du système [27].

II.4 Niveaux de fusion

L'application de la fusion des informations dans un système biométrique multimodale peut être faite dans n'importe quel module du système. La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents [28] : au niveau des données, au niveau des caractéristiques extraites, au niveau des scores issus du module de comparaison ou au niveau des décisions du module de décision. Ces niveaux appartiennent à deux grands sous- ensembles :

- La fusion pré-classification (avant comparaison).
- La fusion post-classification (après la comparaison).

II.4.1 Fusion pré-classification

C'est la fusion des informations issues au niveau du capteur (image brute) ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques.

1. Niveau du capteur : Dans ce niveau, on obtient des données brutes (raw data) à partir des différents capteurs dans le module d'acquisition, puis les combiner ensemble à condition qu'ils soient homogènes. Cette combinaison donne comme résultat un seul signal qui va être utilisé comme entrée d'un système de reconnaissance biométrique [29]. Afin de réaliser cette approche, différentes méthodes de fusion existes dont les principaux sont :

a. Méthode basé sur ACP (Analyse des Composantes Principales) : C'est la méthode de fusion la plus connu au monde de l'imagerie [30], le principe de cette approche est de transformer un ensemble de variables corrélées en un nouvel ensemble de variable non corrélées issue de la combinaison linéaire des variables originales. Elle nous permet une possibilité de retour dans l'espace des variables originales au départ des composantes principales sélectionnées.

Dans cette méthode les pondérations des images d'entrées sont calculées en considérant leurs variances statistiques, qui reflètent les richesses en information de ces images.

Soit X l'ensemble d'images disponibles, formé de n images I_i de taille H*W pixels. La matrice I_i est d'abord convertie en un vecteur colonne v_i de taille d*1 avec d = H.W. En ajoutant chaque colonne, l'une après l'autre pour toutes les images, une matrice des données d'apprentissage $X = [v_1, v_2,\ldots,v_n]$ est alors formée. La taille de X est de d*n, avec n est le nombre total des images d'apprentissage. Après l'obtention de X, on calcule la matrice de l'image moyenne avec l'équation suivante :

$$\Psi = \frac{1}{n}\sum_{i=1}^{n} v_i \qquad \text{(II.1)}$$

Et c'est ensuite qu'on applique un ajustement des données par rapport à la moyenne. L'image moyenne est alors soustraite de chaque image avec la formule suivante :

$$\Phi_i = v_i - \Psi, \quad i = 1 \cdots n \qquad \text{(II. 2)}$$

Enfin, effectuer un calcul de la matrice de covariance avec la formule suivante :

$$C = \sum_{i=1}^{n} \Phi_i \Phi_i^T = AA^T, \quad A = [\Phi_1, \Phi_2, \cdots, \Phi_n] \qquad \text{(II.3)}$$

La prochaine étape consiste à calculer les vecteurs et les valeurs propres de cette matrice. Les poids sont ensuite obtenus par les composantes normalisées du vecteur propre (v_1) qui correspond à la valeur propre la plus élevée :

$$\beta_i = \frac{\nu_{1_i}}{\sum_{i=1}^{n} \nu_{1_i}} \qquad \text{(II.4)}$$

b. Fusion des images par la DWT (Discret Wavelet Transform) : C'est la première transformée utilisé dans le domaine de la fusion des images [31]. Dans le cas de la décomposition multi-résolution, à chaque niveau une image est décomposée dans une version simplifiée (approximation) et une version de détails (présentation des détails de l'image). La fusion dans le plan des ondelettes consiste premièrement à décomposer en ondelettes deux images I_1 et I_2.

Chaque image sera alors représentée par son dernier plan d'approximation et un ensemble de plans de coefficients d'ondelettes correspondants aux détails de l'image

aux différentes échelles. La construction de l'image fusionnée revient, d'une part, à produire un plan de la dernière approximation et, d'autre part, à synthétiser ses coefficients d'ondelettes par l'utilisation d'un modèle de fusion. L'image fusionnée I_F est alors produite par l'application de la transformation en ondelettes inverse (Inverse DWT-IDWT).

Pour synthétiser les coefficients de chaque bande (approximation et détails) de l'image fusionnée à l'échelle i, il faut définir deux modèles de fusion permettant de combiner les coefficients d'ondelettes des images I_1 et I_2, l'un pour l'approximation et l'autre pour les trois détails. Toute en sachant que les deux modèles de fusion sont les mêmes pour chaque niveau de décomposition.

Pour un seul niveau de décomposition, les images I_1 et I_2peuvent être représentées par les ensembles respectifs des plans de décomposition (E_1 et E_2), comme par exemple :

$$E_1 = \{I_{1_{LL}}, I_{1_{LH}}, I_{1_{HL}}, I_{1_{HH}}\}; \qquad E_2 = \{I_{2_{LL}}, I_{2_{LH}}, I_{2_{HL}}, I_{2_{HH}}\} \tag{II.5}$$

Où I_{iLH}, I_{iHL} et I_{iHH} sont les coefficients d'ondelettes correspondants aux détails produits des images (i=1, 2), et I_{iLL} sont les derniers plans d'approximation respectifs. La préservation des caractéristiques des deux images est assurée par la moyenne des deux approximations des images d'entrées :

$$I_{F_{LL}}(x,y) = \frac{1}{2}\left[I_{1_{LL}}(x,y) + I_{2_{LL}}(x,y)\right] \tag{II.6}$$

I_{FLL} représente l'approximation de l'image fusionnée. Pour les trois bandes de détail, chaque bande est divisée en une fenêtre de taille 3*3. Ensuite, calculée la somme des valeurs absolues des tous les pixels dans chaque fenêtre. Enfin, générées des cartes de décision binaire (binary Decision Maps-DM), pour les trois bandes des détails, en utilisant cette équation :

$$DM_X = \begin{cases} 1 & \text{si } \max_{3\times3}(I_{1_X}) \geq \max_{3\times3}(I_{2_X}), \\ 0 & \text{Autrement} \end{cases} \tag{II.7}$$

Les $X \equiv \{LH, HL, HH\}$ sont les cartes de décision binaire générées pour les trois bandes des détails. Basée sur ces cartes, les trois bandes des détails de l'image fusionnée, I_{FX}, sont générées. Finalement, la transformée inverse, IDWT, est ensuite appliquée sur les quatre bandes fusionnées afin de générer l'image fusionnée.

$$I_F = \text{IDWT}(I_{F_{LL}}, I_{F_{LH}}, I_{F_{HL}}, I_{F_{HH}}) \quad \text{(II.8)}$$

Donc, on distingue trois opérations pour réaliser cette fusion :

- La décomposition ou l'analyse de chaque image de départ qui produit une image d'approximation et plusieurs images de détails ;
- Appliquer un critère de fusion à chaque niveau de décomposition ;
- Appliquer l'opération inverse de la décomposition (synthèse), pour créer l'image fusionnée.

c. Fusion des images par l'algorithme pyramidal : Cette méthode nous donne une représentation sous forme d'images de plus en plus petites, et de moins en moins de pixels, qui dessinent une sorte de pyramide.

L'image de la plus haute résolution est appelée la base de la pyramide, tandis que l'image de la plus petite résolution est appelée le sommet, qui peut être de taille 1*1 pixel.

Le principe des algorithmes pyramidaux est de décomposer une image en images de différentes résolutions puis de la recomposer [32]. Effectuant un algorithme pyramidal qui se définit comme la décomposition d'une image sous forme d'arbre, de sorte que l'étage supérieur puisse être restitué à partir de l'étage inférieur.

Dans le cas de la décomposition pyramidale, à chaque niveau des règles de combinaison entre les versions simplifiées des images d'entrée doivent être utilisées pour engendrer la représentation de l'image de sortie à cette étape (I_l). Ensuite, l'image fusionnée créera à partir de l'application d'une opération de synthèse sur l'ensemble des représentations pyramidales.

Les schémas de combinaison utilisent principalement deux sortes d'opérations : la sélection entre les représentations pyramidales et la composition de l'image moyenne de ces représentations sélectionnées. En effet, lors de la dernière étape de décomposition (N), où se trouvent des représentations étendues des images d'entrée (I_i), l'image moyenne de ces représentations est générée comme suit :

$$I_{F_N}(i,j) = \frac{1}{2}\left[I_{1_N}(i,j) + I_{2_N}(i,j)\right] \quad \text{(II.9)}$$

Pour les premières étapes N-1 qui présentent des images de détails, l'algorithme de sélection, appelé « choose max », est employé. Cet algorithme est présenté sous la forme:

$$I_{F_l}(i,j) = \begin{cases} I_{1_l}(i,j), & \text{si} \quad |I_{1_l}(i,j)| > |I_{2_l}(i,j)| \\ I_{2_l}(i,j) & \text{Autrement} \end{cases} \qquad \text{(II.10)}$$

I_{1l}, I_{2l} sont les images d'entrées au niveau l, et I_{Fl} est l'image fusionnée au niveau l. Un autre aspect important est le choix du nombre des niveaux de décomposition. Il est à noter qu'il n'y a pas de technique d'évaluation pour déterminer le nombre des niveaux minimal pour obtenir une fusion de bonne qualité.

2. Niveau caractéristiques : C'est l'obtention de différents vecteurs de caractéristiques à partir des différentes phases de traitements et d'analyses, puis les combiner avec une nécessité d'homogénéité des données, lorsque ce critère est réalisé on passe à la méthode de fusion au niveau des caractéristiques, cette dernière nous donne comme résultat après la combinaison un seul vecteur de caractéristique, en sachant que ces vecteurs sont issue de différentes sources suivantes : plusieurs instances du même trait biométrique, plusieurs unités du même trait biométrique, plusieurs capteurs du même trait biométrique ou encore plusieurs traits biométriques [33].

II.4.2 Fusion post-classification

C'est la fusion au niveau des scores issus des modules de comparaison, ou au niveau des décisions.

1. Niveau des scores : Les scores sont issus du module de comparaison qui nous donne comme résultat des scores individuels, ces derniers vont être combiné par une méthode de fusion afin d'obtenir un seul score utilisé pour prendre la décision finale.

   Cette approche est la plus utilisée car elle peut être appliquée à tous types de système par des méthodes simples et efficaces.

   Supposons que nous avons n scores disponibles, d_i, pour i = 1 à n, issus des n systèmes. Le score résultant D_f est alors donné par [34] :

   a. Somme des scores (sum_score : SUM)

      la combinaison des scores par la somme qui consiste à calculer D_f tel que :

$$\mathcal{D}_f = \sum_{i=1}^{n} d_i \qquad \text{(II.11)}$$

b. Somme pondérée des scores (Sum_weighting_score : WHT)

C'est une extension de la somme des scores, le score de chaque système est pondéré en se basant sur le taux d'erreur qui lui est associé, la fusion des scores est calculée comme suit :

$$\mathcal{D}_f = \sum_{i=1}^{n} w_i d_i \quad \text{(II.12)}$$

En notant l'erreur d'un système i comme ε_i, i= 1,2,…n avec n est le nombre total des systèmes. La pondération w_i associée au système i est donnée par :

$$w_i = \frac{1/\sum_{j=1}^{n} \frac{1}{\varepsilon_j}}{\varepsilon_i} \quad \text{(II.13)}$$

Notons que $\sum_{i=1}^{n} w_i = 1$ et les pondérations sont inversement proportionnelles aux erreurs correspondantes et sont par conséquent plus grandes pour les systèmes les plus précis.

c. Minimum des scores (Min_score : MIN)

Dans cette méthode, on assigne au score final le meilleur (minimum) score calculé par les différents systèmes. Le minimum est défini comme suit :

$$\mathcal{D}_f = \min_i \{d_i\} \quad \text{(II.14)}$$

d. Maximum des scores (Max_score : Max)

Dans cette technique, on obtient le maximum des scores au score final (fusionné) de la façon suivante :

$$\mathcal{D}_f = \max_i \{d_i\} \quad \text{(II.15)}$$

e. Produit des scores (Mul-score : MUL)

Dans cette technique, on combine les scores par le produit qui consiste à multiplier tous les scores tel que :

$$\mathcal{D}_f = \prod_{i=1}^{n} d_i \quad \text{(II.16)}$$

Pour réaliser cette méthode, il faut que tous les scores des sous-systèmes soient homogènes. Ainsi, une étape préalable de normalisation des scores est nécessaire :

1.1 Normalisation des scores

L'objectif de cette étape est de rendre les scores obtenus des sous-systèmes homogènes, avant de les combiner, ces scores peuvent être de nature différente, exemple : Certains systèmes produisent des scores de similarité, et d'autres produisent des distances.

En effet, les sorties des systèmes individuels ne sont pas nécessairement inclues dans le même intervalle, et pour ces raisons là qu'il est nécessaire de normaliser les scores avant les combiner. Dans toute la suite, nous considérerons que tous les scores à fusionner ont été transformés en scores de similarité.

Les différentes techniques de normalisation de scores sont :

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

Ces méthodes traitent des scores qui varient déjà tous dans le même sens, en général on considère tous les scores sous forme de similarité, et pour transformer des distances en similarité il existe deux solutions : l'inverse ou l'opposé.

Normalisation par la méthode Min-Max

Dans cette méthode, on peut facilement translater les valeurs minimales et maximales des scores vers 0 et 1, respectivement. Le score normalisé par la méthode Min-Max est donné par la formule suivante :

$$n(i)=\frac{s(i)-\min(i)}{\max(i)-\min(i)} \qquad \text{(II.17)}$$

Les paramètres min(i) et max(i) sont déterminés pour chaque sous-système sur une base de développement.

Cette méthode met chaque score normalisé n(i) dans l'intervalle [0, 1], sous forme de score de similarité, avec les clients proches de la borne supérieure ou inférieure (0 ou 1) et les imposteurs proches de la borne supérieure ou inférieure (0 ou 1).

2. Niveau des décisions

La fusion au niveau des décisions est l'exécution de la combinaison des décisions issue à partir des sous-systèmes uni-modaux.

La personne présente son identifiant au système multimodal qui effectue les différentes captures nécessaires à la vérification d'identité, ensuite chaque sous-système (système unimodal) produit son décision binaire sous la forme de : OUI ou NON (0 ou 1 : client ou imposteur), ce qui nous donne comme résultat une série de OUI et de NON. Il existe plusieurs méthodes de fusion, mais les plus utilisées sont les méthodes à base de votes telles que le AND (si tous les systèmes ont décidé 1 alors OUI), le OR (si un système a décidé 1 alors OUI ou le vote à la majorité (si la majorité des systèmes ont systèmes ont décidé 1 alors OUI) [34].

II.5 Systèmes hybride

Est un système multi-biométriques qui permet d'associer les performances de plusieurs scénarios combinés. Par exemple un système multi-biométriques avec un système multi-algorithmes. Donc les systèmes hybrides disposent un grand nombre d'informations qui nous permettent une identification plus performante (taux d'identification élevée) que les précédents. [35].

II.6 Mesures de performance d'un système biométrique

Les performances d'un système biométrique sont mesurées par trois critères principaux illustrés dans la figure II.4 :

1. Taux d'erreurs égales (Equal Error Rate EER) : Il est calculé à partir des deux taux : taux de faux rejet et le taux de fausse acceptation et qui correspond à l'endroit où le FRR=FAR (le meilleur compromis entre les faux rejets et les fausses acceptations).

2. Taux de faux rejet (False Reject Rate FRR) : Il représente le pourcentage des personnes censées être reconnue mais qui sont rejeté par le système.

3. Taux de fausse acceptation (False Accept Rate FAR) : Il représente le pourcentage des personnes censées ne pas être reconnue mais qui sont accepté par le système.

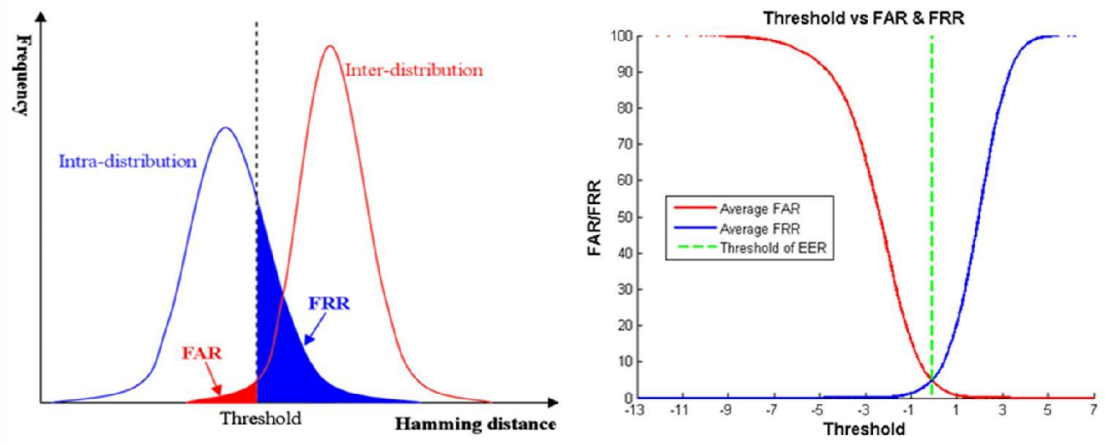
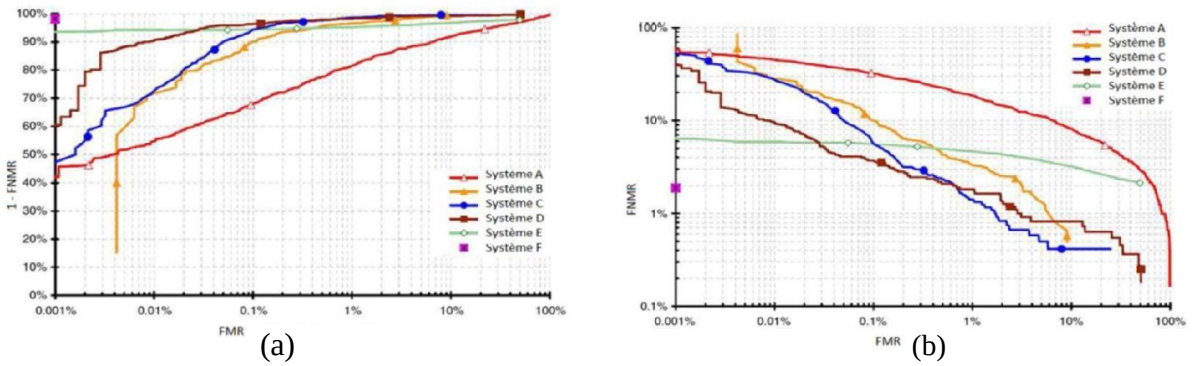


Fig. II.4 : mesures de performance d'un système biométrique : FRR, FAR et EER.

Les mesures de performance décrites dépendent généralement de la nature du système :

1) Système en mode authentification

Ce mode est caractérisé par l'utilisation de la courbe ROC (Receiver Operating Characteristic), figure II.5 (a), qui trace le taux de rejet correct en fonction du taux de fausse acceptation [36], Cependant cette courbe connaît ses limites à partir de certaines valeurs de FRR, pour cela nous avons utilisé dans notre travail une courbe nommée DET (Detection Error Trade-off), figure II.5 (b), qui représente directement le taux de faux rejet en fonction de la fausse acceptation. On dit que le système est performant si la courbe tend à épouser la forme du repère (taux de reconnaissance globale élevé).



(a) (b)

Fig. II.5 : (a) Courbe ROC et (b) Courbe DET.

2) Système en mode identification

Dans ce mode nous avons utilisé la courbe CMC (Cumulative Match Characteristic), figure II.6, qui donne le pourcentage de personne reconnues en fonction d'une variable rang [37]. On distingue deux types de reconnaissance de système :

- Système reconnait au rang 1 : lorsqu'il choisit la plus proche image comme résultat de la reconnaissance.
- Système reconnait au rang 2 : lorsqu'il choisit, parmi deux images, celle qui correspond le mieux à l'image d'entrée.

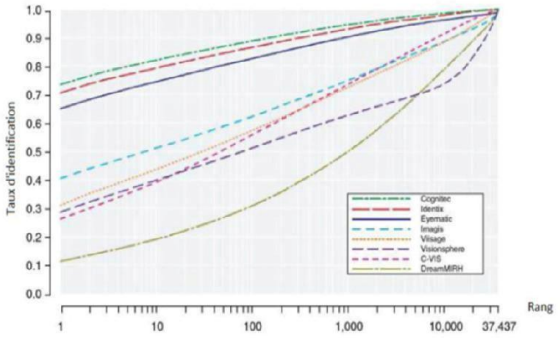


Fig. II.6 : Exemple d'un ensemble de courbes CMC.

II.7 Méthodes existantes

Les modalités biométriques palmaire et l'articulation des doigts sont attiré l'attention des chercheurs depuis quelques décennies, et reste jusqu'à présent un sujet de recherche attractif et ouvert.

Plusieurs approches sont proposées dans la littérature pour la vérification et l'identification des empreintes palmaires, les empreintes d'articulations des doigts et la fusion de ces deux modalités.

Dans cette section, nous présentons quelques systèmes biométriques unimodaux et multimodaux basées sur les deux modalités : empreinte palmaire et articulation des doigts.

Abdallah Meraoumia et al. [38]ont introduit un modèle pour la texture de l'empreinte palmaire basée sur le modèle de Markov caché (Hidden Markov Model-HMM). Leur méthode utilise la transformée en contourlet discrète pour le processus d'extraction des caractéristiques. Ensuite, le vecteur d'observations est compressé par le PCA, puis, modélise avec un HMM.

Les résultats expérimentaux montrent que la fusion de toutes les bandes spectrales donne un taux d'erreur de 0.017 %, ce taux indique que la méthode a amélioré d'une manière significative les performances du système. Ahmed Bouridane et al. [39] ont appliqué la transformation DCT sur les images de la modalité FKP pour réduire les effets dus aux changements. Les Coefficients de tous les blocs sont réorganisés afin d'obtenir un vecteur des caractéristiques. Ces vecteurs sont ensuite modélisés à l'aide d'une distribution normale multivariée (Multivariate Normal density function-MVN). Ainsi, les caractéristiques de chaque doigt sont déterminées et

plusieurs règles de fusion sont appliquées afin de construire un système multimodal. Les résultats expérimentaux obtenus montrent que cette méthode donne de meilleures performances avec un excellent taux. Lin Zhang et al. [40]choisissent d'extraire les caractéristiques biométriques à l'aide d'une ondelette de Gabor. Leur contribution consiste en la conception d'un système biométrique basé sur la combinaison de l'information locale et globale pertinente à la modalité FKP. Particulièrement, les caractéristiques biométriques, qui représentent la mesure de l'orientation locale, sont obtenues à l'aide des filtres de Gabor. Cependant, plus l'échelle des filtres de Gabor augmente plus la transformation avec ces filtres converge vers la transformée de Fourier discrète (Discrete Fourier Transform-DFT) de l'image entière. Par conséquent, la DFT de l'image entière offre un ensemble de coefficients permettant de représenter l'information globale de la modalité FKP. Leurs résultats expérimentaux sur une base de données contenant165 personnes indiquent que le système peut fonctionner avec une erreur égale à 0.402%. Abdallah Meraoumia et al. [41]proposent un système biométrique multimodal pour la reconnaissance de personne intégrant l'empreinte palmaire et la modalité FKP. Un algorithme efficace de mise en correspondance basée sur la fonction de corrélation de phase (Phase-Correlation Function-PCF) est utilisé. Les résultats expérimentaux de l'identification ont montré que le système réalise un excellent taux de reconnaissance et permet de fournir une sécurité plus élevée que le système biométrique unimodal.

II.8 Conclusion

La multi-modalité, consiste à la combinaison de plusieurs technologies biométriques, ou plusieurs algorithmes de reconnaissance. Dans ce chapitre, nous avons présenté la biométrie multimodale ainsi les différentes limitations des systèmes biométriques unimodaux. D'autre part, nous avons présenté les différents types de combinaisons des modalités possibles, les architectures et les niveaux de fusion qui peuvent être utilisés dans un système multimodal. La fusion au niveau des scores est le type de fusion le plus utilisé. Afin de réaliser une fusion au niveau des scores, il faut que tous les scores issus des sous-systèmes soient homogènes. Pour cet raison les méthodes de combinaison des scores nécessitent une étape préalable de normalisation des scores.

Conception et résultats Expérimentaux

III.1 Introduction

Dans les systèmes biométriques on distingue plusieurs étapes enchainées pour arriver à l'identification des individus : l'acquisition d'une modalité biométrique, l'extraction d'un vecteur de caractéristiques, et la classification. Le choix de caractéristiques qui composent les vecteurs d'entrée du système biométrique est une étape cruciale qui déterminera la qualité de classifieur. Dans ce chapitre, nous avons utilisé l'Histogramme de Gradient Orienté (HOG) afin d'extraire un vecteur qui peut être représenté efficacement les caractéristiques discriminantes des différentes modalités. Afin de concevoir un système robuste et efficace, dans une deuxième étape, nous avons testé plusieurs systèmes biométriques unimodal et multimodal. Des bases des données types sont utilisées pour évaluer les performances des systèmes proposés.

III.2 Méthode proposée

Dans notre travail, nous avons proposé des systèmes biométriques multimodaux basés sue deux modalités biométriques liées à la main et deux classifieur a savoir le classifieur à distance minimale (1-ppv) et la fonction à base radiale (RBF). Dans les différents systèmes l'extraction des caractéristiques est basée sur le HOG. La figure suivante (voir Fig. III.1) montre nos systèmes proposés. Comme montre cette figure deux niveaux de fusion sont utilisés, à savoir la fusion au niveau des images et la fusion au niveau des scores. Pour les systèmes unimodaux,

les caractéristiques de chaque modalité sont extraites, séparément, via la méthode HOG, ensuite ces derniers sont utilisés dans les deux classifieurs (S1, S2, S3 et S4).

Quant aux systèmes multimodaux, dans une première série des tests, les deux modalités (PLM et LIF) sont fusionnées au niveau des images via l'utilisation de trois méthodes de fusion (DWT, PCA et LP).L'image résultante est utilisée comme une nouvelle modalité biométrique et le reste de système est similaire au system unimodal (par exemple (S5et S4). Dans la deuxième série de tests, la fusion au niveau des scores est examinée. Dans cette série, plusieurs systèmes multimodaux, à savoir le système multi-biométrique (S9 et S10), le système multi-algorithmique (S8 et S11) et le système hybride (S7, S12 et S13), sont évalués.

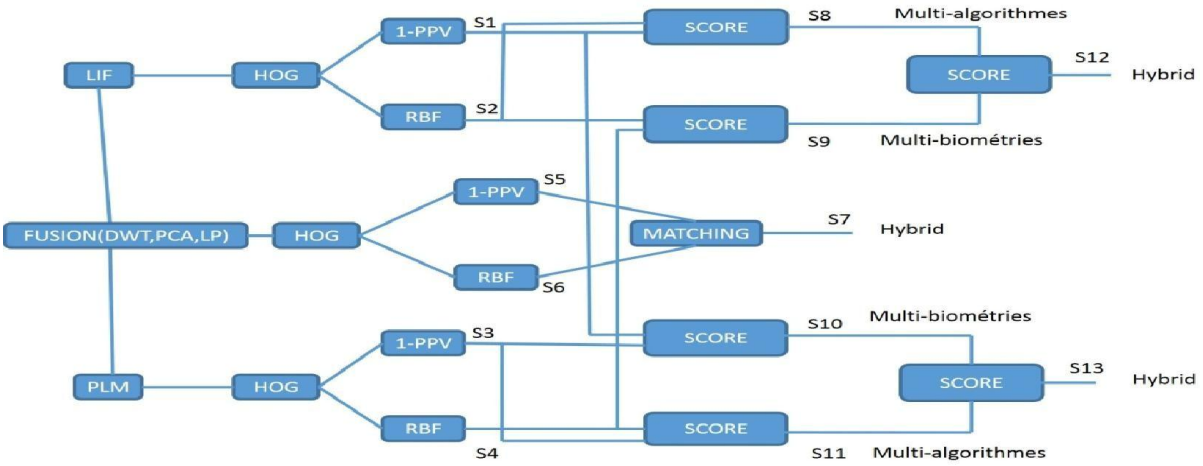


Fig. III.1 : Architecture proposée

III.2.1 Histogramme des gradients orientés

Le HOG est une nouvelle méthode utilisée en vision par ordinateur pour la détection d'objet et la détection des régions d'intérêts. Le principe de base de cette méthode est de calculer les histogrammes locaux de l'orientation du gradient sur une grille dense, c'est-à-dire sur des zones régulièrement réparties sur l'image.

L'objectif du de la méthode HOG est que l'apparence et la forme locale d'un objet dans une image peuvent être décrites par la distribution de l'intensité du gradient ou la direction des contours. La figure III.2, illustre les différentes étapes de la méthode HOG. Le principe de cette méthode consiste à diviser une image à des régions adjacentes de petite taille, appelées cellules, et en calculant pour chaque cellule l'histogramme des directions du gradient ou des orientations des contours pour les pixels à l'intérieur de cette cellule. La combinaison des histogrammes forme alors le descripteur HOG. Pour de meilleurs résultats, les histogrammes locaux sont normalisés en contraste, en calculant une mesure de l'intensité sur des zones plus larges que les

cellules, appelées des blocs, et en utilisant cette valeur pour normaliser toutes les cellules du bloc. Cette normalisation permet une meilleure résistance aux changements d'illuminations et aux ombres.

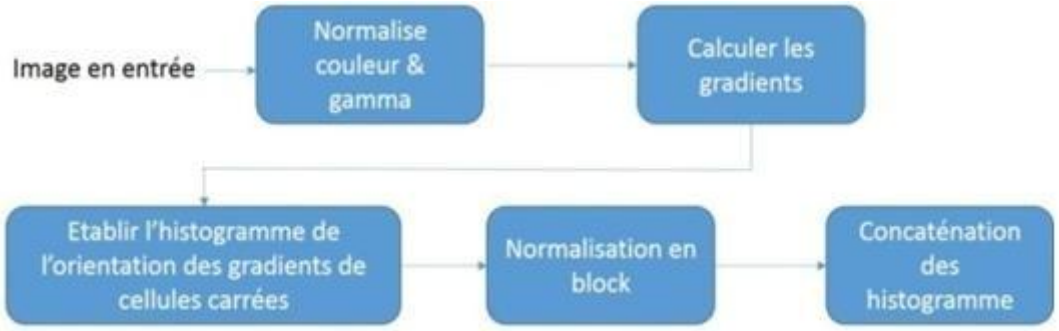


Fig. III.2 : Schéma des blocs de méthode HOG

III.2.2 Classifieur à distance minimale (1-PPV)

Ce le classifieur le plus simple pour concevoir une chaine de reconnaissance des formes. Il est basé sur des distances mesurées entre des vecteurs extraits de l'image de test et l'ensemble des vecteurs préenregistrées dans une base de références. Plusieurs distances peuvent être utilisées, distance euclidienne, distance Hamming….etc. Dans nos tests, une distance euclidienne, la somme des absolues des déférences (Sum of Absolute Diference (SAD), est utilisée.

III.2.3 Classifieur à fonction de base radiale (RBF)

Les réseaux à fonctions de base radiales (RBF) sont des modèles connexionnistes simples à mettre en œuvre et assez intelligibles, et sont très utilisés pour la régression et la discrimination. Leur propriétés théoriques et pratiques ont été étudiées en détail depuis la fin des années 80 ; il s'agit certainement, avec le Perceptron multicouche, du modèle connexionniste le mieux connu. Une fonction de base radiale (RBF) est une fonction Ø symétrique autour d'un centre μ_j:$Ø_j(x) = Ø(||x - \mu_j||)$, où ||.|| est une norme.

III.3 Résultats et discussions

II.3.1 Bases de données

1) Base de données LIF : Dans notre travail nous avons utilisé la base d'empreinte d'articulation de doigts de l'index gauche (LIF) créé par l'Université de Polytechnique de Hong Kong (PolyU). Cette base de données contient 165 personnes dont 125 personnes sont des masculins. 143 personnes ayant l'âge compris entre 20 et 30 ans et les autres ayant l'âge entre 30 et 50 ans. Les images de chaque doigt sont capturées en deux sessions avec un intervalle de

25 jours entre deux sessions. Six images de chaque doigt ont été collectées. Ce qui nous donne une base de données finale de 1980 images en niveaux de gris.

2) Base de données PLM : La deuxième base de données qu'on a utilisée dans notre travail est l'empreinte palmaire créée par la même université. Cette base de données contient 165 personnes dont 131 personnes sont des masculins. 138 personnes ayant l'âge de 30 ans et les autres ayant l'âge entre 30 et 50 ans. Les images de chaque palme sont capturées en deux sessions chaque session contient dix images, l'intervalle moyen entre les deux sessions est 69 jours. Ce qui nous donne une base de données finale qui rassemble un total de 3300 images en niveaux de gris.

3) Base de données multimodale : Il est à noter qu'il n'existe pas une base des données multimodale qui regroupe les deux modalités (PLM et FKP), pour cela une base synthétique, avec les bases précédemment décrites, est utilisée. La Fig III.3 montre un exemple des images dans la base multimodale décrite.

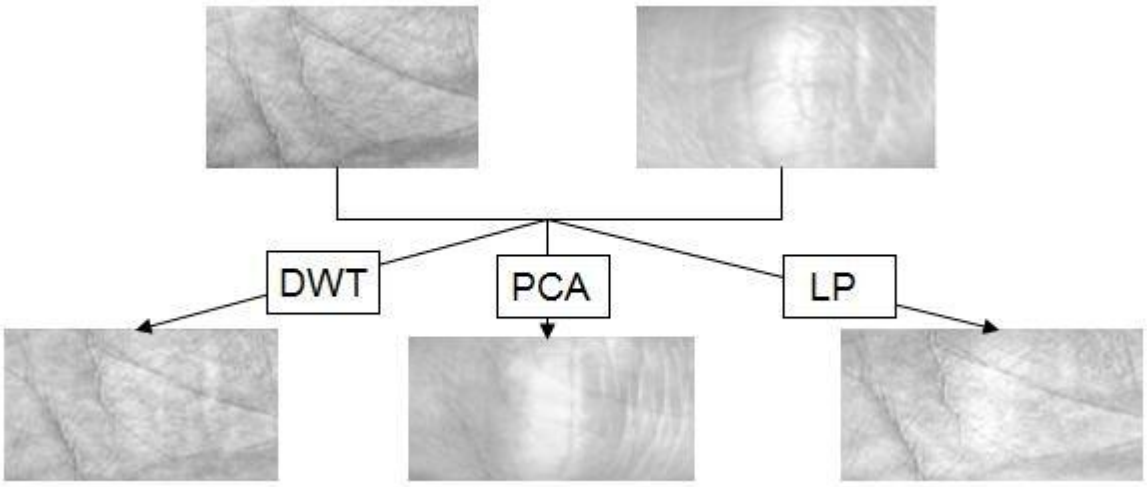


Fig. III.3 : Exemple des images dans la base multimodale. (gauche) Image fusionnée par la méthode DWT, (milieu) Image fusionnée par la méthode PCA et (droite) Image fusionnée par la méthode LP (c)

III.3.2 Protocole de tests

Dans la phase d'identification, nous avons utilisé une base de données contenant 165 personnes (12 images pour chaque personne). Trois images (prises aléatoirement dans des sessions écartées) pour construire la base de références, en totale 495 images sont utilisées dans la phase d'enrôlement. Le reste des images (1485 images), huit images pour chaque personne, sont utilisées pour tester les performances des systèmes proposés. Dans la phase des tests, 109560 distances sont calculées, dont 1320 représentent des distances clients et le reste (108240 distances) sont des distances imposteurs. Tous les systèmes sont testés dans les points de

fonctionnement représenté par le EER. En outre, les différents systèmes sont testés dans deux modes d'identification, ensemble ouvert et ensemble fermé.

III.4 Evaluation des performances

Les résultats expérimentaux que nous allons présenter dans cette section sont divisés dans deux grandes parties. La première partie contient tous les systèmes unimodaux. Tandis que la deuxième partie regroupe les systèmes multimodaux. Cette partie est à la fois décomposée en trois sections qui traitent les différentes architectures proposées. Dans la fin de ces expériences une comparaison entre les meilleurs systèmes est faite afin de sélectionner le meilleur système.

III.4.1 Systèmes unimodaux

Dans cette section les performances des systèmes unimodaux proposés sont évaluées. Comme nous l'avons déjà présenté dans la section précédente (Fig. III. 1) quatre systèmes unimodaux sont proposés. Les deux premiers systèmes (S1 et S2) sont basés sur les LIFs. Quant aux systèmes S3 et S4, les PLMs sont utilisées. Pour chaque modalité, nous avons utilisé, séparément, deux classifieur (1PPV et RBF).

Avant d'évaluer les performances des différents systèmes, une phase de sélection de paramètre concernant l'algorithme HOG est exécutée. Ce dépend de deux paramètres importants qui sont la taille de bloc et le pourcentage de chevauchement entre les blocs adjacents. Ce que nous intéressent c'est bien la taille de bloc (plusieurs travaux montrent que un pourcentage de chevauchement égale à 50%est suffisant pour que l'algorithme fonctionne efficacement).Pour avoir des meilleurs paramètres (paramètres optimaux), nous avons testé l'algorithme HOG avec des blocs de différents tailles, par exemple 3×3, 5×5,…,33×33 et avec le même pourcentage de chevauchement pour les deux modalités et avec les deux classifieurs 1-PPV et RBF. L'objectif de la variation dans la taille des blocs est d'avoir des meilleurs résultats en fonction de temps d'enrôlement, temps de reconnaissance, de la taille de vecteur de caractéristiques, la taille de vecteur de caractéristiques sur disques et le taux d'erreurs.

1) Classifieur 1-ppv: Les tableaux III.1 et III.2 représentent les différents résultats obtenus en utilisant plusieurs tailles des blocs et le classifieur 1-ppv. Dans notre travail, la sélection de paramètre de HOG est basée essentiellement sur le EER (c'est le paramètre d'évaluation le plus important dans les systèmes biométriques).

Tableau III.1: Résultats d'exécution du HOG avec la modalité LIF et le classifieur 1-PPV

W*W	EER	Temps		Tailles	
		Enrôlement	Reconnaissance	Vecteur de caractéristiques	Sur disque(Ko)
3*3	4.0437	7.105531	0.0137	81	0.843
5*5	3.0976	8.072950	0.0172	225	1.88
7*7	3.0415	8.519990	0.0196	441	3.43
9*9	2.3388	9.764864	0.0274	729	5.42
11*11	2.5947	9.822992	0.0254	1089	7.89
13*13	3.5686	10.820667	0.0285	1521	10.5
15*15	3.7276	13.861840	0.0352	2025	13.7
17*17	3.4518	13.260013	0.0380	2601	16.8
19*19	5.1026	15.214206	0.0418	3249	20.4
21*21	4.5791	15.565848	0.0503	3969	23.6
23*23	6.1051	17.229365	0.0570	4761	28.3
25*25	5.7301	27.647703	0.0657	5625	31.6
27*27	12.3728	20.313632	0.0707	6561	35.6
29*29	12.1643	23.029499	0.0780	7569	42.4
31*31	11.3805	25.060343	0.0906	8649	48.6
33*33	10.9903	27.636942	0.1041	9801	55.1

Tableau III.2 : Résultats d'exécution du HOG avec la modalité PLM et le classifieur 1-PPV

W*W	EER	Temps		Tailles	
		Enrôlement	Reconnaissance	Vecteur de caractéristiques	Sur disque(Ko)
3*3	0.5378	8.932	0.0312	81	0.843
5*5	0.404	12.7747	0.0438398	225	1.88
7*7	0.404	9.596394	0.0485488	441	3.43
9*9	0.3574	11.011900	0.0467876	729	5.42
11*11	0.3646	13.918887	0.0599732	1089	7.89
13*13	0.2694	15.193169	0.052252	1521	10.5
15*15	0.2694	18.660288	0.0687096	2025	13.7
17*17	0.2694	18.656470	0.0751018	2601	16.8
19*19	0.5387	19.375805	0.076147	3249	20.4
21*21	0.404	22.056992	0.1058964	3969	23.6
23*23	0.4774	25.063378	0.0992962	4761	28.3
25*25	0.8754	25.453316	0.1108592	5625	31.6
27*27	0.6146	28.678815	0.143922	6561	35.6
29*29	0.6061	32.097001	0.1437054	7569	42.4
31*31	0.5284	36.808255	0.1883806	8649	48.6
33*33	0.6061	39.149008	0.1663702	9801	55.1

Pour l'empreinte LIF, le tableau III.1montres que notre système a identifié une personne d'une façon efficace, avec un taux d'erreur EER égal à 2.3388% pour un bloc de taille 9×9. Par contre, pour l'empreinte PLM, cette taille est égale à 13×13, dans ce cas l'EER devient 0.2694%. Pour mieux illustrés l'influence des autres paramètres, la figure III. 4 montres l'évolution des autres paramètres d'évaluation en fonction de la taille de bloc. Il est clair que ces paramètres sont très influencés par la taille de bloc. L'augmentation de ce dernier provoque des mauvaise performances vis-à-vis la taille de template, temps d'exécution pour l'enrôlement et la reconnaissance.

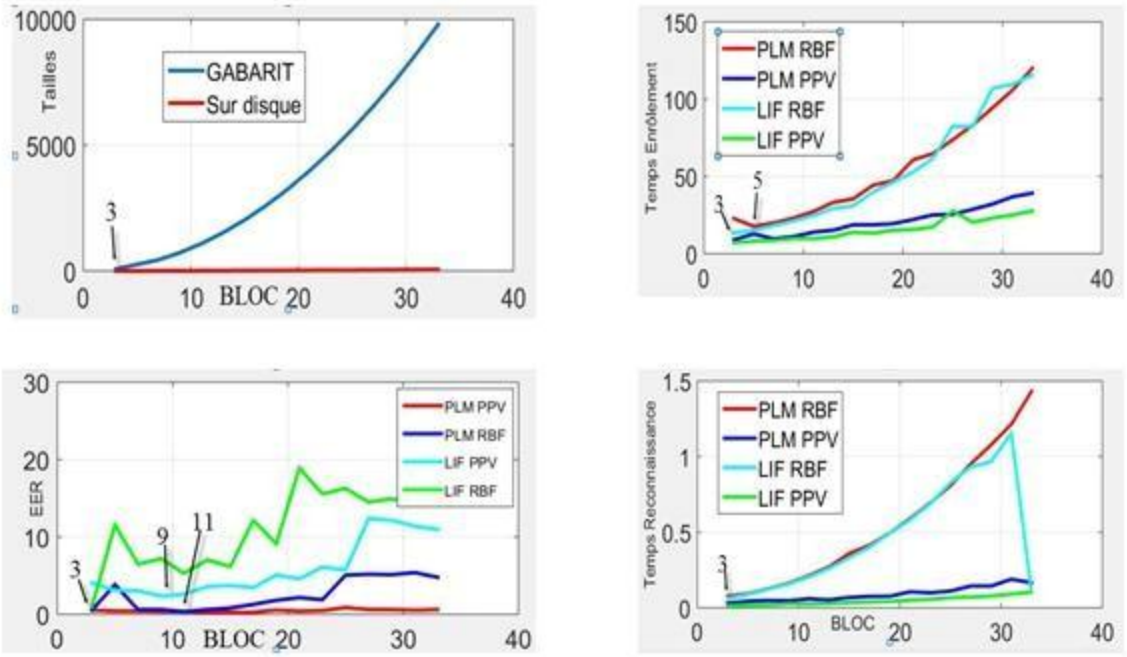


Fig. III.4: Résultats d'exécution du HOG.

2) Classifieur RBF : Les mêmes tests effectués dans le cas de 1-PPV sont répétés dans l'utilisation de classifieur RBF afin de sélectionner le meilleur paramètre minimisant le EER. Pour l'empreinte LIF, le tableau III. 3 montres que notre système fonctionne d'une façon efficace, avec un taux d'erreur EER égal à 0.9712% pour un bloc de taille 3× 3. Par contre, pour l'empreinte PLM, cette taille est égale à 11×11, dans ce cas l'EER devient 0. 3367%.

Tableau III.3:Résultats d'exécution du HOG avec la modalité LIF et le classifieur RBF

W *W	EER	Temps		Tailles	
		Enrôlement	Reconnaissance	Vecteur de caractéristiques	Sur disque(Ko)
3*3	0.9712	13.477403	0.0619	81	0.843
5*5	11.5351	15.157918	0.0891	225	1.88
7*7	6.4692	18.124101	0.1225	441	3.43
9*9	7.2054	21.107682	0.1571	729	5.42
11*11	5.2848	24.660319	0.2040	1089	7.89
13*13	7.037	29.273841	0.2597	1521	10.5
15*15	6.1715	31.032362	0.3309	2025	13.7
17*17	12.1526	39.909061	0.4012	2601	16.8
19*19	9.1149	46.236219	0.4934	3249	20.4
21*21	18.9153	52.894519	0.5816	3969	23.6
23*23	15.5628	61.587901	0.6887	4761	28.3
25*25	16.2791	82.442336	0.8274	5625	31.6
27*27	14.4896	82.118172	0.9325	6561	35.6
29*29	14.9454	107.014457	0.9658	7569	42.4
31*31	14.1209	109.564342	1.1536	8649	48.6
33*33	27.6102	115.634474	0.1052	9801	55.1

Tableau III.4:Résultats d'exécution du HOG avec la modalité PLM et le classifieur RBF

W *W	EER	Temps		Tailles	
		Enrôlement	Reconnaissance	Vecteur de caractéristiques	Sur disque(Ko)
3*3	0.5387	22.811430	0.0764	81	0.843
5*5	3.8384	17.655904	0.0936	225	1.88
7*7	0.6061	19.855800	0.1256	441	3.43
9*9	0.6168	23.033645	0.1622	729	5.42
11*11	0.3367	27.267891	0.2118	1089	7.89
13*13	0.6061	33.196044	0.2698	1521	10.5
15*15	0.8081	35.442743	0.3594	2025	13.7
17*17	1.2795	44.335075	0.4126	2601	16.8
19*19	1.8118	47.165685	0.4948	3249	20.4
21*21	2.1549	60.652585	0.5893	3969	23.6
23*23	1.8855	64.726470	0.6939	4761	28.3
25*25	5.0505	73.765120	0.8088	5625	31.6
27*27	5.1852	83.166549	0.9519	6561	35.6
29*29	5.1178	94.374456	1.0770	7569	42.4
31*31	5.3872	105.838685	1.2137	8649	48.6
33*33	4.7811	119.979891	1.4311	9801	55.1

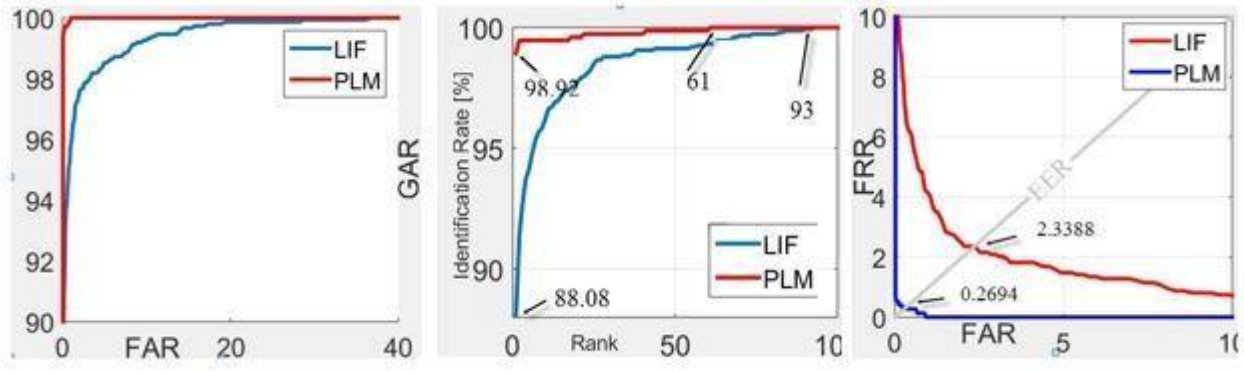
Après avoir sélectionné la meilleure taille de bloc pour les deux modalités, une comparaison entre les différents systèmes est effectuée. Les résultats de comparaison sont illustrés dans le tableau III.5 qui regroupe les deux modes d'identifications (ensemble ouvert et fermé).

Tableau III.5 : Performances des systèmes unimodaux

Classifieurs	Modalité	Systèmes	Ensemble ouvert		Ensemble fermé	
			T_0	EER	ROR	RPR
1-PPV	LIF	S1	0,1928	2,3388	88.08	93
	PLM	S3	0,2085	0,2694	98.92	61
RBF	LIF	S2	0,7158	0,9712	95.55	127
	PLM	S4	0,7123	0,3367	98.38	100

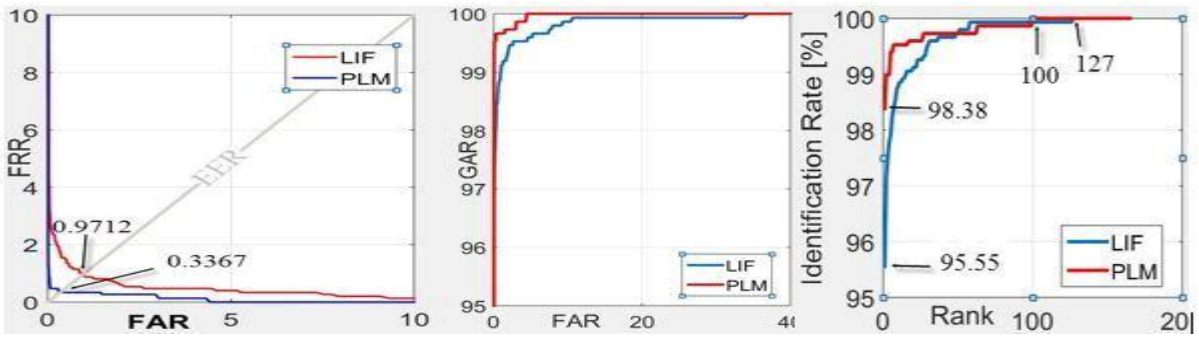
Nous observons que, en général, dans le classifieur 1-PPV, les erreurs obtenus sont très acceptables et en particulier dans le cas de la modalité PLM qui fonctionne avec une erreur égale à 0,2694 % pour un seuil To = 0,2085 dans l'identification ensemble ouvert. Un ROR de 98,92 % et un RPR de 61 en mode ensemble fermé sont obtenus.

D'une façon similaire les deux modalités sont utilisées dans un classifieur RBF et les résultats sont représentés dans le même tableau. La modalité PLM est toujours meilleure par rapport au LIF donnant une erreur égale à 0,3367 % avec un seuil To =0,7123 en mode ensemble ouvert, et un ROR de 98,38 % avec un RPR de 100 en mode ensemble fermé.



(a) (b) (c)

Fig. III. 5: Performances d'identification des PLMs et LIFs avec le classifieur 1-PPV. (a) courbe ROCs, (b) courbe DET, (c) courbe CMC.



(a) (b) (c)

Fig. III.6 : Performances d'identification des PLMs et LIFs avec le classifieur RBF. (a) courbe ROCs, (b) courbe DET, (c) courbe CMC.

Les figures III.5 et III.6 (performances des systèmes dans les deux modes d'identification) montres bien l'efficacité de la modalité PLM par rapport au LIF. Pour le classifieur 1-PPV (figure III.8) ; une amélioration de 88.50% pour l'ensemble ouvert et de 90.94% pour l'ensemble fermé sont obtenues si en remplacer cette dernière avec le LIF. Des faibles améliorations de 65.33% et de 63 .6% pour l'ensemble ouvert et fermé, respectivement, sont obtenues dans le cas de classifieur RBF (figure III.9).

III.4.2 Systèmes multimodaux

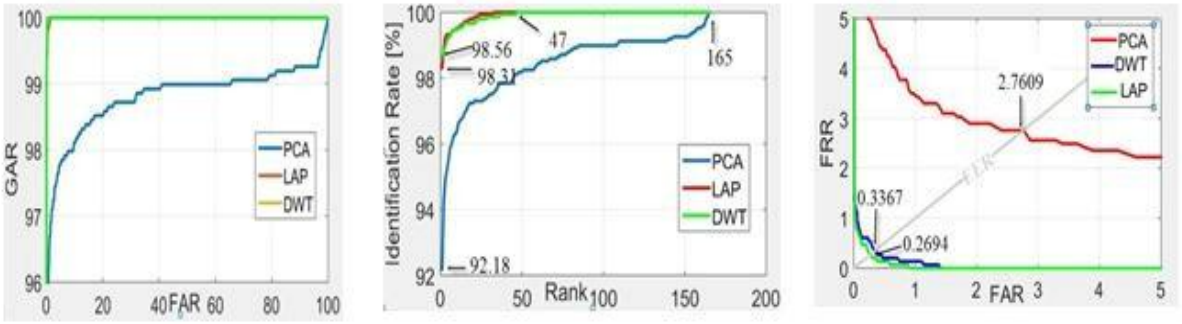
Dans cette deuxième partie, les performances des systèmes multimodaux proposés sont évaluées. Comme nous l'avons déjà mentionné précédemment, deux niveaux de fusion sont utilisés. Pour cela, dans la première sous-partie nous allons essayer d'évaluer, en premier temps, les systèmes multi-biométriques basés sur la fusion au niveau image (S5 et S6). Ensuite, le même scenario est examiné, mais cette fois-ci avec la fusion au niveau score (S9 et S10). Dans la deuxième sous-partie, les systèmes multi-algorithmiques (S8 et S11) sont évalués. Finalement, les performances des systèmes hybrides (S7, S12 et S13) sont testées dans la dernière sous-partie.

1) Systèmes multi-biométriques : Dans ce scénario, les deux modalités biométriques PLM et LIF sont combinées avec les trois méthodes de fusion d'images, décrites dans le chapitre II, (DWT, PCA et LP). Le tableau et ci-dessous représente les différents résultats obtenus. D'après ce tableau, la méthode de fusion basée sur LP est bien adaptée pour le classifieur 1-PPV, elle donne une erreur égale à 0.2694% avec un seuil, To, égal à 0.2548. Contrairement, le classifieur RBF fonctionne bien avec les images fusionnées par la méthode DWT. Dans ce cas, une erreur égale à 0.9428% (To = 0.1891) est obtenue.

Tableau III.6 : Résultats des systèmes multi-biométriques (fusion au niveau image)

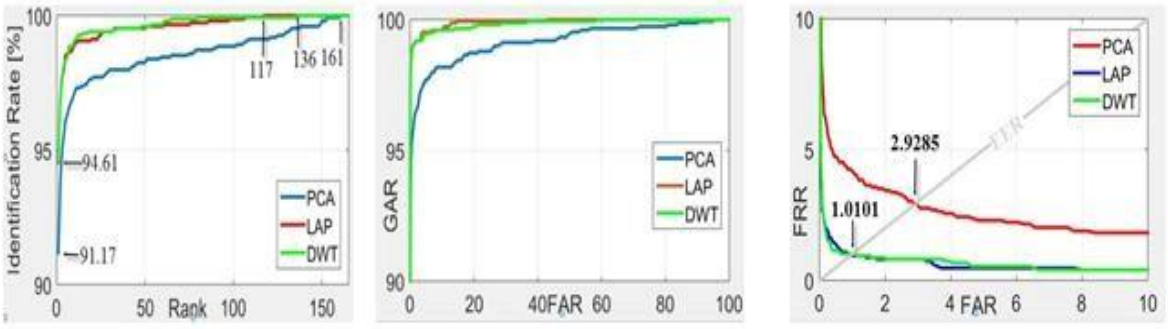
METHODES DE FUSION		1-PPV (S5)	RBF (S6)
PCA	T_0	0.2548	0.5594
	EER	2.7609	2.9285
	ROR	92.18	91.17
	RPR	165	161
DWT	T_0	0.1891	0.6940
	EER	0.3367	0.9428
	ROR	98.65	94.61
	RPR	47	136
LP	T_0	0.1854	0.6704
	EER	0.2694	1.0101
	ROR	98.31	94.54
	RPR	33	117

Afin de montré les performances des différentes méthodes de fusion, nous avons présenté, dans les figure III.7 et III.8, une comparaison entre eux dans les modes d'identification.



(a) (b) (c)

Fig. III.7 : Performances d'identification des images fusionnées par les méthodes DWT, PCA et LP avec le classifieur 1-PPV. (a) courbe DETs (b), courbe CMCs, (c) courbe ROCs.



(a) (b) (c)

Fig. III.8 : Performances d'identification des images fusionnées par les méthodes DWT, PCA et LP avec le classifieur RBF. (a) courbe CMCs, (b) courbe DETs, (c) courbe ROCs

Dans ce que se suit, les systèmes multi-biométriques basés sur la fusion au niveau scores sont évalués. Une faible erreur égale à 0.0107% pour le classifieur RBF avec la règle de fusion SUM est obtenue. Dans ce cas, des taux d'amélioration 96.03% et 94.87%par rapport, respectivement, au système multi-biométrique basé sur la fusion au niveau images et système uni-modal basé sur la modalité PLM et le classifieur 1-PPV. Ces résultats montrent bien la haute performance de la fusion au niveau scores.

Tableau III.7- Résultats des systèmes multi-biométriques (fusion au niveau score).			
Modalité Classifeur		PLM-LIF	PLM-LIF
		1-PPV (S10)	RBF (S9)
SUM	T_0	0.0329	0.7805
	EER	1.6424	0.0107
	ROR	99.93	99.73
	RPR	2	3
MIN	T_0	0.1515	0.999
	EER	0.0345	0.0337
	ROR	99.59	96.70
	RPR	5	2
MAX	T_0	2.9996	0.6418
	EER	0.0805	0.1291
	ROR	93	99.59
	RPR	4	37
MUL	T_0	2.9975	0.5595
	EER	0.0821	0.0329
	ROR	93	99.73
	RPR	3	6

2) Systèmes multi-algorithmiques : Dans ce scenario, nous allons mettre en commun les deux classifieurs (1-KPP et RBF) afin de créer un système multi-algorithmiques, en fusionnant les scores issues du chaque classifieur (fusion au niveau scores). Normalement, il est possible d'améliorer l'efficacité et la robustesse des systèmes d'identification de l'empreinte quand la fusion a été réalisée. Dans notre méthodologie, deux représentations différentes de l'empreinte (PLM ou LIF) ont été fusionnées au niveau des scores par les quatre règles de fusion (SUM, MAX, MIN et MUL). Cependant, une étude comparative concernant la performance du système est effectuée. Le but étant de pouvoir choisir la meilleure règle de fusion (on change à chaque fois la règle de fusion) pour concevoir un système d'identification biométrique fonctionne avec une minimale. Donc, l'objectif principal de cette sous-partie est l'étude de l'effet de la règle de fusion sur la performance du système d'identification. Pour ce faire, les taux d'erreurs du système en fonction des différentes règles ont été mesurés et les résultats sont illustrés dans le tableau ci-dessous (Tableau III.8).

Nous pouvons tout d'abord noter que toutes les règles de fusion améliorent les performances du système, cela confirme bien l'importance de la fusion au niveau des scores. Pour l'identification ensemble ouvert, il est clair d'après ce tableau, que la règle de fusion SUM offre la meilleure performance en comparaison avec les autres règles conduisant à un faible taux d'erreur, égal à 0.1347%, pour la modalité PLM.

Tableau III.8 : Performance des systèmes multi-algorithmiques.

Modalité / Classifeur		PLM	LIF
		1-PPV-RBF (S11)	1-PPV-RBF (S8)
SUM	T_0	0.7865	0.7181
	EER	0.1347	0.2320
	ROR	99.12	96.56
	RPR	54	112
MIN	T_0	0.8052	0.8217
	EER	0.1873	1.3395
	ROR	98.38	91.51
	RPR	52	97
MAX	T_0	0.9614	0.7028
	EER	0.2694	0.8754
	ROR	99.25	96.16
	RPR	71	115
MUL	T_0	0.5797	0.5571
	EER	0.2093	0.8754
	ROR	99.12	96.49
	RPR	54	114

La règle MIN aussi peut améliorer efficacement la performance de système avec une faible erreur égal à 0.1873%. Finalement, pour compléter le protocole de test, le même tableau montre une comparaison entre les déférents systèmes dans l'identification ensemble fermé. D'après ces résultats, nous constatons que la règle de fusion MAX donne le meilleur taux d'identification et il peut atteindre, dans le cas de PLM, un ROR = 99.25% (RPR = 71) au lieu de 96.56% (RPR = 112) dans le cas du LIF.

3) Systèmes hybrides : Les systèmes hybrides permettent d'associer les performances des différents scenarios en combinant les systèmes multi-biométriques avec les systèmes multi-algorithmiques. Ils permettent d'augmenter les performances de l'identification du point de vue taux d'erreur. Dans le mode d'identification ensemble ouvert et fermé, le Tableau III.9 présente les taux retenus pour les différents systèmes en respectant les différentes règles de fusion. Ce tableau montre que les règles de fusion SUM, MUL et MAX donnent des résultats parfaits, soit avec l'ensemble ouvert (EER = 0%), ou avec l'ensemble fermé (ROR = 100%) dans le cas de système S12. Tandis que la règle MIN donne un mauvais résultat, EER = 2.4637% et ROR = 99.73% pour respectivement l'identification ensemble ouvert et fermé.

Tableau III.9 : Résultats des systèmes hybrides.				
SYSTEME HYBRIDES		S12	S7	S13
SUM	T_0	0.981	0.7885	0.2694
	EER	0000	0.1347	0.7246
	ROR	100	99.95	98
	RPR	1	15	52
MIN	T_0	0.9601	0.999	0.8160
	EER	2.4637	0.0846	0.3367
	ROR	99.73	92.92	96
	RPR	3	6	34
MAX	T_0	0.99	0.7706	0.6759
	EER	0000	0.1347	0.4040
	ROR	100	99.59	98.72
	RPR	1	45	125
MUL	T_0	0.963	0.6524	0.564
	EER	0000	0.1347	0.2694
	ROR	100	99.59	98
	RPR	1	18	83

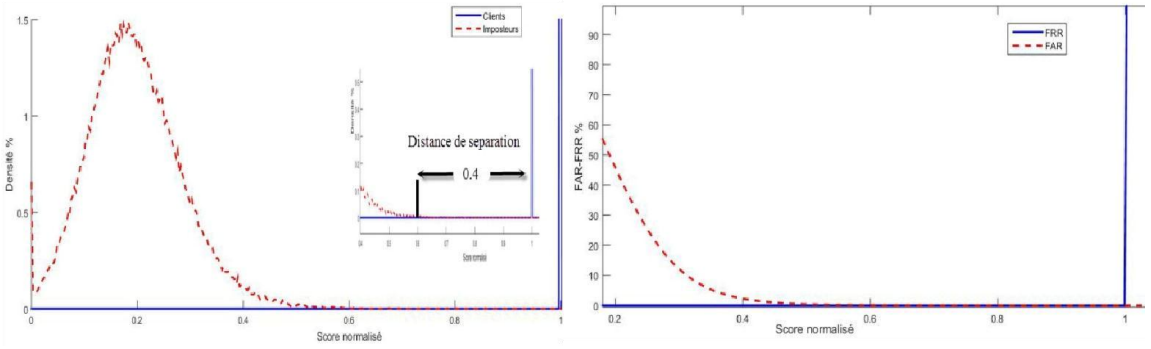
Pas d'amélioration vraiment remarquable pour les deux autres systèmes (S7 et S13). Une minimum erreur égale à 0.0846% est obtenue dans le mode d'identification ensemble ouvert pour le système S7. Ce système fonction avec un ROR = 99.95% dans le mode d'identification ensemble fermé.

III.5 Commentaires sur l'évaluation

Noter bien qu'il n'existe pas encore de critères universels ni de méthodologie standard permettant de comparer des algorithmes de fusion entre eux ; de même qu'il est encore difficile de trouver des bases de données multimodales composées d'utilisateurs réels en nombre élevé. En revanche, notre étude comparative est basée sur le taux de reconnaissance de système. Cependant, nous avons effectué une étude comparative concernant ce taux de reconnaissance dans les différentes architectures (unimodal et multimodal). Le but étant de pouvoir choisir la meilleure architecture pour concevoir un système de reconnaissance biométrique. Il est clair, d'après nos résultats, qu'une combinaison des plusieurs systèmes uni-modaux peut être employée pour atteindre une performance plus élevée.

D'après les résultats des tests, le système d'identification basé le PLM et/ou le LIF est un système fiable. Il permet une bonne séparabilité des classes clients et imposteurs. Cependant, La figure Fig. III.18.(a) illustre les densités de probabilité des scores (clients et imposteurs) et la distance de séparation entre les deux distributions pour le meilleur système (système S12). Notons qu'une distance de séparation négative indique un recouvrement entre les distributions tandis qu'une distance de séparation positive indique un espacement entre les distributions. D'après cette figure, il est clair que la région de recouvrement entre les scores clients et

imposteurs est nulle avec une large distance de séparation égale à 0.4 à partir de 0.6 jusqu'au 1.0. La figure Fig. III.9.(b) montre l'évolution des deux taux d'erreurs, le FAR et le FRR lorsque le seuil varie. Il est clair que les allures de ces deux courbes sont totalement séparées ce qui génère un taux d'erreur égal à zéro. Cependant, le seuil de sécurité, T_o, doit être choisi dans l'intervalle [0,843 … 0,996].



(a) (b)

Fig. III.9- Performances d'identification de meilleur système S1. (a)Distribution des clients et imposteurs, (b) taux d'erreur FAR et FRR.

Pour résumé, nous considérons les résultats obtenus comme satisfaisants. L'ensemble des tests effectués a permis de conclure, qu'avec l'utilisation de la fusion des deux modalités (fusion multi-biométrique) et la fusion des deux algorithmiques (fusion multi-algorithmique), nous avons apporté une amélioration considérable au taux d'identification grâce à ces fusions, ces résultats induisent l'augmentation des performances du système.

Finalement, nous pouvons remarquer que nos méthodes ont été testées sur un grand nombre d'utilisateurs multimodaux possibles (165) provenant d'une base de données officielle qu'est PolyU. Ce nombre d'utilisateurs, qui est un paramètre très important pour juger de la robustesse d'une méthode, est plus élevé que celui issu dans plusieurs travaux effectués dans la littérature. Enfin, dans la plupart des travaux concurrents, il est rare que les résultats soient présentés de manière aussi complète que nous l'avons fait : uniquement les taux erreur ou les taux de reconnaissance dans un seul mode opératoire (ensemble ouvert ou fermé) est présenté.

III.6 Conclusion

Dans ce chapitre, les travaux biométriques présentés ont conduit à l'élaboration d'un système d'identification des personnes par reconnaissance d'empreintes PLM et LIF. Pour ce faire, Nous avons proposé plusieurs systèmes biométriques. Outre les systèmes unimodaux, nous avons exploré quelques systèmes multimodaux. Ces différents systèmes sont testés dans le but d'améliorer le taux d'identification dans les deux modes d'identification, ensemble ouvert et

ensemble fermé. En validant ces systèmes sur une base de données type de 165 personnes, nous avons dégagé une amélioration considérable du taux d'identification (100%) avec la méthode d'extraction des caractéristiques utilisée (HOG). Cette méthode a montré une amélioration remarquable par rapport à d'autres méthodologies basée sur des méthodes d'analyses de texture (par exemple LBP et LPQ).

Conclusion Générale

Le travail présenté dans ce mémoire s'inscrit dans le contexte de l'identification automatique des personnes. Nous avons utilisés deux modalités biométriques, à savoir l'empreinte palmaire (PLM) et les empreintes des articulations des doigts (LIF) afin de réaliser nos systèmes biométriques proposés, mono et multimodaux.

Après avoir introduit les concepts généraux de la biométrie, nous avons présenté les méthodes de fusion des modalités biométriques ainsi la méthode des Histogrammes des Gradients Orientés (HOG) permettant d'extraire un vecteur de caractéristique discriminant.

Nous avons proposé plusieurs systèmes biométriques, outre les systèmes unimodaux, nous avons proposé quelques systèmes multimodaux. Ces différents systèmes sont testés dans le but d'améliorer le taux d'identification dans les deux modes d'identification, ensemble ouvert et ensemble fermé. Ces systèmes sont testés sur une base de données type de 165 personnes. Nous avons dégagé une amélioration considérable du taux d'identification (100%) avec la méthode d'extraction des caractéristiques utilisée (HOG). Cette méthode a montré une amélioration remarquable par rapport à d'autres méthodologies basée sur des méthodes d'analyses de texture (par exemple LBP et LPQ).

Référence :

[1] A. Bouridane, « Imaging For Forensics and Security: From Theory to Practice », Springer series on Singnals ans Communication Technology, Springer Science and Business Media, ISBN, 2009.

[2] S. Pankanti, R. M. Bolle, and A. K. Jain., « Biometrics: The Future of Identification », IEEE Computer, 2000.

[3] A. K. Jain, P. Flynn and A. A. Ross, « Handbook of biometric », Springer Science and Business Media, ISBN, 2008.

[4] Abdallah Meraoumia, Salim Chitroub and ahmed Bouridane., « Multimodal Biometric Person Recognition System based on Iris and Palmprint Using Correlation Filter Classifier », International Conference On Computing And Information Technology-ICCIT 2012, Al Madinah, Saudi Arabia, March 12-14, 2012.

[5] Peter Gregory and Michel A.Simon, « Biometrics For Dummies », Cisa, Cissp, 2008.

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

[7] N.V.Boulgouris, K. N. Plataniotis and E. Micheli-Tzanakou, « Biometrics: Theory, Methods, and Applications », David B. Fogel, Series Editor, Willy publisher, IEEE Press on Computational Intelligence, 2010.

[8] Son, B., Ahn, J.-H., Park, J.-h., Lee, Y., « Identification Of Humans Using Robust BiometricFeatures », Lecture Notes in Computer Science, 2004.

[9] A. Kumar, D. Wong, H. Shen, and A.Jain, "Personal verification using palmprint and hand geometry biometric", Audio and Video based biometric Person Authentification, LNCS 1688, 2003.

[10] Maltoni Davide, Dario Maio, Anil K. Jain, Salil Prabhakar, « Handbook of fingerprint recognition », Springer, New York, 2003.

[11] Rui Zhao, Kunlun Li, Ming Liu, Xue Sun, « A Novel Approach of Personal Identification Based on Single Knuckle-print Image », Asia-Pacific Conference on Information Processing-APCIP, 2009.

[12] Cardinaux F, Sanderson C, Bengio S, « Face verification using adapted generative models », The 6th IEEE International Conference Automatic Face and Gesture Recognition-AFGR, Seoul, 2004.

[13] Julian Ashbourn, « Guide To Biometrics For Large-Scale Systems », Springer 2011.

[14] C.Tisse, L.Martin, L. Torres and M. Robert, « Person identification technique using human iris recognition », Proc. Of Vision Interface, 2002.

[15] Jain, A. K., Griess, F.D. and Connell, S.D, « On-line signature verification », Pattern Recognition, 2002.

[16] Suman Senapati, Goutam Saha, « Speaker Identification by Joint Statistical Charactcterization in the Log-Gabor Wavelet Domain », Inernational Journal of Intelligent Systems and Technologies, winter, 2007.

[17] Qiuhong Yu, Yilong Yin, Gongping Yang, Yanbin Ning, Yanan Li, « Face and Gait Recognition Based on Semi-supervised Learning », The 5th Chinese Conference on Pattern Recognition CCPR2012, BeiJing, China, Sep. 24-26, 2012.

[18] Ying Zhang, Guiran Chang, Lin Liu, JieJia, « Authetificating User's Keystroke Based on Statistical Models », Fourth International Conference on Genetic and Evolutionary Computing, Shenzhen, China, Dec 2010.

[19] C.M.Most, « Towards privacy enhancing applications of biometrics », Digital ID World. Magazine, Issue 11, June/ July 2004.

[20] Florent Perronnin, Jean-Luc Dugelay, « Inroduction à la biométrie : Authetification des individus par traitement audio-vidéo », Institut Eurocom, Multimedia Communications Department, Revue Traitement du signal, 2002.

[21] S. Liu, M. Silveman, « A pratical Guide to Biometric Security Technology », IEEE Computer Society, IT Pro-Security, Janvier-Février 2001.

[22] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, « Handbook of Fingerprint Recognition », Second Edition, Springer, 2009.

[23] A. K. Jain, L. Hong, and S. Pankanti, « Biometric Identification », Comm, ACM, February 2000.

[24] J.Ruiz-del-Solar, C.Devia, P. Loncomilla and F. Concha, « Offine signature very cation using local interest points and descriptors », Progress in Pattern Recognition, Image Analysis and applications, Lecture Notes in Computer Sciences, 2008.

[25] F. Perronnin and J.-L. Dugelay. "Introduction à la biométrie Authentification des individus par traitement audio-vidéo". Traitement du signal, 2002.

[26] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior. "The Relation between the ROC Curve and the CMC". In : Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies, 2005.

[27] Jain A.K, Dass S.C and Nandakumar K, « Can soft biometric traits assist user recognition? », Procedings of SPIE International symposium on defense and security: Biometric technology for human identification, 2004.

[28] K. Nanda kumar, A. Ross, and A. K. Jain, « Biometric Fusion: Does Modeling Correlation Really Matter? », The 3rd Int`l Conf. on Biometrics: Theory, Applications and Systems, Washington DC, Sept. 2009.

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

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

[31] Thèse-Mohamad-ElAbed-« Evaluation de systèmes biométriques » 2011.

[32] Merouane Asmaa « Identification biométrique par les veines dorsales de la main » 2013.

[33] A.A. Ross, A. K. Jain and K. Nandakumar, « Levels of fusion in Biometrics », Handbook of Multibiometrics, Springer, US, 2006.
[34] La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées Par Melle Lorène ALLANO 2009.
[35] Modèles acoustiques à structure temporelle renforcée pour la vérification du locuteur embarquée. Par Anthony LARCHER.
[36] Article A. Ross and A. Jain. " Information fusion in biometrics ". Pattern Recognition.
[37] Nirosha Joshitha J, R. Medona Selin, « Image Fusion using PCA in Multifeature Based Palmprint Recognition », International Journal of Soft Computing and Engineering-IJSCE, May 2012.
[38] Salim Chitroub, \Classifier combination and score level fusion: concepts and practical aspects", International Journal of Image and Data Fusion, 2010.
[39] Shekhar Karanwal, Davendra Kumar and Rohit Maurya, "Fusion of Fingerprint and Face by using DWT and SIFT", International Journal of Computer Application, Jun 2010.
[40] Flitti F, Collet C, Slezak E, "Image fusion based on pyramidal multiband multiresolution markovian analysis", Signal, Image And Video Processing, 2009.
[41] Othaila Chergui, Abdallah Meraoumia, Hakim Bendjenna, Salim Chitroub, " Robust Multimodal Personal Identification System Using Palmprint & Palm-vein Images" , International Conference on Information Technology for Organization Development, Octobre 2014.
[42] Abdallah Meraoumia, Salim Chitroub and ahmed Bouridane, "An Efficient Hand-Based Biometric Recognition System Using Finger-Knuckle-Print Data", Recent Patents on Telecommuni- cation, Bentham Science Publishers, 2012.
[43] Lin Zhang, Lei Zhang, David Zhang and Hailong Zhu, "Ensemble of local and global information for finger-knuckle-print recognition", Pattern Recognition, 2011.
[44] Zhu Le-qing and Zhang San-yuan, \Multimodal biometric identi_cation system based on finger geometry, knuckle print and palmprint", Pattern Recognition Letters, 2010.