REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

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

MEMOIRE MASTER ACADEMIQUE

Domaine : Science et Techniques.
Filière : Électronique.
Spécialité : Automatique.

Présenté par :

Abdelatif GHACHOUA
Ibrahim KAHLAOUI

THÈME

Reconnaissance de personnes en utilisant L'empreintes Palmaires multispectral basés sur L'apprentissage approfondi

Soutenu publiquement
Le :25/05/2016

Devant le jury :

Mr.	Fatah HAMMOUCHI	MAA	Président	UKM Ouargla
Mr.	Mourad CHAÂ	MAA	Examinateur	UKM Ouargla
Mr.	Abdallah MERAOUMIA	MCB	Encadreur	U.TEBESSA
Mr.	Maarouf KORICHI	Doctorant	Co-Encadreur	UKM Ouargla

Année Universitaire: 2016/2017

Remerciements

J'ai l'honneur d'être dirigé par mon Professeur ***Mr. Abdellah MERAOUMIA***, ***Mr. Djamel SAMAI*** et ***Mr. Maarouf KORICHI*** dans la présente recherche. Je vous remercie énormément mon professeur pour avoir encadré et suivi ce travail.

Merci beaucoup pour votre disponibilité, pour les nombreuses et intéressantes discussions scientifiques, pour les remarques et orientations constructives, pour les nombreux conseils avisés, pour vos encouragements quotidiens, pour ne pas avoir cessé, pour le soutien permanent, pour votre compréhension, pour la confiance que vous avez accordée et qu'il a toujours témoignée à mon égard, pour votre écoute et tout simplement pour votre gentillesse.

Sans oublier ***Mr. Bensid Khaled,*** merci beaucoup pour que vous êtes encouragés et vous êtes aidés. Je tiens à exprimer tout au fond de mon cœur mes reconnaissances à département d'électronique et télécommunication pour toutes les années de spécialité et ce que je pris de la science et de la connaissance.

Remercie également monsieur le directeur du centre de recherche Mr.***Ghilani Nacer***, ce qui nous a donné l'occasion à la recherche et l'accomplir de ce travail.

Dédicace

JE DÉDIE CE MODESTE TRAVAIL

A MES CHÈRES PARENTES : MA MÈRE (DALILA) ET MON PÈRE (AZZEDINE).

A MES TRÈS BEAUX FRÈRES : SOUFIENE ET SALAH

A MES TRÈS BELLES SŒURS : MANEL ET SARA

A MES TRÈS PETITS CHERS : HOUSSAM ET NOR ALYAKINE

A TOUTE MA FAMILLE KAHLAOUI EST SURTOUT À MA GRAND-MÈRE

A TOUS MES AMIES

SANS OUBLIER TOUS LES ENSEIGNANTS ET LES PROFESSEURS QUI M'ONT ORIENTÉ DURANT TOUTE MA CARRIÈRE D'ÉTUDE.

KAHLAOUI BRAHIM.

Dédicace

JE DÉDIE CE MODESTE TRAVAIL

A MES CHÈRES PARENTES : MA MÈRE (SAADIA) ET

MON PÈRE (AMOR).

A TOUTE MA FAMILLE GHACHOUA EST SURTOUT À

MA GRAND-MÈRE

A TOUS MES AMIES

SANS OUBLIER TOUS LES ENSEIGNANTS ET LES

PROFESSEURS QUI M'ONT ORIENTÉ DURANT TOUTE

MA CARRIÈRE D'ÉTUDE.

GHACHOUA ABD ELATIF.

Table Des Matières

Page

Liste des tableaux

Liste des figures

Abréviations

ADN : Acide Désoxyribose Nucléique

CMC : Cumulative Match Curve

DBN : Réseau Deep Belief

EER : Equal Error Rate

FAR : False Acceptation Rate

FRR : False Rejection Rate

NIR : Near Infra-Red

NG : Niveau de gris

PLM : Palm print

RGB : Red Green Blue

ROC : Receiver Operating Characteristic

ROR : Rank One Recognition

RBM : Machine de Boltzmann Restreinte

Introduction Générale

Introduction générale

Durant tout le XX siècle, le mot « biométrie » a été utilisé quasi exclusivement dans le sens très large de « étude quantitative des êtres vivants », notamment à l'aide des méthodes statistiques. C'est dans cette optique que la revue Biométrique paraît depuis 1901 et que Société internationale de Biométrie (The International Biométrique Society) a été fondée en 1947.

La reconnaissance des individus a connu plus d'importance dans la vie humaine quotidienne. Elle assure les transactions des personnes en différant domaines afin d'assurer une sécurité pertinente. Dans les dernières années, la pratique des systèmes de reconnaissance reste limitée aux grands secteurs tels que le secteur militaire et d'autres secteurs nécessitant de nombreuses applications telles que la protection de l'accès à un ordinateur, un téléphone portable, une clé USB, un établissement, des cartes bancaires.... De nombreuses technologies biométriques ont été développées, toutes basées sur les identificateurs biométriques physiologiques et comportementales telles que : l'iris, la voix, les empreintes digitales, le visage, la signature.... Ces derniers sont plus fiables que les systèmes classiques (clé, mot de passe. . .) dans la reconnaissance d'une personne car ils sont difficilement falsifiables. C'est la raison pour laquelle les systèmes biométriques sont actuellement de plus en plus sollicités.

La reconnaissance d'empreintes palmaire dans le cas usuel, civil ou commercial, n'est autre qu'un processus de comparaison de deux images d'empreintes complètes de qualité contrôlée. La nature de l'empreinte palmaire similaire à celle digitale a incité les chercheurs à exploiter les concepts et les approches conçues pour la reconnaissance digitale.

Dans cette étude, on a choisi un système de reconnaissance par les empreintes palmaires. Ce système utilise la forme de la partie intérieure de la main pour extraction des caractéristiques biométriques d'identification des individus. Ces caractéristiques sont permanentes et stables durant toute la vie, aussi uniques pour chacun. Ce travail a pour objectif la réalisation des systèmes biométriques uni-modal et multimodal basés sur les méthodes : RBM et DBM appliquées sur des vecteurs binaires issues d'un filtre Log-Gabor.

Notre travail est articulé sur trois chapitres :

- **Le premier chapitre :** Dans ce chapitre, nous allons suivre l'évolution de la reconnaissance biométrique dans « aperçu de la biométrie », mettre le point sur le concept et les bases de la

reconnaissance automatique ainsi que sur les différentes modalités dans les « Généralité sur la biométrie ». Une étude détaillée d'un système biométrique sera dressée dans « Le système biométrique » et ses domaines d'application.

➢ **Le deuxième chapitre :** Est consacré à la fusion multimodale. Dans ce chapitre plusieurs notions sur la façon d'utiliser et de combiner plusieurs modalités ont été abordées. Notre contribution à l'extraction de caractéristiques est également présentée dans ce chapitre. Dans cette contribution, des notions sur les deux techniques RBM et DBN, ainsi que la façon de les appliqués pour extraire les caractéristiques discriminantes sont présentés.

➢ **Le troisième chapitre :** Est consacré pour les résultats expérimentaux. Dans la première section de ce chapitre, nous avons mis en œuvre un système d'identification uni-modale basé à chaque fois sur empreintes palmaires. Une description détaillée des résultats obtenus, par les algorithmes filtre log-Gabor, est présentée dans cette section. La deuxième section de ce chapitre discute les résultats expérimentaux obtenus pour les systèmes biométriques multimodaux. Trois scenarios de fusion, à savoir le système le système multi algorithmique et Système Multi-échantillons et le système hybride ont été évalués. Afin de sélectionner le meilleur système, qui présente la plus faible erreur d'identification, une comparaison entre les différents systèmes est exécutée dans cette section. Ensuite, nous avons essayé les quatre règles et compare entre les quatre règles de fusion des scores Enfin, nous avons terminé notre mémoire avec une conclusion et quelques perspectives visées.

CHAPITRE I

SÉCURITE ET BIOMÉTRIE

I.1 Préambule

Les systèmes biométriques sont de plus en plus utilisés depuis quelques années L'apparition de l'ordinateur et sa capacité à traiter et à stocker les données ont permis la création des systèmes biométrie informatisés. Il existe plusieurs caractéristiques physiques uniques pour individu, ce qui explique la diversité des systèmes appliquant la biométrie [1].

C'est quoi la biométrie ?

Il existe trois possibilités pour prouver son identité :

- Ce que l'on possède (carte, badge, document).
- Ce que l'on sait (un nom, un mot de passe).
- Ce que l'on est (empreintes digitales, main, visage...)'' Il s'agit de la biométrie''.

La biométrie permet l'identification ou l'authentification d'une personne sur la base de données reconnaissable et vérifiable qui lui est propre [1].

I.2 la biométrie

I.2.1 Définition

La biométrie peut être définie comme étant "la reconnaissance automatique d'une personne en utilisant des traits distinctifs". Une autre définition de la biométrie est ''toutes caractéristiques physiques ou traits personnels automatiquement mesurables, robustes et prétendue d'un individu. La biométrie consiste en l'analyse mathématique des caractéristiques biologique d'une personne et a pour objectif de déterminer son identité de manière irréfutable. Contrairement à ce que l'on sait ou ce que l'on possède la biométrie est basée sur ce que l'on est et permet ainsi d'éviter la duplication, le vol, l'oubli ou perte [2].

I.2.2 Caractéristiques biométriques

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en trois catégories : biométrie biologique, comportementale et morphologique. Pratiquement, n'importe quelle caractéristiq$ue morphologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle satisfait les propriétés suivantes :

- ***Universalité :*** toutes les personnes à identifier doivent la posséder.
- ***Unicité :*** l'information doit être aussi dissimilaire que possible entre les déférentes personnes.
- ***Collectabilité :*** l'information doit être collectable et mesurable afin d'être utilisée Pour les comparaisons.
- ***Permanence :*** l'information collectée doit être présente pendant toute la vie d'un individu**.**
- ***Acceptabilité :*** le système doit respecter certains critères (facilité d'acquisition, rapidité…etc.) afin d'être employés.

I.3 La marche mondiale de la biométrie

Régulièrement, un rapport sur le marché de la biométrie est édité par IBG (Internationale Biométrie Group). Cette étude est une analyse complète des chiffres d'affaires, des tendances de croissance, et des développements industriels pour le marché de la biométrie actuel et futur.

La lecture de ce rapport est essentielle pour des établissements déployant la technologie biométrique, les investisseurs dans l'entreprise biométrique, ou les développeurs de solution biométrique. Le chiffre d'affaires de l'industrie biométrique incluant les applications judiciaires et celles du secteur public, se développe rapidement. Une grande partie de croissance sera attribuable au contrôle d'accès aux systèmes d'information (ordinateur/réseau) et au commerce électronique, bien que les applications du secteur public continuent à être une partie essentielle de l'industrie.

On prévoit que le chiffre d'affaires des marchés émergents (accès aux systèmes d'information, commerce électronique et téléphonie, accès physique et surveillance) dépasse le chiffre d'affaires des secteurs plus mateur (identification criminelle et identification des citoyens) [3].

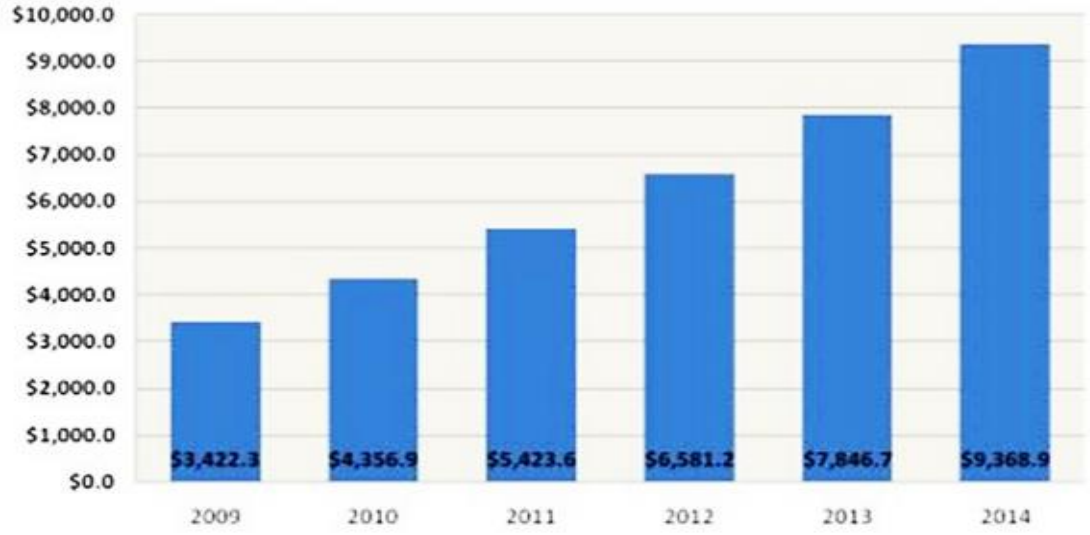

Figure I.01 : *Evolution du marché international de la biométrie*

I.4 Les parts de marché par technologie

Les empreintes digitales continuent à être la principale technologie biométrique en termes de part de marché, près de 50%du chiffre d'affaires total (hors application judiciaires). La reconnaissance du visage, avec 12%du marché (hors application judicaires), dépasse la reconnaissance de la main, qui avait avant la deuxième place en termes de source de revenus après les empreintes digitales [3].

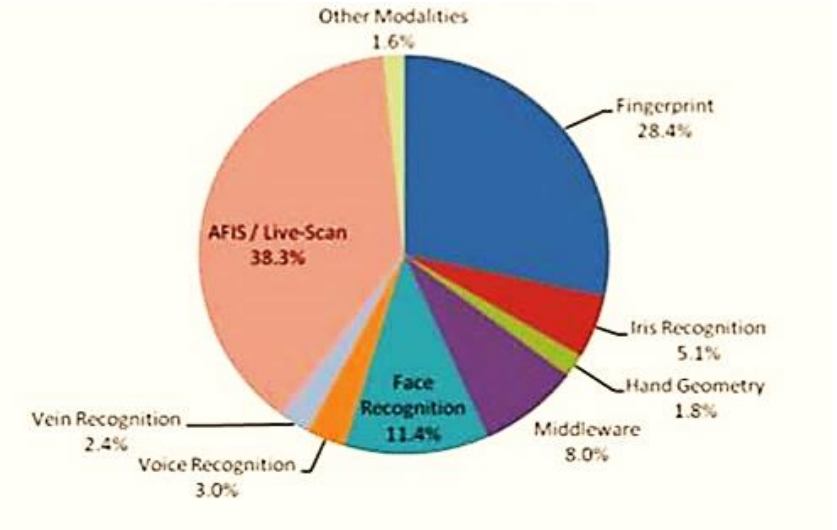

Figure I.02 : *Parts de marché des différentes méthodes biométrique*

I.5 Comment choisir un moyen biométrique ?

Plutôt que de comparer les performances des diverses technologies (empreintes, visage, main…), il faut surtout tenir compte de l'environnement de leur usage, (facilité de : saisie,

d'analyse, de stockage, de vérification). Chaque technologie possédant des avantages et des inconvénients, acceptables ou inacceptables suivant les applications. Ces solutions ne sont pas concurrentes, elles n'offrent ni les mêmes niveaux de sécurité ni les mêmes facilités d'emploi. En comparaison aux systèmes d'authentification utilisant un objet ou un mot de passe, qui offrent une réponse stable (oui ou non, 0% ou 100%) ; les informations biométriques sont plus fluctuantes et donnent des réponses en termes de pourcentage de similitude (entre 0% et 100%, le 100% n'étant jamais atteint). Cette variation des résultats d'identification d'un individu est plus liée à la qualité de la capture de l'information biométrique (on n'a jamais deux images ou deux sons identiques), qu'à la modification de la caractéristique biométrique de l'individu qui est généralement stable dans le temps. Il faut donc définir un seuil de décision (acceptation ou refus) compris entre 0% et 100% de similitude au sein d'application. Ce seuil peut être différent pour chaque personne [4].

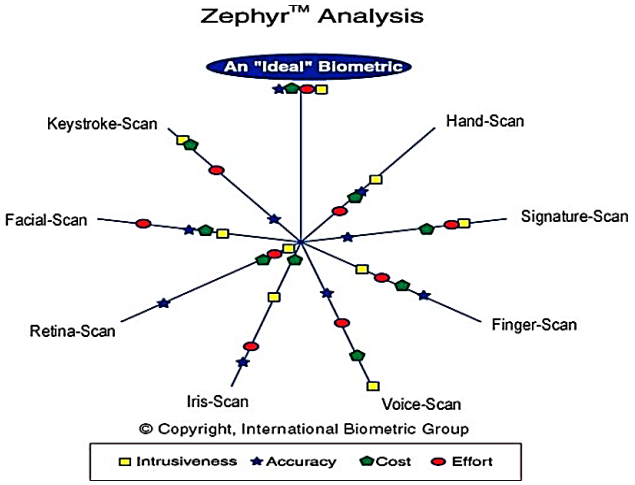

Figure I.03 : *Méthodes de Reconnaissances Biométriques*

- Intrusiveness : niveau de perception par l'utilisateur du test comme intrusif.
- Cost : coût de la technologie (lecteurs, capteurs, etc.…).
- Accuracy : efficacité de la méthode (capacité à identifier quelqu'un).

I.6 Techniques biométriques

Il existe plusieurs techniques biométriques utilisées dans plusieurs application et secteurs, on peut en distinguer trois catégories :

I.6.1 Analyse morphologique (physiologique)

Elle est basée sur l'identification de traits physique particuliers qui, pour toute personne, sont unique et permanents. Cette catégorie regroupe l'iris de l'œil, le réseau veineux de la rétine la forme de la main, les empreintes digitales, les traits du visage, les veines de la main, etc…

✓ **Empreint digitale :** La reconnaissance des empreintes digitales est la technique biométrique la plus utilisée. Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers et constituent un motif unique, universel et permanant. Les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Ces éléments sont appelés minuties. Il existe plusieurs types de minuties : lac, bifurcation, delta ou impasse…etc. Ce type de technique biométrique est utilisé par les institutions financières pour leurs clients et se trouve en même temps dans les hôpitaux, les écoles, les aéroports…etc. [5].

Figure I.04 : *Empreinte digitale*

Avantages	Inconvénients
• La technologie la plus éprouvée techniquement et la plus connue du grand public. • Petite taille du lecteur facilitant son intégration dans la majorité des applications (téléphones portables, PC). • Faible coût des lecteurs grâce aux • Nouveaux capteurs de type "Chip silicium". • Traitement rapide • Bon compromis entre le taux de faux rejet et le taux de fausse acceptation.	• Image "policière" des empreintes digitales. • Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur). • Certains systèmes peuvent accepter un moulage de doigt ou un doigt coupé (la détection du doigt vivant permet d'éviter ce type d'usurpation).

✓ **Visage :** Nos visages sont des objets complexes avec des traits qui peuvent varier dans le temps. Cependant, les humains ont une capacité naturelle à reconnaitre les visages et d'identifier les personnes dans un coup d'œil. Bien sûr, notre capacité de reconnaissance naturelle n'étend au-delà de la reconnaissance du visage, où nous somme également en mesure de repérer rapidement des objets, des sons ou des odeurs. Malheureusement, cette aptitude naturelle n'existe pas dans les ordinateurs, c'est ainsi qu'est né le besoin de simuler artificiellement la reconnaissance afin de créer des systèmes intelligents autonomes simuler notre capacité naturellement. La reconnaissance des visages dans les machines est une tâche difficile mais pas impossible. Tout au long de notre vie, de nombreux visages sont vus et conservés naturellement dans nos mémoires formant une sorte de base de données. La reconnaissance du visage est utilisée comme un système de surveillance ou d'identification par les autorités ou les corps policiers principalement dans les lieux publics. Elle est parmi les techniques les plus acceptables, mais elle nécessite un arrière- plan simple et fixe pour que le résultat soit précis [6].

Figure I.05 : *visage*

Avantages	Inconvénients
• Très bien accepté par le public • Ne demande aucune action de l'usager (peu intrusive), pas de contact physique • Technique peu coûteuse	• Technologie sensible à l'environnement (éclairage, position, expression du visage...) • Les vrais jumeaux ne sont pas différenciés • Sensible aux changements (barbe, moustache, lunette, piercing, chirurgie...)

✓ **Iris :** L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'œil, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. La reconnaissance de l'iris est développée dans les années 80 c'est pour cela elle est une technologie plus récente. L'image de l'iris est capturée par un appareil qui contient une caméra infrarouge, lorsque la personne se place à une courte distance de l'appareil [6].

Figure I.06 : *Image de l'iris*

Avantages	Inconvénients
• Grande quantité d'information contenue dans l'iris • Vrais jumeaux non confondus	• Aspect psychologiquement invasif de la méthode • L'iris est aisément visible et peut être photographié. Le problème de sécurité est alors lié aux vérifications effectuées lors de la prise de vue. (Problème identique pour les empreintes, la voix, l'oreille, ... Mais moins pour la rétine)

✓ **Empreintes des articulations des doigts (FKP) :** C'est la technologie biométrique basée sur la surface arrière de doigt, elle contient des caractéristiques distinctives, telles que les lignes principales, les lignes secondaires et les crêtes, qui peuvent être extraites à partir des images à basse résolution. La main contient plusieurs doigts, pour cela, il faut conserver les informations à chaque doigt pour une reconnaissance précise dans le domaine d'identification [7].

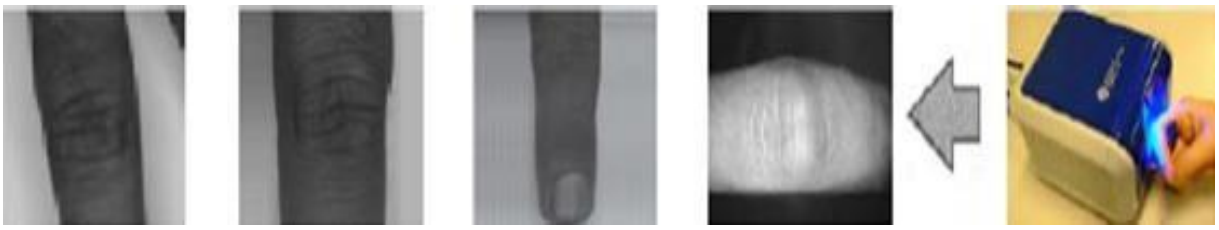

Figure I.07 : *Empreinte des articulations des doigts*

Avantages	Inconvénients
• Technique acceptable. • Utilisation simple. • En combinant tous les doigts de la main, il est possible d'établir un système biométrique robuste et précise.	• Très similaire pour les jumeaux. • Problème dans le cas de couper un doigt. • Pose incorrecte de doigt sur le lecteur provoque une grande erreur

✓ **Empreinte palmaire :** Cette technique utilise la surface intérieure de la paume pour l'identification et/ou la vérification des personnes. Elle est bien adaptée pour les systèmes de moyenne sécurité telle que le contrôle d'accès physique ou logique [7].

Figure 08 : *Empreinte palmaire*

Avantages	Inconvénients
• Facile à utiliser, Il a une grande acceptation. • Après l'utilisation, la main resté propre et ne laisser aucune trace. • Presque disponible par tous les individus.	• Pourrait être similaire dans des jumeaux ou des membres de la famille. • Il n'est pas permanent en termes de changements tels que le vieillissement.

I.6.2 L'analyse comportementale

Elle se passé sur l'analyse de certains comportements d'une personne. Cette catégorie regroupe la reconnaissance vocale, la dynamique de frappe de clavier, la dynamique de signature, l'analyse de la démarche, etc. Il existe, par ailleurs, une autre catégorie qui est l'étude des traces biométrique telles que : l'ADN, le sang, la salive, l'urine, l'odeur

✓ **Voix :** La voix humaine varie d'une personne à l'autre et peut se constituer de composantes physiologiques et comportementales. L'identification par la voix basée sur la forme et la taille des appendices (bouche, cavités nasales et les lèvres) utilisées dans la synthèse du son. La reconnaissance des locuteurs est plis utilisés par les téléphones, les corps policiers, les hôpitaux…etc [6].

Figure I.09 : *Signal de voix*

Avantages	Inconvénients
• Il est plus facile de protéger le lecteur que dans les autres technologies • Seule information utilisable via le téléphone • Impossible d'imiter la voix • Pas intrusif	• Sensible à l'état physique et émotionnel de l'individu • Fraude possible par enregistrement • Sensible aux bruits ambiants • Taux de faux rejet et fausse acceptation élevés

✓ **Signature manuscrite :** C'est une écriture personnelle d'un individu, la vérification de la signature est basée sur deux modes :

- Mode statique : la vérification de la signature statique met l'accent sur les formes géométriques de la signature, dans ce mode en générale la signature est normalisée à une taille connue ensuite décomposer en élément simple.
- Mode dynamique : il utilise les caractéristiques dynamiques telles que l'accélération, la vitesse et les profils de trajectoire de la signature [8].

Figure I.10 : *Signature manuscrite.*

Avantages	Inconvénients
• La signature écrite sur un document peut être conservée des certains documents • Action qui implique (responsabilité) le demandeur	• Besoin d'une tablette graphique • Sensible aux émotions de l'individu • Pas utilisable pour du contrôle d'accès en extérieur par exemple

✓ **Frappe dynamique sur le clavier :** C'est un système de reconnaissance d'un individu basé sur la manière de ses écritures par un dispositif logicielle qui calcule la vitesse de frappe, la suite des lettres, le temps de frappe et la pause entre chaque mot.

Figure I.11 : *Frappe dynamique sur le clavier*

Avantages	Inconvénients
• Non intrusif, geste naturel pour un individu	• Dépend de l'état (physique, émotion, fatigue...)

✓ **Démarche :** Chaque personne a une façon particulière de marche, nous pouvons identifier les individus de la nature du mouvement des jambes, des bras et des articulations ou le mouvement spécial obtenus par un caméra vidéo afin de l'envoyer à un ordinateur pour l'analyse afin de déterminer la vitesse et l'accélération de chaque individu [8].

Figure I.12 : *Démarche*

Avantages	Inconvénients
• Très acceptable par les individus.	• N'est pas permanant (âge, fatigue, maladie)

I.6.3 Biométrie biologique

✓ **Veines de la main :** Les veines de la main sont du réseau ne varient de personne à l'autre. L'analyse de cette différence permet de maintenir des points pour différencié une personne à l'autre [9].

Figure I.13 : *Veines de la main*

Avantages	Inconvénients
• Ne nécessite pas de contact. • Difficile à falsifier.	• Très cher

✓ **Analyse de l'ADN :** Il est la façon la plus précise pour déterminer l'identité de la personne. Il est impossible de trouver deux personnes qui ont le même ADN. Cette modalité possède l'avantage d'être unique et permanant durant toute la durée de vie [9].

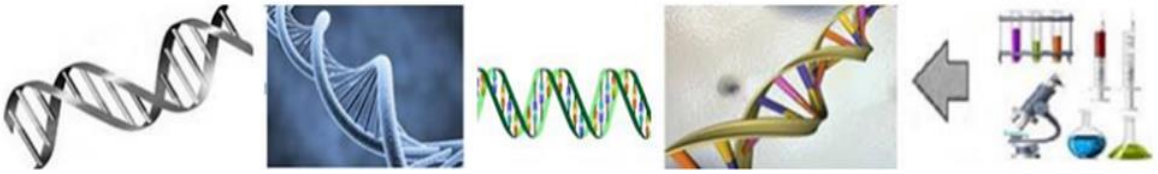

Figure I.14 : *Exemple de l'ADN*

Avantages	Inconvénients
• Distinguer les individus avec une grande précision • Il facilite la détection des délinquants	• Lente pour obtenir les résultats • Avoir un coût élevé

✓ **Thermo gramme faciale :** La quantité de chaleur émise par les différentes parties du visage caractérise chaque individu. Elle dépend de la localisation des veines mais aussi de l'épaisseur du squelette, la quantité de tissus, de muscles, de graisses, etc. contrairement à la reconnaissance de visage, la chirurgie plastique n'a que peu d'influence sur les thermo grammes faciaux. Pour capturer l'image, il est possible d'utiliser un appareil photo ou une caméra numérique dans le domaine de l'infrarouge. La capture peut se faire dans n'importe quelle condition d'éclairage et même dans le noir complet ce qui est un avantage supplémentaire sur la reconnaissance de visage classique [10].

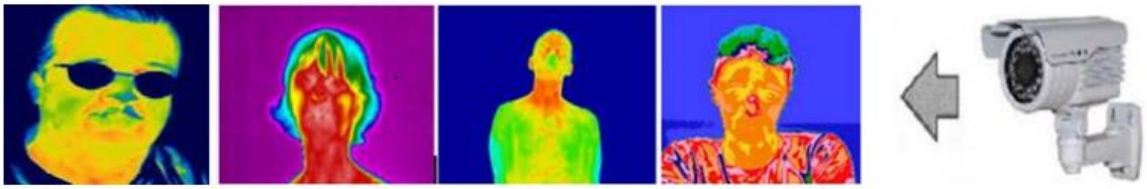

Figure I.15 : *Thermo gramme faciale*

Les cheveux et les poils : Rudolf Virchow, médecin et anthropologue allemand, étudia pour la première fois en 1869 des poils humains. En 1910, V. Balthazar, professeur de médecine à la Sorbonne, et M. Lambert publièrent la première étude approfondie. En effet, l'examen de cheveux ou de poils permet d'identifier certaines caractéristiques propres à chaque individu, et d'apporter des éléments d'identification intéressants [10].

I.6.4 Les autres techniques

Comme l'iris, le visage ou la voix, d'autres techniques ont été développées ces 20 dernières années dans le but spécifique d'effectuer l'authentification ou l'identification d'une personne. Ces recherches ont permis de mettre sur le marché des dispositifs de reconnaissance de la rétine, de la signature, ou encore de la dynamique de frappe au clavier. Mais d'autres champs restent à explorer et certaines de nos caractéristiques sont encore à l'étude dans divers laboratoires. Parmi les systèmes à l'étude, on peut citer : la géométrie de l'oreille (Ce principe peut être parfois utilisé par la police pour identifier un individu à partir d'une photo prise sur le lieu d'un délit), la démarche, la denture, le dessin des lèvres, l'odeur corporelle, les battements du cœur, l'analyse des pores de la peau, la salive, l'irrigation sanguine et bien d'autres. Les recherches dans le domaine de la biométrie ne sont donc pas encore terminées. Toutefois, il est encore trop difficile de leur prédire lesquelles de ces technologies auront un usage industriel. Les autres techniques Comme l'iris, le visage ou la voix, d'autres techniques ont été développées ces 20 dernières années dans le but spécifique d'effectuer l'authentification ou l'identification d'une personne. Ces recherches ont permis de mettre sur le marché des dispositifs de reconnaissance de la rétine, de la signature, ou encore de la dynamique de frappe au clavier. Mais d'autres champs restent à explorer et certaines de nos caractéristiques sont encore à l'étude dans divers laboratoires. Parmi les systèmes à l'étude, on peut citer : la géométrie de l'oreille (Ce principe peut être parfois utilisé par la police pour identifier un individu à partir d'une photo prise sur le lieu d'un délit), la démarche, la denture, le dessin des lèvres, l'odeur corporelle, les battements du cœur, l'analyse des pores de la peau, la salive, l'irrigation sanguine et bien d'autres. Les recherches dans le domaine de la biométrie ne sont

donc pas encore terminées. Toutefois, il est encore trop difficile de leur prédire lesquelles de ces technologies auront un usage industriel [11].

I.7 Architecture d'un système biométrique

Dans ces jours les systèmes biométriques sont de plus en plus utilisés aux dernières années. En général, un système de reconnaissance des personnes basé sur leurs descripteurs biométriques peut se décomposer en deux phases, phase d'enrôlement (création de la base de données) et phase de reconnaissance [5] (voir **Figure 16**)

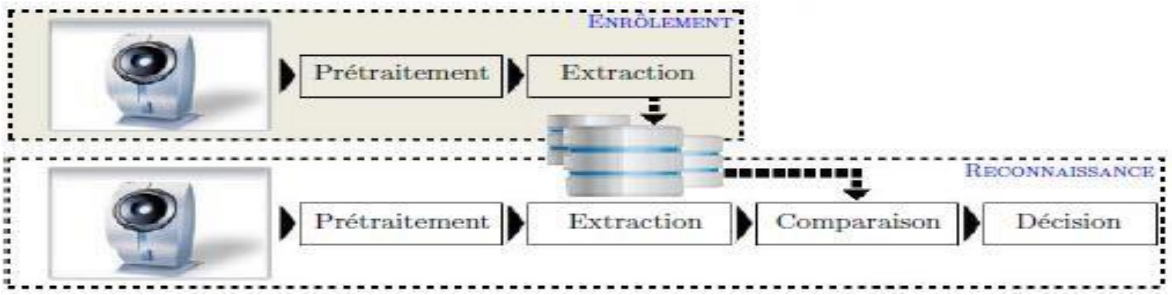

Figure I.16 : *Système biométrique*

I.7.1 Fonctionnement

Chaque système biométrique comprend deux phases distinctes :

1) Phase d'enrôlement : La phase d'enrôlement est définie par le procédé de la collection de traits biométriques d'un individu et le convertir en référence biométrique (Template, vecteur de caractéristique), et à la stocker dans une base de données pour une comparaison ultérieure.

2) Phase de reconnaissance : Au cours de la reconnaissance, la modalité biométrique est mesurée et un ensemble des caractéristiques distinctives (Template) est extrait comme lors de l'enrôlement [1]. Cette phase peut être décomposée en deux modes :

- ***Mode vérification€*** : le système doit répondre à une question de type : « Suis-je bien la personne que je prétends être ?». L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de données (type ***1:1***). En mode vérification, on parle de problème ouvert puisque l'on suppose qu'un individu qui n'a pas de modèle dans la base de données (imposteur) peut chercher à être reconnu. [12]

- ***Mode identification***, le système doit deviner l'identité de la personne. Il répond donc à une question de type : « Qui suis-je ?». Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données (type ***1 : N***). En général, lorsque

l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que toute personne qui utilise le système possède un modèle dans la base de données

i. ***Identification en mode ensemble fermé :*** Par exemple on utilise. Ce type d'identification afin d'enregistrer la présence de personnes dans certaine entreprise. Si l'échantillon possède un certain degré de similitude avec les échantillons dans le système, la personne sera acceptée.

ii. ***Identisation en mode ensemble ouvert :*** S'il y a une grande similitude entre l'échantillon biométrique testé et tous les modèles préenregistrés et si cette similitude est inférieure (ou supérieure) au seuil de sécurité, cette personne est rejetée. Cela signifie que la personne ne fait pas partie de celles enregistrées par le système. Sinon le système est l'acceptée.

I.7.2. Principaux Modules

Le système biométrique est un système pour identifier les tendances et le stockage des données à sauvegarder ou de les identifier dans la forme de matrices. Ensuite, le système est prêt à identifier les intrus. Ce système se compose de quatre unités : l'acquisition, l'extraction des caractéristiques, la comparaison (mesure de similarité) et la décision. L'inscription ou l'enrôlement est utilisé pour une future comparaison tandis que la décision est de reconnaître la personne ou non [13].

➢ **Acquisition des données :** Cette phase collecte les données biométriques des personnes clients. Plusieurs processus industriels peuvent être utilisés pour l'acquisition telle qu'un appareil photo, un lecteur d'empreintes digitales, etc.

➢ **Extraction des caractéristiques :** Les images sont traitées pour en extraire des caractéristiques du procédé. Ce processus sert à éviter les informations inutiles qui existent. Donc, ce module sert à traiter l'image afin d'extraire uniquement les caractéristiques biométriques, sous forme d'un vecteur ou Template, qui ensuite peuvent être utilisées pour reconnaitre les personnes. Ces caractéristiques sont uniques à chaque personne et stable.

➢ **Comparaison :** Dans ce module, les caractéristiques biométriques extraites sont comparées avec un vecteur précédemment stocké dans la base de données et en marquant le degré de similitude (différence ou distance).

➢ **Décision :** Vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) vecteur(s) stocké(s).

I.8 Système en linge et système hors linges

Les systèmes de reconnaissance biométriques sont classifiés en deux catégories (reconnaissance en ligne et reconnaissance hors ligne).

I.8.1 Système en ligne

Dans ce type des systèmes, les images de modalité sont capturées par un dispositif de capture spécifique et les images numériques acquises sont traitées en temps réel.

I.8.2 Système hors ligne

Ce type des systèmes traite les images de chaque modalité capturée précédemment par un scanner numérique. Ces approches fournissent des images à haute résolution, mais ne sont pas convenables aux systèmes de sécurité en temps réel [14].

I.9 Évaluation d'une performance

La performance d'un système d'identification biométrique peut se mesurer principalement à l'aide de trois critères : sa précision, son efficacité (vitesse d'exécution) et le volume de données qui doit être stocké pour chaque personne. Nous nous concentrerons dans cette section sur le premier aspect. Comme nous l'avons vu précédemment, l'identification et la vérification sont des modes opératoires différents. Elles nécessitent donc des mesures de précision différentes que nous étudierons dans les deux sous-sections suivantes.

Taux d'erreurs : Lorsqu'un système en mode d'identification ensemble ouvert, il existe deux types d'erreur qui peuvent être utilisés pour évaluer leur performance. La première erreur mesure le taux de faux rejet (False Rejection Rate ou FRR) et la deuxième erreur mesure le taux d'acceptation des imposteurs, on parle alors à la fausse acceptation (False Acceptance Rate ou FAR) [15].

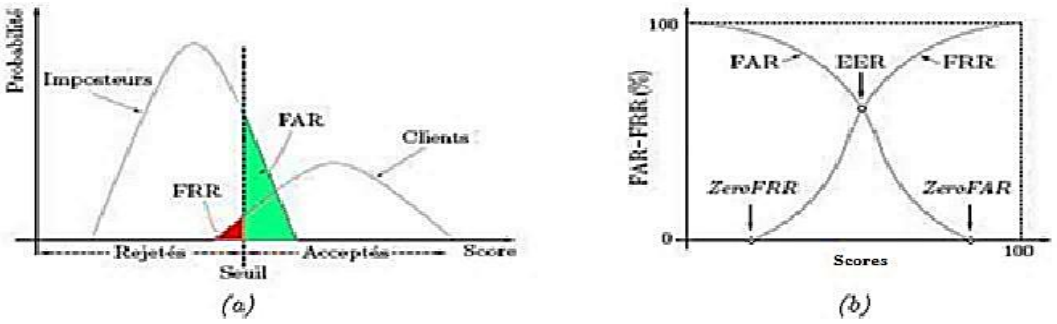

Figure I.17 : Distribution des scores et les taux d'erreurs pour un seuil donné.

FAR : C'est le pourcentage d'individus reconnus par le système biométrique, ce système clase alors deux caractéristiques provenant de deux personnes différentes

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

EER : Ce taux est calculé à partir de FAR et FRR et constitue un point de mesure de performance courant, c.-à-d. **EER=FRR=FAR**.

$$\boldsymbol{EER} = \frac{\textbf{nombre de fausses accceptation+nombre de faux rejets}}{\boldsymbol{nombre\ \ totale\ d'accés}} \qquad \text{(I.2)}$$

✓ **Courbe caractéristiques :** Les performances d'un système biométrique peuvent être présentées graphiquement à l'aide de la courbe ROC (Receiver Operating Characteristic) [4]. Cette courbe représente les valeurs de FRR en termes de FAR. Ceci est obtenu en calculant le couple (FAR, FRR) ou chaque valeur du seuil de décision. Celui-ci diffère de la plus petite valeur obtenue à une valeur supérieure. Cette courbe peut être décomposée en trois zones : zone de haute sécurité, zone de compromis et zone de basse sécurité [16].

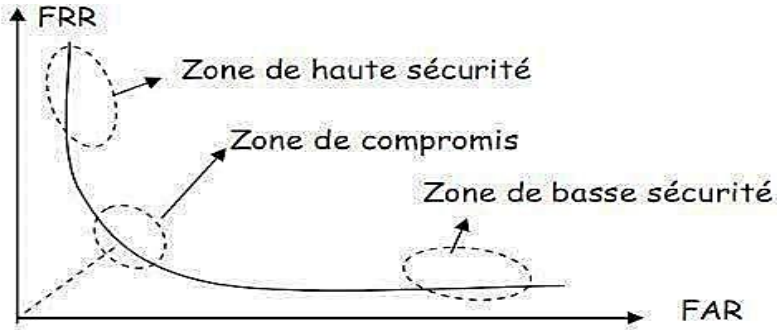

Figure I.18 : *courbe ROC*

Le taux d'identification (ensemble fermé) est la mesure la plus couramment utilisée mais il n'est pas toujours suffisant. En effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve dans les N premiers. On trace alors le score cumulé (cumulative match score) qui représente la probabilité que le bon choix se trouve parmi les N premiers [16]. Dans le cas où

il existe plusieurs modèles pour chaque individu$ dans la base de données, les mesures classiques des systèmes de recherche dans une base de données peuvent être utilisées.

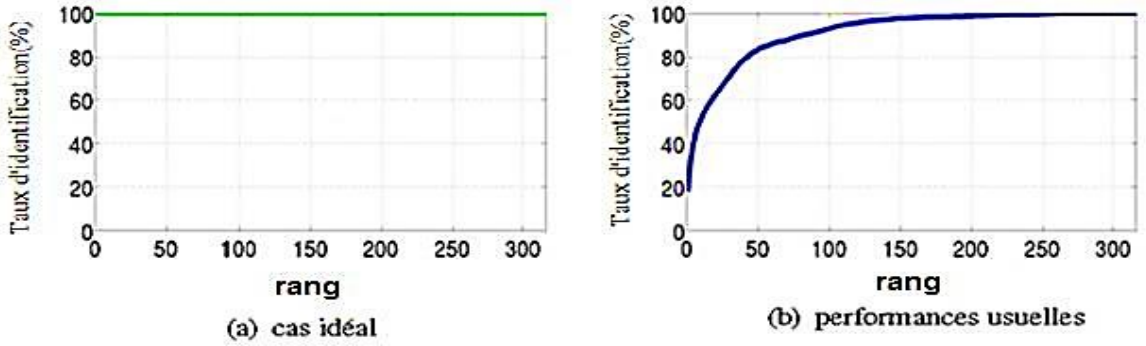

Figure I.19 : *Différentes courbes CMC*

I.10 Domaine d'applications

La biométrie répond aux exigences de sécurité par les secteurs particuliers et les entreprises dans tous les pays. La sécurité biométrique couvre presque tous les domaines. Aujourd'hui, La sécurité biométrique est utilisée dans l'accès aux réseaux et aux systèmes d'information, paiement électronique et cryptage des données. Généralement, les applications de la sécurité biométrique peuvent être classées en quatre sections principales [17].

I.10.1 Service public

- Le contrôle et la sécurité des bâtiments gouvernementaux frontière.
- Contrôle les immigrants qui entrent et sortent du pays.
- Utilisés dans les aéroports et la santé.

I.10.2 Pouvoir judiciaire

- L'utilisation des empreintes digitales pour prouver certains faits concernant les infractions pénales.
- L'utilisation de l'ADN extrait du sang ou des cheveux dans la scène du crime pour obtenir le criminel.

I.10.3 Secteurs des banques

- Les transactions bancaires (retraits en espèces, les cartes bancaires, paiement par le téléphone et Internet).

- La réduction de la proportion de la fraude grâce à l'intégration des cartes à puce avec reconnaissance des empreintes digitales.

I.10.4 Accès physique et logique

Ceci se rapporte au contrôle d'accès physique comme la sécurisation des lieux (bâtiment ou une pièce) ou le contrôle d'accès logique comme la sécurisation d'une session informatique (ordinateur ou base de données).

I.11 Conclusion

De nos jours la biométrie est considéré comme le moyen le plus sûr pour la sécurité. Elle est de plus en plus appliquée dans la réalité grâce à ses avantages. Dans ce chapitre, Nous avons présenté un état de l'art sur les technologies biométriques et mis l'accent sur le grand nombre de ces technologies. Nous avons aussi indiqué quelques points forts et points faibles de chaque technologie qui mettent en évidence le fait qu'elles ne sont pas toutes de la même efficacité. Comme nous avons introduit la notion de vérification de l'identité du modèle et de la structure globale et les applications analytiques ou magazines sur l'utilisation du système de la technologie biométrique.

CHAPITRE II

FUSION ET MULTIMODALITÉ

II.1 Introduction

Comme il a introduit dans le premier chapitre, ils existent plusieurs modalités biométriques appliquées dans le domaine d'identification et d'authentification. Parmi ces modalités, on trouve que l'empreinte palmaire est une biométrie relativement nouvelle. Notre objectif est d'appliques la méthode d'apprentissage et extraction des caractéristiques sur un système biométrique basé sur la modalité de l'empreinte palmaire.

II.2 Système unimodale

Le système unimodal, c'est un système plus simple qui utilise une seule modalité biométrique, par exemple l'utilisation d'un seul band ou un seul algorithme pour identifier les personnes. Ce type des systèmes possède généralement un taux d'erreur très €. Ainsi, ce type des systèmes à plusieurs limitations qui peuvent être rend la sécurisation biométrique inapplicable pour des entreprises ou des personnes particulières.

II.3 Limitations des systèmes unimodaux

Bien que les techniques de reconnaissance biométrique promettent d'être très performantes, on ne peut garantir actuellement un excellent taux de reconnaissance avec des systèmes biométriques unimodaux, basés sur une unique signature biométrique. De plus, ces systèmes sont souvent affectés par les problèmes suivants [18].

- **Bruit introduit par le capteur :** du bruit peut être présent dans les données biométriques acquises, ceci étant principalement dû à un capteur défaillant ou mal entretenu. Par exemple, l'accumulation de poussière sur un capteur d'empreintes digitales, un mauvais focus de caméra entraînant du flou dans des images de visage ou d'iris, etc. Le taux de reconnaissance d'un système biométrique est très sensible à la qualité de l'échantillon biométrique et des données bruitées peuvent sérieusement compromettre la précision du système.
- **Non-universalité :** si chaque individu d'une population ciblée est capable de présenter une modalité biométrique pour un système donné, alors cette modalité est dite universelle. Ce principe d'universalité constitue une des conditions nécessaires de base pour un module de reconnaissance biométrique. Cependant, toutes les modalités biométriques ne sont pas vraiment universelles. Le National Institute of Standards and Technologies (NIST) a rapporté

qu'il n'était pas possible d'obtenir une bonne qualité d'empreinte digitale pour environ 2% de la population (personnes avec des handicaps liés à la main, individus effectuant de nombreux travaux manuels répétés, etc.). Ainsi, de telles personnes ne peuvent pas être enrôlées dans un système de vérification par empreinte digitale. De la même manière, des personnes ayant de très longs cils et celles souffrant d'anormalités des yeux ou de maladies oculaires (comme certains glaucomes et cataractes) ne peuvent fournir des images d'iris, ou de rétine, de bonne qualité pour une reconnaissance automatique. La non-universalité entraîne des erreurs d'enrôlement ("Failure to Enroll" ou FTE) et/ou des erreurs de capture ("Failure to Capture" ou FTC) dans un système biométrique.

- **Manque d'individualité :** les caractéristiques extraites à partir de données biométriques d'individus différents peuvent être relativement similaires. Par exemple, une certaine partie de la population peut avoir une apparence faciale pratiquement identique due à des facteurs génétiques (père et fils, vrais jumeaux, etc.). Ce manque d'unicité augmente le taux de fausse acceptation ("False Accept Rate" ou FAR) d'un système biométrique.
- **Manque de représentation invariante :** les données biométriques acquises à partir d'un utilisateur lors de la phase de reconnaissance ne sont pas identiques aux données qui ont été utilisées pour générer le modèle de ce même utilisateur lors de la phase d'enrôlement. Ceci est connu sous le nom de "variations intra classe". Ces variations peuvent être dues à une mauvaise interaction de l'utilisateur avec le capteur (par exemple, changements de pose et d'expression faciale lorsque l'utilisateur se tient devant une caméra), à l'utilisation de capteurs différents lors de l'enrôlement et de la vérification, à des changements de conditions de l'environnement ambiant (par exemple, changements en éclairement pour un système de reconnaissance faciale) ou encore à des changements inhérents à la modalité biométrique (par exemple, apparition de rides dues à la vieillesse, présence de cheveux dans l'image de visage, présence de cicatrices dans une empreinte digitale, etc.). Idéalement, les caractéristiques extraites à partir des données biométriques doivent être relativement invariantes à ces changements. Cependant, dans la plupart des systèmes biométriques, ces caractéristiques ne sont pas invariantes et, par conséquent, des algorithmes complexes sont requis pour prendre en compte ces variations. De grandes variations intra classe augmentent généralement le taux de faux rejet ("False Reject Rate" ou FRR) d'un système biométrique.
- **Sensibilité aux attaques** : bien qu'il semble très difficile de voler les modalités biométriques d'une personne, il est toujours possible de contourner un système biométrique en utilisant des modalités biométriques usurpées. Des études ont montré qu'il était possible de

fabriquer de fausses empreintes digitales en gomme et de les utiliser pour contrer un système biométrique. Les modalités biométriques comportementales telles que la signature et la voix sont plus sensibles à ce genre d'attaque que les modalités biométriques physiologiques.

II.4 Système multimodal

Les humaines se reconnaissent entre eux à partir de plusieurs modalités biométriques physiques ou comportementales. Chaque modalité en soin peut pas toujours être utilisée de manière fiable pour effectuer la reconnaissance [18]. Cependant, la consolidation d'information présentées par les déférentes modalités peut paramètre une reconnaissance précise de l'identité. Cette stratégie peut être utilisée pour réduire quelques problèmes et limitations, liées aux systèmes multimodaux. En effet, la combinaison de plusieurs modalités a pour but d'améliorer les performances se reconnaissance. En augmentant la quantité d'information discriminantes de chaque personne, on souhaite augmenter le pouvoir de reconnaissance du système (vérification ou l'identification) [19].

II.5 Score

Les scores sont les résultats générés par le système de reconnaissance lors d'une mode identification le score indique la personne incluse dans la base des clients qui ressemble le plus à la personne proclamant. Dans ce mode, le résultat est un ensemble de N scores où N est le nombre des personnes enregistrés dans la base de données et chaque score si représente la vraisemblance entre les paramètres test et le modèle $\boldsymbol{\lambda_i}$ sauvegardé dans la base [20]. Afin de s'assurer que ces vecteurs de similarité soient cohérents entre eux, il est nécessaire de les normaliser avant de considérer une fusion des scores [21].

II.6 Fusion des données

La fusion des données est une technique utilisée en traitement d'informations issues des sources multiples [21]. Elle consiste à combiner des données issues de plusieurs sources afin d'obtenir une décision meilleure que celle obtenue à partir de chacune des sources prise isolément. La fusion de données a été initialement développée surtout dans un contexte militaire pour des objectifs tels que la localisation des cibles ennemies et la fusion d'images radar [22]. Les systèmes employés ont recours à des techniques diverses issues de domaines variés tels le traitement du signal, l'intelligence artificielle, la reconnaissance des formes, la classification, etc... De façon générale, la fusion de données est une opération d'intégration de plusieurs

données en vue d'en extraire une nouvelle information plus représentative de l'ensemble des données. Actuellement, la fusion des données prend une place de plus en plus importante dans de nombreux domaines. Elle permet d'aider efficacement les scientifiques à extraire des informations de plus en plus pertinentes et précises. La fusion de données a d'abord visé d'améliorer la qualité des réponses aux problèmes posés par les militaires mais aujourd'hui elle touche énormément de domaines telles que [22] : la télédétection, la prévision météorologique, la biométrie multimodale, l'application médicale et la robotique.

II.7 Sources des informations

Le problème général de la fusion est la synthèse d'un ensemble d'informations obtenues à partir de la mise en commun d'informations provenant des sources différentes. Cependant, il existe, de nombreux scénarios possibles pour les sources d'information qui peuvent être considérées dans un système biométrique multimodal [23].

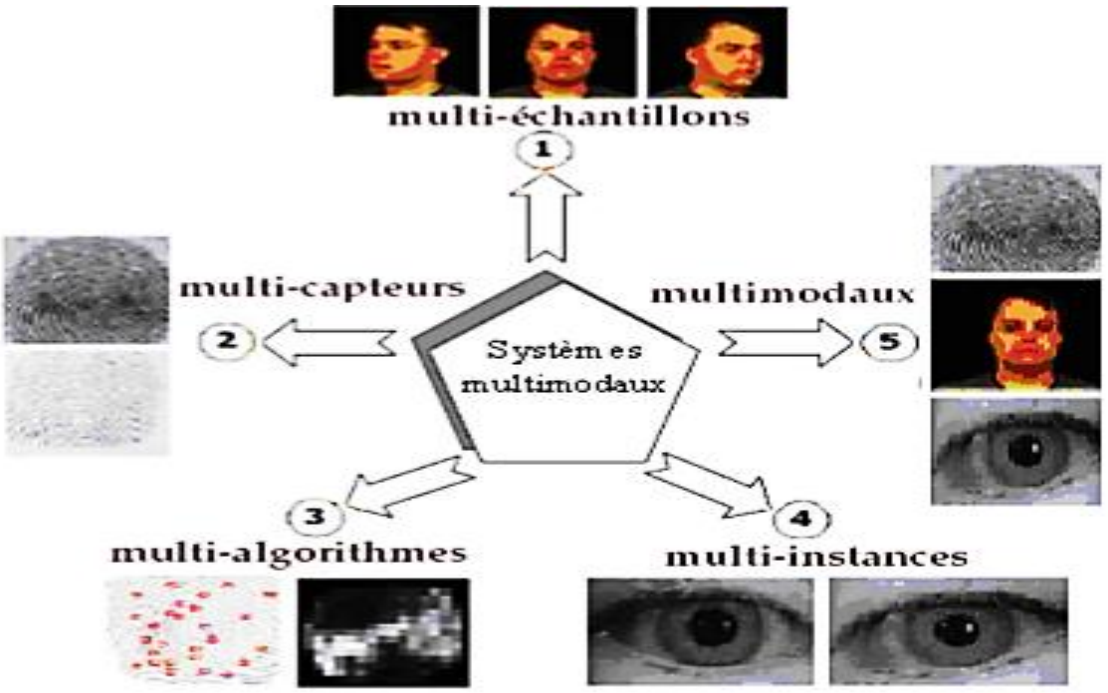

Figure II.1: *Différents systèmes biométriques multimodaux.*

II.7.1 Systèmes multi-algorithmes

Dans ces systèmes, les mêmes données biométriques sont traitées à travers plusieurs algorithmes. Par exemple, des algorithmes d'analyse de texture et de minuties peuvent être associés pour traiter la même image d'empreinte digitale afin d'extraire diverses caractéristiques qui peuvent améliorer la performance du système [24]. Ainsi, ce genre de

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

II.7.2 Systèmes multi-instances

Un unique capteur peut être utilisé pour acquérir plusieurs instances de la même modalité biométrique dans le but de prendre en compte les variations qui peuvent se produire au sein de cette modalité. Par exemple, un système de reconnaissance faciale peut capturer plusieurs images du visage avec des changements de pose (profil frontal, profils gauches et droits), d'expression ou d'illumination de tenir compte des variations de la pose faciale [25].

II.7.3 Systèmes multi-capteurs

Correspondant à l'utilisation de plusieurs capteurs pour l'acquisition d'une seule modalité biométrique. Pour la reconnaissance de l'image, par exemple, il est possible d'utiliser plusieurs caméras 2D, des capteurs 3D ainsi que des capteurs infrarouges. L'utilisation de plusieurs capteurs permet d'acquérir des informations complémentaires pour accroître les performances des systèmes unimodaux [25].

II.7.4 Systèmes Multi-biométries

Dans ces systèmes, différentes modalités biométriques sont combinées afin d'établir l'identité d'un individu. Par exemple, les caractéristiques du l'empreinte palmaire et l'empreinte digitale. Cette stratégie de fusion consiste à exploiter les avantages de chaque système biométrique tout en évitant leurs inconvénients. En fait, les systèmes combinant plusieurs informations issues de la même biométrie permettent d'améliorer les performances en reconnaissance, en réduisant l'effet de la variabilité infra-classe. Mais ils ne permettent pas de traiter efficacement tous les problèmes des systèmes monomodaux. C'est pour cette raison que les systèmes multi-biométries ont reçu beaucoup d'attention [26].

II.7.5 Systèmes multi-échantillons

Lorsqu'ils associent plusieurs échantillons différents de la même modalité, par exemple deux empreintes digitales de doigts différents ou les deux iris. Dans ce cas les données sont traitées par le même algorithme mais nécessitent des références différentes à l'enregistrement contrairement aux systèmes multi-instances qui ne nécessitent qu'une seule référence [27].

II.8 Niveaux des fusions

Dans un système biométrique multimodal, la fusion peut se faire en utilisant l'information disponible dans n'importe quel ces modules. 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 quatre niveaux de fusion peuvent être classés en deux sous-ensembles : La fusion pré-classification (avant comparaison) et la fusion post-classification (après la comparaison).

II.8.1 Fusion au niveau du capteur

On dit aussi bas niveau ; Il concerne la fusion d'informations directement issues des capteurs **(Figure.II.2).** La fusion au niveau du capteur ou des données brutes est relativement peu utilisée car elle nécessite une homogénéité entre les données. Par exemple il est possible de combiner plusieurs images de visages dans des canaux de couleurs différents ou en visible et en infrarouge s'ils correspondent à la même scène. Il est également possible de faire une mosaïque à partir d'images prises de différents points de vue. Plusieurs techniques peuvent être utilisées. Par exemple, la transformée en ondelette discrète et la transformation des plans couleurs (RGB p YUV), sont deux techniques pour fusionner plusieurs modalités.

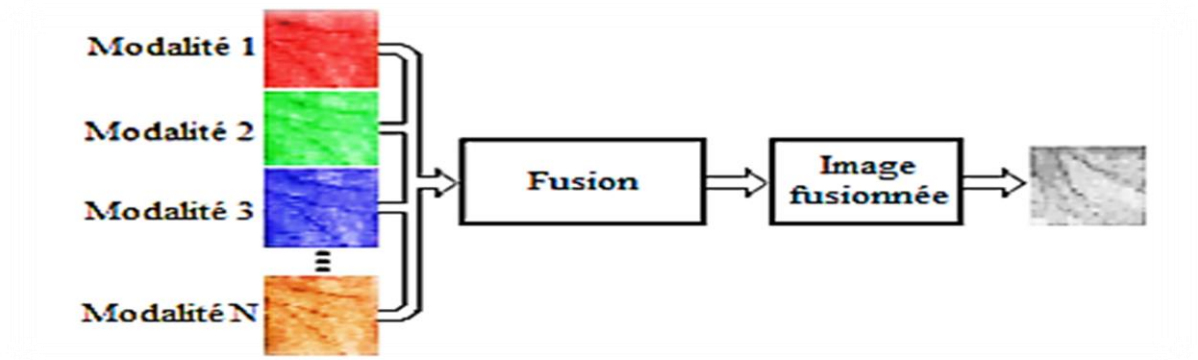

Figure II.2 : *Schéma de fusion au niveau d'image*

II.8.2 Fusion au niveau des caractéristiques

On dit aussi niveau intermédiaire ; il concerne la combinaison d'informations extraites après diverses phases de traitement et d'analyse des mesures. La fusion au niveau caractéristiques consiste à combiner différents vecteurs de caractéristiques qui sont obtenus à partir d'une des sources suivantes **(Figure II.3) :** plusieurs capteurs du même trait biométrique,

plusieurs algorithmes du même trait biométrique, ou encore plusieurs traits biométriques. Quand les vecteurs de caractéristiques sont homogènes (par exemple, plusieurs images d'empreinte palmaires d'un utilisateur), un unique vecteur de caractéristiques résultant peut-être calculé comme une somme pondérée des vecteurs de caractéristiques individuels. Lorsque les vecteurs de caractéristiques sont hétérogènes (par exemple, des vecteurs de caractéristiques de différentes modalités biométriques comme le visage et la géométrie de la main), nous pouvons les concaténer pour former un seul vecteur de caractéristiques.

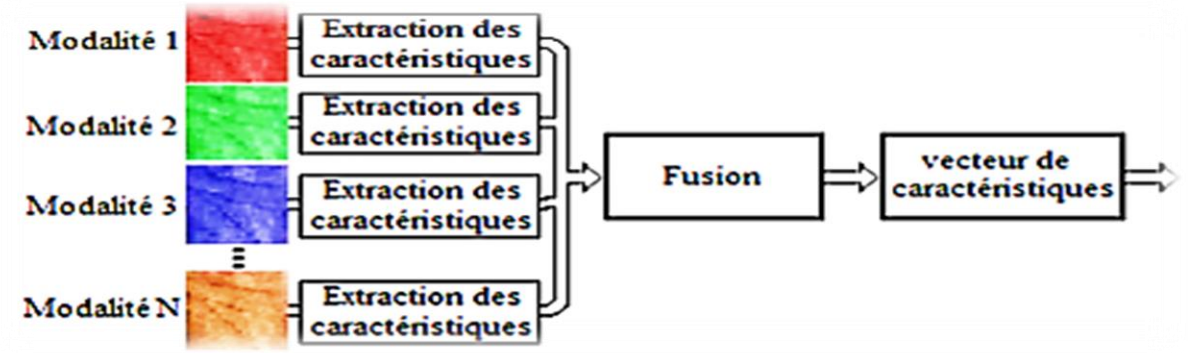

Figure II.3 : *Schéma de fusion au niveau d'extraction*

II.8.3 Fusion au niveau de score

La fusion au niveau des scores **(Figure II.4)** est le type de fusion le plus utilisé car elle peut être appliquée à tous les types de systèmes, dans un espace de dimension limité (un vecteur de scores dont la dimension est égale au nombre de sous-systèmes), avec des méthodes relativement simples et efficaces mais traitant plus d'information que la fusion de décisions. Il existe un grand nombre de méthodes de fusion de scores. Généralement, avant la fusion, une opération de normalisation est nécessaire pour rendre tous les scores dans le même intervalle.

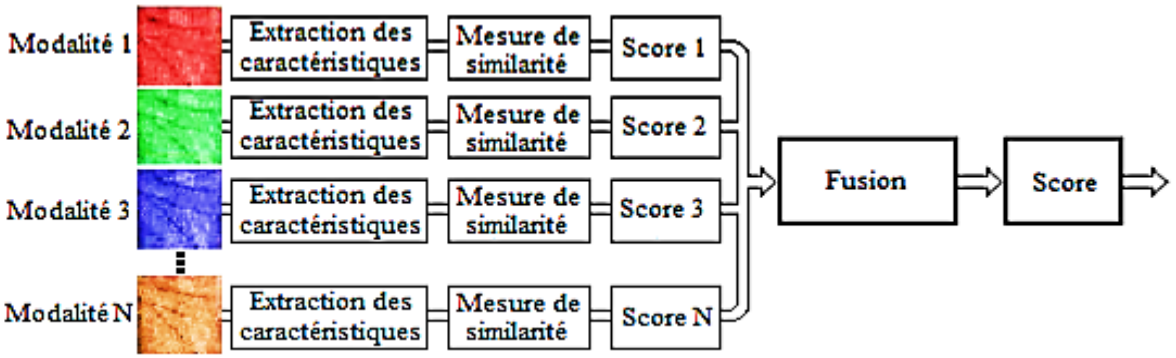

Figure II.4 : *Schéma de fusion au niveau score*

II.8.4 Fusion au niveau décision

On dit aussi haut niveau, celui-ci concerne la combinaison des décisions obtenues à partir de chaque source **(Figure II.5)**. La fusion au niveau des décisions est souvent utilisée pour sa simplicité. En effet, chaque système fournit une décision binaire sous la forme OUI ou NON que l'on puisse représenter par 0 et 1, et le système de fusion de décisions consiste à prendre une décision finale en fonction de cette série de 0 et de 1. Les méthodes les plus utilisées sont des méthodes à base de votes telles que l'OR (si un système a décidé 1 alors OUI), le AND (si tous les systèmes ont décidé 1 alors OUI) ou le vote à la majorité (si la majorité des systèmes ont décidé 1 alors OUI). On peut également utiliser des méthodes plus complexes qui pondèrent les décisions de chaque sous-système. Ces méthodes de fusion au niveau des décisions sont très simples mais utilisent très peu d'information (0 ou1).

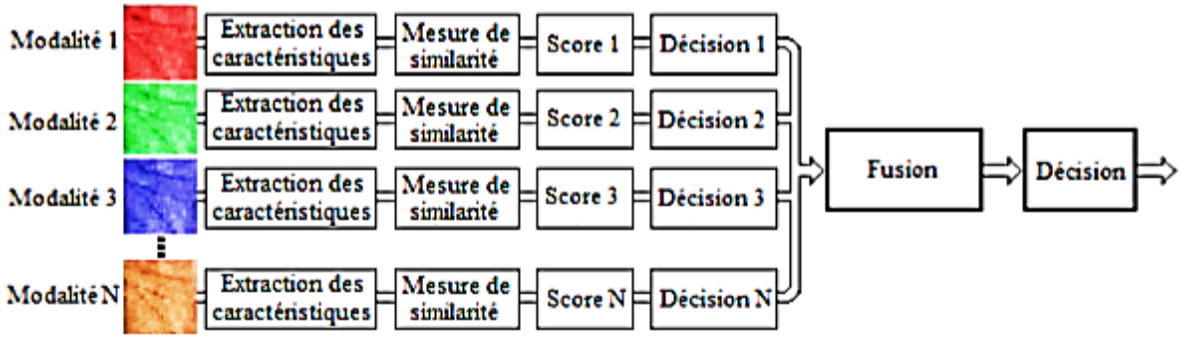

Figure II.5 : *Schéma de fusion au niveau décisions.*

Les méthodes de combinaisons de scores sont des méthodes très simples dont l'objectif est d'obtenir un score final S à partir des N scores disponibles si pour i = 1 à N issus de N systèmes. Les méthodes les plus utilisées sont la moyenne, le produit, le minimum, le maximum ou la médiane [14].

Somme des scores : combiner les scores par la moyenne consiste à calculer

$$\boldsymbol{S = \sum_{i=1}^{N} S\, i} \qquad (2.1)$$

Combiner les scores par le produit : consiste à multiplier tous les scores tel que :

$$\mathbf{S = \frac{1}{N} \Pi_{i=1}^{N} Si} \qquad (2.2)$$

Minimum des scores : Dans cette technique, on assigne au score final (fusionné) le meilleur (Minimum) score calculé par les différents systèmes. Le minimum est alors défini par :

$$\boldsymbol{S = \min(Si)} \qquad (2.3)$$

Maximum des scores : la règle maximum est obtenue en assignant la valeur maximum des scores au score final (fusionné) de la façon suivante :

$$\boldsymbol{S = \max(Si)} \quad (2.4)$$

La règle somme pondérée : C'est une méthode un peu plus évoluée qui nécessite une adaptation par le réglage de paramètres :

$$\boldsymbol{S = 1/N \sum_{i=1}^{N} S\, i\, \omega i} \quad (2.5)$$

La somme pondérée permet de donner des poids différents ωi à chacun des systèmes en fonction de leur performance individu elle ou de leur intérêt dans le système multi algorithmes

II.9 Pourquoi normaliser les scores ?

Trois problèmes importants ont besoin d'être considérés avant même de combiner les scores de correspondance en un seul et unique score. Tout d'abord, les scores de correspondance au niveau des sorties des matchers individuels peuvent ne pas être homogènes. Par exemple, un matcher peut donner en sortie une mesure de distance (dissimilarité)pendant qu'une autre donne en sortie une mesure de proximité(similarité). Ensuite, les sorties des matchers individuels ne sont pas nécessairement inclus dans le même intervalle. Enfin, les scores de correspondance en sortie des matchers peuvent suivre différentes distributions statistiques. A cause de ces raisons, la normalisation de score est essentielle pour transformer les scores des matchers individuels dans un domaine commun avant de les combiner. La normalisation de score est une étape critique dans la conception d'un schéma de combinaison pour la fusion au niveau score.

II.9.1 Normaliser Les Scores

La normalisation est une étape nécessaire lors de la fusion de scores, car la distribution des scores issus des différents sous-systèmes est rarement compatible (c'est-à-dire, il est inutile de faire la somme des scores du système A avec ceux du système B si la distribution des scores du système A est [0;1] et celle du système B est [1000;10000]). Ce paragraphe présente les principales méthodes de normalisation [28]. Une des méthodes de normalisation les plus simples est la normalisation min max. Elle est utilisée lorsque les bornes de la distribution des scores sont connes. En utilisant cette technique, les scores sont normalisés entre 0 et 1. A partir d'un ensemble de scores {Sk} k=1, 2,n, les scores normalisés sont obtenus de la façon suivante :

$$S'k = \frac{Sk - min}{\max - \min} \quad (2.6)$$

II.10 Motivations

La technologie d'identification par leurs empreinte palmaire reconnaît les individus aux mains. Cette modalité représente la surface intérieure du main caractéristiques bien distinctives, surtout au les lignes principales. Ces dernières années, ce nouveau descripteur biométrique basé sur cette surface, appelé empreinte palmaire est commencé à utiliser comme une nouvelle technologie biométrique, plusieurs travaux montrent que cette l'empreinte peut être utilisée dans le domaine d'identification des personnes pour une reconnaissance robuste et précise.

Notre travail proposé consiste un système d'identification basé sur empreint palmaire par l'utilisation d'une nouvelle technologie s'appelle (deep Learning).

II.11 L'empreinte palmaire

II.11.1 Définition de l'empreinte palmaire

On appelle paume de la main la partie intérieure de la main (partie non visible lorsque la main est fermée) du poignet aux racines des doigts, comme le montre la **Figure.II.6**. Ainsi, l'empreinte palmaire n'est autre que l'impression (image) de la paume de la main faite par la pression de cette dernière sur une surface donnée. En d'autres termes, elle peut être définie comme étant le modèle de la paume de la main illustrant les caractéristiques physiques du motif de sa peau tel que les lignes (principales et rides), points, minutie et texture [29].

Figure II.6 : *La paume de la main*

Une identification palmaire peut être vue comme étant l'aptitude d'identifier une personne parmi d'autres d'une manière unique à travers un algorithme approprié exploitant les caractéristiques de l'empreinte palmaire.

II.11.2 Caractéristique biométrique d'une empreinte palmaire et les type de reconnaissance

L'empreinte palmaire présente différents types de caractéristiques qui peuvent être exploitées dans la reconnaissance des individus [29]

➢ Des caractéristiques géométriques

Comme toute image, l'empreinte palmaire présente des caractéristiques géométriques telles que : la longueur, la largeur, et la surface. Ces caractéristiques ne sont pas distinctives mais peuvent tout de même être utiles pour une première vérification.

➢ Les lignes principales

L'empreinte palmaire est caractérisée par trois plis de flexion, dites lignes principales : la ligne de tête, la ligne de vie et celle du cœur. La **Figure II.7** montre les différents plis d'empreintes palmaires.

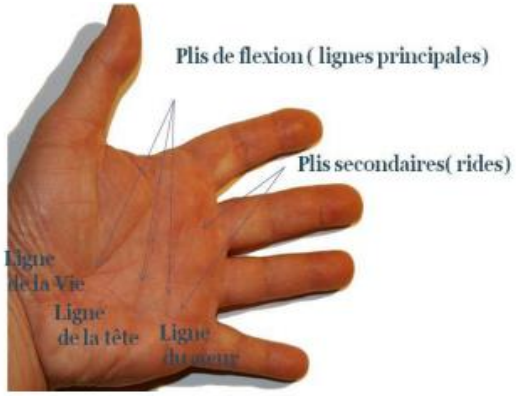

Figure II.7 : *L'empreinte palmaire et ses plis*

➢ Les points de référence

Les points représentant les deux extrémités d'empreintes palmaires sont appelés point de références. Ce sont les points a et b dans la **Figure II.8**.

Ils servent de point de repère lors de l'alignement et l'extraction des caractéristiques de l'empreinte palmaire. La taille de cette dernière peut être aussi estimée grâce à ces deux points.

Figure II.8 a et b : *les points de référence de l'empreinte palmaire*

II.11.3 Reconnaissance par empreinte palmaire

Le système que nous nous proposons de concevoir est un système « en ligne » d'analyse biométrique de la main. Il doit être capable d'identifier un individu préalablement enregistré par ses caractéristiques de l'empreinte palmaire. Les images capturées font l'objet de différents traitements pour extraire les caractéristiques discriminantes de l'empreinte palmaire. Ensuite le système doit réaliser un apprentissage et enfin être capable de décider, quelle est l'identité exacte de l'utilisateur à identifier en fusionnant les informations en sortie des différents modules de recherche.

II.12 Extraction des caractéristiques

Cette étape représente le cœur du système de reconnaissance, on extrait de l'image les informations qui seront sauvegardées en mémoire pour être utilisées plus tard dans la phase de décision. L'extraction des caractéristiques utilise plusieurs méthodes, Parmi lesquelles on cite long-Gabor.

II.13 Filtre de Gabor

Pour les applications nécessitant une analyse par orientations, les fonctions de Gabor produisent une décomposition en ondelettes très utilisé. De nombreuses applications en traitement d'images font appel à l'utilisation ces types des fonctions, comme par exemple l'analyse de textures ou objets par attributs fréquentiels. En effet, les lignes de l'empreinte sont caractérisées par leur fréquence locale et leur orientation. En utilisant des filtres de Log Gabor [29, 30] bien choisis, il est possible d'en extraire les caractéristiques biométriques. Cependant,

lorsque ceux-ci sont correctement paramètres, ils permettent de préserver les lignes et fournissent des informations sur l'orientation locale de la texture. Dans le domaine fréquentiel, la réponse (f_{Gb}) de filtre log-Gabor 1D se définit comme [30].

$$\boldsymbol{fGb = \exp[\frac{-(\log(\frac{f}{fo}))^2}{2(\log(\frac{\sigma}{fo}))^2}]} \quad (2.7)$$

Ou f_0 est la fréquence centrale et dénote la variance. L'application de filtre de Log-Gabor un choix empirique de paramètres de filtre (f_0 et σ) Ces paramètres empiriques sonttrès difficiles a déterminer et c'est l'un des inconvénients des approches basées sur ce filtre

II.14 Classification

Cette étape consiste à modéliser les paramètres extraits d'une modalité d'un individu en se basant sur leurs caractéristiques communes. Un modèle est un ensemble d'informations utiles, discriminantes et non redondantes qui caractérise un ou plusieurs individus ayant des similarités, ces derniers seront regroupés dans la même classe, et ces classes varient selon le type de décision [31].

Dans ce travail, nous utilisons deux algorithmes sont RBM (Machine de Boltzmann Restreinte) DBN (Réseau Deep Belief), à base d'Un réseau de neurones.

II.14.1 Machine de Boltzmann Restreinte

La machine Boltzmann restreinte (RBM) est une double couche, bipartite, Modèle graphique non dirigé avec un ensemble d'unités cachées binaires h, Un ensemble d'unités visibles (binaire ou valeur réelle) v, et des connexions symétriques entre ces deux couches représentées par une matrice de poids W. La sémantique probabiliste pour un RBM est dé finie par sa fonction énergétique comme suit :

$$\mathrm{P(v,h)} = \frac{1}{Z}\exp\big(-E(v,h)\big) \quad (2.8)$$

Où Z est la fonction de partition. Si les unités visibles sont à valeur binaire, nous définissons la fonction d'énergie comme suit :

$$\mathrm{E(v,h)} = \sum_{ij} \mathrm{vi\ Wij\ hj} - \sum_{j} \mathrm{bj\ hj} - \sum_{i} \mathrm{ci\ vi} \quad (2.9)$$

Où bj sont des biais unitaires cachés et ci sont des biais unitaires visibles. Si les unités visibles sont réellement évaluées, nous pouvons définir la fonction énergie comme suit :

$$E(v,h) = \frac{1}{2}\sum_i \ vi^2 \sum_{ij} vi\ Wij\ hj\ - \sum_j \ bj\ hj - \sum_i \ ci\ vi \qquad (2.10)$$

De la fonction énergétique, Il est clair que les unités cachées sont conditionnellement indépendantes l'une de l'autre compte tenu de la couche visible, et vice versa. En particulier, les unités d'une couche binaire (conditionnées sur l'autre couche) sont des variables aléatoires Bernoulli indépendantes. Si la couche visible est à valeur réelle, les unités visibles (conditionné sur la couche cachée) sont gaussiennes avec covariance diagonale. Par conséquent, nous pouvons effectuer un échantillonnage de Gibbs à blocs efficaces en échantillonnant alternativement les unités de chaque couche (en parallèle) étant donné l'autre couche. Nous nous référerons souvent à la valeur attendue d'une unité comme activation. En principe, les paramètres RBM peuvent être optimisés en effectuant une montée en gradient stochastique sur la probabilité logarithmique des données de formation. Malheureusement, l'informatique du gradient exact du log-vraisemblance est intraitable. Au lieu de cela, on utilise généralement l'approximation de divergence contrastive (Hinton, 2002), Ce qui a montré qu'il fonctionnait bien dans la pratique [32].

II.14.2 Réseau Deep Belief (Deep Belief Network)

La RBM seule est limitée dans ce qu'elle peut représenter. Son véritable pouvoir émerge lorsque les RBM sont empilés pour former un réseau de croyances profondes, Un modèle générateur composé de plusieurs couches. Dans un DBN, chaque couche comprend un ensemble d'unités binaires ou à valeur réelle. Deux couches adjacentes ont un ensemble complet de connexions entre elles, Mais pas deux unités dans la même couche sont connectées. Hinton. (2006) a proposé un algorithme efficace pour la formation de réseaux de croyances profondes, En entraînant avidement chaque couche (du plus petit au plus haut) en tant que RBM en utilisant les activations de couche précédente comme entrées. Cette procédure fonctionne bien en pratique [32].

II.15 Conclusion

Actuellement, il y'a une nouvelle tendance qui arrive et qui commence à susciter les efforts, c'est le multimodal, dans lequel on combine plusieurs technologies biométriques, ou plusieurs algorithmes de reconnaissance, ou on utilise divers systèmes pondères dans l'optique

d’améliorer les performances de reconnaissance. Dans ce contexte, nous avons présenté dans ce chapitre la reconnaissance par l’empreinte palmaire biométrie multimodale. Après avoir présenté biométrie multimodale et les limitations des systèmes biométriques, lorsqu'ils utilisent une seule modalité biométrique ainsi que les avantages des systèmes multimodaux, 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.

CHAPITRE III

RESULTATS EXPERIMENTAUX

III.1 Introduction

L'étude expérimentale de cette étude est basée sur la reconnaissance de personnes par leurs empreintes palmaire en utilisant la méthode décrite dans le chapitre précédent. Elle est réalisée sur la base de données.

Afin d'évaluer l'efficacité des méthodes étudiées et les performances de notre système biométrique proposé, et vue l'importance affectée à la modalité de l'empreinte palmaire dans les dernières années, nous allons présenter brièvement les caractéristiques de l'empreinte palmaire.

III.2 Architecture du système proposé

Le système **(voir Figure III.1)** est composé de trois modules principaux : Extraction des caractéristiques, classification, et Décision. En fait, le module d'extraction des caractéristiques est basé sur la filtre de log-Gabor. L'image d'entrée peut être une modalité parmi les quatre modalités qui sont formées l'image multi-spectrale (R, G, B, N). Donc, on peut former 4 sous-systèmes différents, par le changement de l'image (modalité) d'entrée.

Dans cette section, Nous avons effectué une étude comparative entre les 4 modalités (bandes spectrales de l'image) dans le deux modes opératoire (vérification et identification). Le but étant de pouvoir choisir la meilleure modalité qui lui donne une meilleure performance.

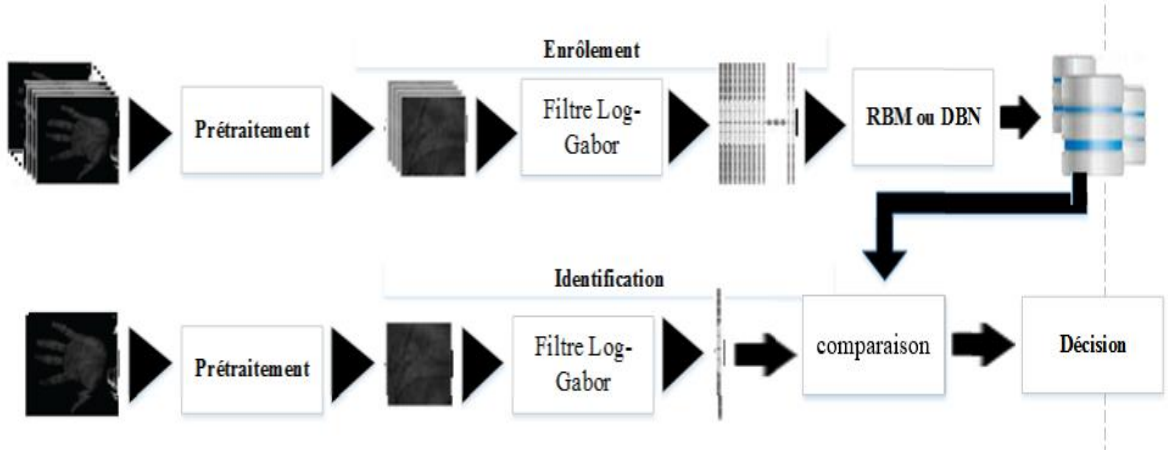

Figure III.1 : *Schéma du principe d'un système d'identification uni-modal*

III.3 Base de données de l'empreinte palmaire

Les images de palm priants que nous avons utilisé dans nos expérimentations sont issues de la base de données PolyU Data base. Les images de cette base ont été collectées parmi 400 individus en utilisant un dispositif de capture d'images de palm priants conçu par des chercheurs de l'université polytechnique de Hong Kong. Les images ont été prises dans deux périodes différentes séparées par un intervalle de temps d'environ deux mois. Durant chaque période, chaque individu devait prendre au moins six images de ses palm priants. De plus, dans la deuxième période, la source de lumière et l'objectif de la caméra CCD (**la figure III.2**) ont été ajustés de telle sorte que les images de la première et deuxième période donnent l'impression d'avoir été prises par deux dispositifs de Palmprint , Application sur un système uni-modal différents [33].

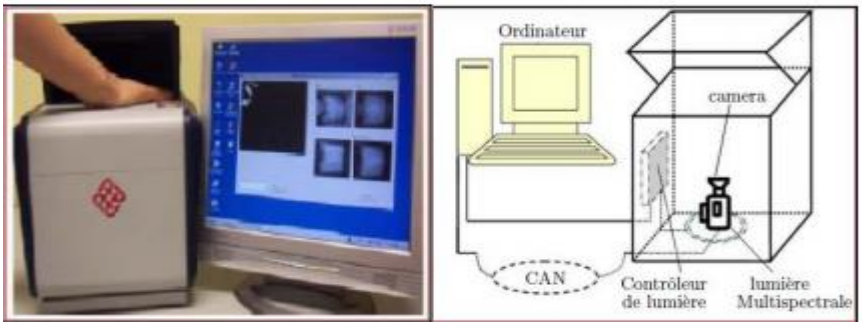

Figure III.2: *Schéma de principe de dispositif d'acquisition des images multi-spectrales (MSP)*

Les images ont, aussi, été prises dans des conditions de lumière différentes afin de tester la robustesse du système de reconnaissance. La taille des images est de 128×128 pixel avec une résolution de 75 dpi. Le système collecte quatre images depuis quatre bandes (Rouge, Vert, Blue et NIR). **La figure II.2** montre des échantillons d'empreinte palmaire multi-spectrale sous les quatre bandes spectrales. Cette base d'images contient 4800 images pour chaque bande provenant des 400 paumes différentes [38]

Figure III.3: *Quelques images de la base de données PolyU-MSP*

III.4 Séparation des bases de données

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

➢ **Images d'apprentissages :** La première, la quatrième, la Septème et dixième image de chaque personne servent pour la phase d'apprentissage.

➢ **Images de Tests :** Les 8 images restantes de chaque individu nous ont servi pour la réalisation des différents tests.

III.5 Résultat du système unimodal

Nous avons utilisé l'algorithme de filtre log-Gabor pour extraire les caractéristiques des empreintes palmaires. Ces algorithmes sont classés parmi les meilleurs descripteurs de textures actuels. Nous avons effectué plusieurs expérimentations afin de voir quel est la meilleure méthode ainsi que la meilleure bande qui donnent des résultats performants. Dans ce cas, les résulte des quatre bande (**NIR, Blue, Green et Red**) sont illustré dans les deux tableaux suivants :

DBN	**Ensemble Ouvert**		**Ensemble fermé**	
	EER	T_0	ROR	RPR
Green	**0.029**	**0.8909**	99.25	8
Blue	0.047	0.886	99.00	11
Red	0.043	0.856	**99.50**	**9**
NIR	0.0312	0.891	99.125	4

Tableau III.1 : *Performance de système uni modal la méthode DBN*

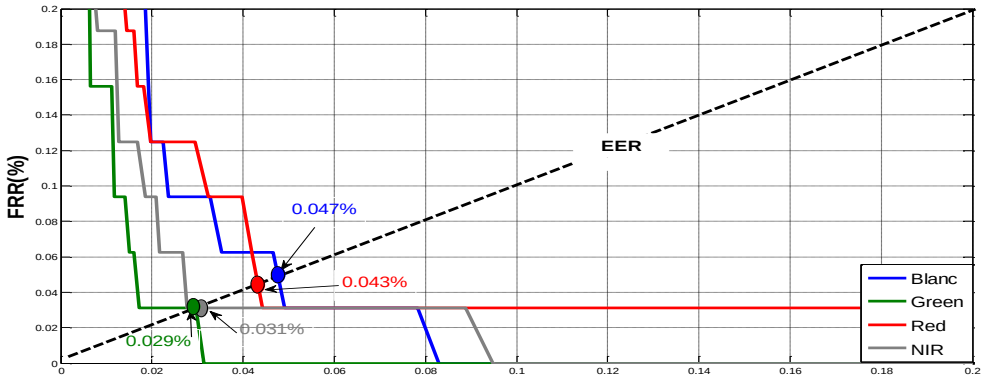

Figure III.4 : *Performance de système unimodal, ensemble ouvert.*

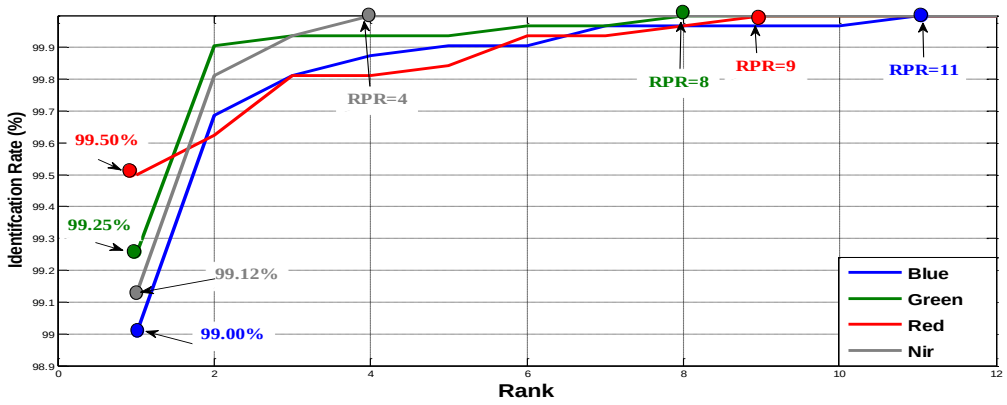

Figure III.5 : *Performance de système uni modal, ensemble fermé.*

Il est clair que l'erreur la plus faible, dans le mode d'identification **ensemble ouvert**, a été réalisée par la bande **Green**, cette bande donne un **EER** égale à **0.029%** avec un seuil **To** égal à **0.08906**. Dans le mode d'identification ensemble fermé, la bande **Red** donne la meilleure performance avec un **ROR = 99.50%** et un **RPR = 9**

RBM	**Ensemble Ouvert**		**Ensemble fermé**	
	EER	T_0	ROR	RPR
Green	0.125	0.840	98.468	22
Blue	0.25	0.8435	**96.468**	**19**
Red	**0.093**	**0.848**	98.343	21
NIR	0.187	0.815	97.625	62

Tableau III.2 : *Performance de système uni modal basé sur la méthode RBM*

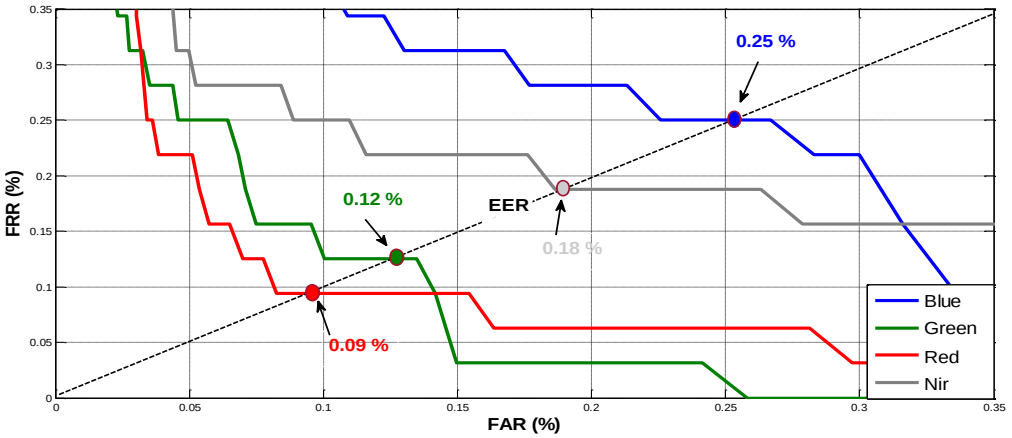

Figure III.6 : *Performance de système uni modal, ensemble ouvert.*

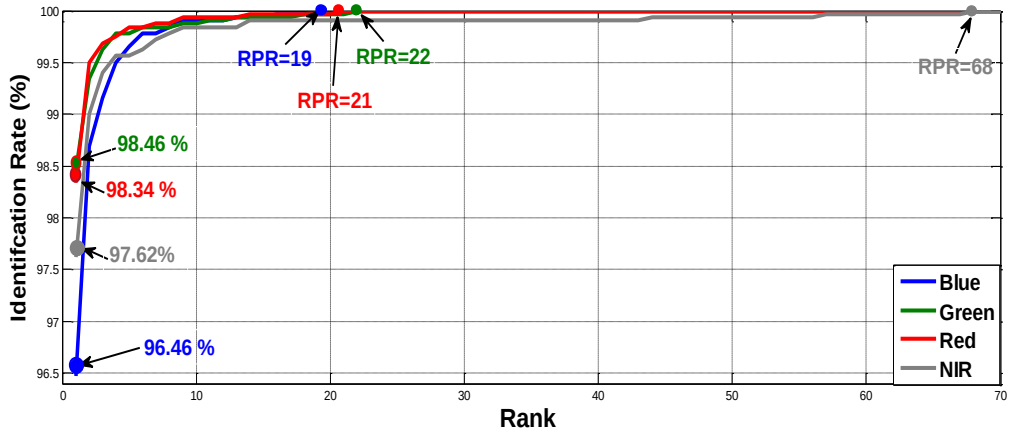

Figure III.7 *: Performance de système unimodal, ensemble fermé.*

Après l'application de l'algorithme RBM le **Tableau III.2** semble que la band Red est donne un meilleur résulte en Ensemble ouvert par rapport les D'autres band (**Blue**=0.25, **Green**=0.12, **Red**=0.093, **NIR**=0. 18). Ainsi, que l'Ensemble Fermé donne des résultats du **ROR** et du **RPR** sont moyen, la bande **Green** donne un bonne résulta **ROR=98.468**, **RPR=22.**

Discussion et analyse des résultats

La méthode d'extraction des caractéristiques basée sur la méthode filtre log-Gabor est utilisée pour tous les bandes. Pour mieux comprendre le comportement de système sous ces paramètres, la courbe **Figure III.4**, montre le taux des clients acceptés (Genuine Acceptance Rate (GAR)) du système en fonction de différentes valeurs de chaque bande. Après avoir sélectionné les paramètres optimums de l'algorithme, les performances des systèmes basés sur les autres bandes ont été évaluées. Le **tableau III.2** montre les résultats des tests dans les deux modes d'identification, ensemble ouvert et ensemble fermé.

À travers la comparaison entre les différentes méthodes, ainsi les résultats obtenus dans le **Tableau III.1** et le **Tableau III.2** On remarque que :

Dans l'ensemble ouvert (voir **figure III.4**), l'algorithme **DBN** est donné un résultat de **EER** moindre par rapport l'algorithme **RBM**. Ainsi que l'ensemble fermé (voire **figure III.5**) l'algorithme **DBN** montre un résultat du **RPR** et **ROR** mieux que le résultat qui donne par l'algorithme **RBM**.

Pour cela, on insérera la méthode DBN qui possède une très grande réputation au niveau de la reconnaissance de formes. Ainsi, pour une classification efficace des empreintes palmaires utilisées, nous avons utilisé le classificateur DBN recommandé.

III.6 Système multimodal

Le but de la multimodalité est d'amélioré le niveau de sécurité du système tel que le taux d'identification des modalités biométriques fusionnées soit supérieur au maximum des taux d'identification des modalités prises séparément. Ainsi, en utilisant deux bande différentes (NG. NIR pour palmaire) ainsi que les deux méthodes de classification (BRM et DBN), plusieurs systèmes multimodaux peuvent être exploités. Cependant, nous nous limitons, dans ces tests, aux trois scenarios, le multi-algorithmiques, le multi-échantillon et l'hybridation entre les deux scenarios. En utilisant les règles de fusion.

III.6.1 Systèmes multi-échantillons

Chaque personne dispose deux bande (deux modalités biométriques), par conséquence, la fusion de ces modalités permet d'obtenir un taux d'identification supérieur (au maximum) aux taux d'identification des mêmes modalités prises séparément. Dans notre méthodologie, la fusion au niveau des scores a été testée. Et, nous avons utilisé seulement deux combinaisons, une fois pour la méthode **DBN** et autre fois pour la méthode **RBM**. Les **Tableau III.3** et **Tableau III.4** montre les performances du système en utilisant les deux combinaisons sous les différentes règles de fusion avec les deux méthode (**RBM** et **DBN**).

DBN : NIR + NG									
Ensemble Ouvert									
SUM		**MUL**		**MIN**		**MAX**		**WHT**	
EER	T_0	EER	T_0	EER	T_0	EER	T_O	ERR	T_O
0	0.92	**0**	**0.85**	0.0003	0.89	0.007	0.97	0.0001	0.93
Ensemble Fermé									
SUM		**MUL**		**MIN**		**MAX**		**WHT**	
ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
99.96	2	99.96	2	99.96	2	99.40	5	99.96	2

Tableau III.3 : *Performance de système multi-échantillons basé sur la méthode(DBN)*

Après appliqué la fusion au niveau de score des bandes **NIR** et **NG** par l'algorithme **DBN** au système multi-échantillons. Le tableau au-dessus (**tableau III.3**) semble l'erreur **EER** en fonction de temp dans le mode ensemble ouvert, ainsi que le mode ensemble fermé montre le taux d'identification.

RBM : NIR + NG									
Ensemble Ouvert									
SUM		**MUL**		**MIN**		**MAX**		**WHT**	
EER	T_0	EER	T_0	EER	T_0	EER	T_O	ERR	T_O
0.05	0.83	**0.06**	**0.69**	0.088	0.78	0.076	0.88	0.062	0.82
Ensemble Fermé									
SUM		**MUL**		**MIN**		**MAX**		**WHT**	
ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
99.18	25	99.21	27	99.18	48	98.18	15	99.21	21

Tableau III.4 : *Performance de système multi-échantillons basé sur la méthode(RBM)*

On outre la fusion au niveau de score des bandes **NIR** et **NG** par l'algorithme **RBM** au système multi-échantillons. Le tableau au-dessus (**Tableau III.4**) semble ainsi l'erreur **EER** en fonction de temp dans le mode ensemble ouvert, ainsi que le mode ensemble fermé montre le taux d'identification.

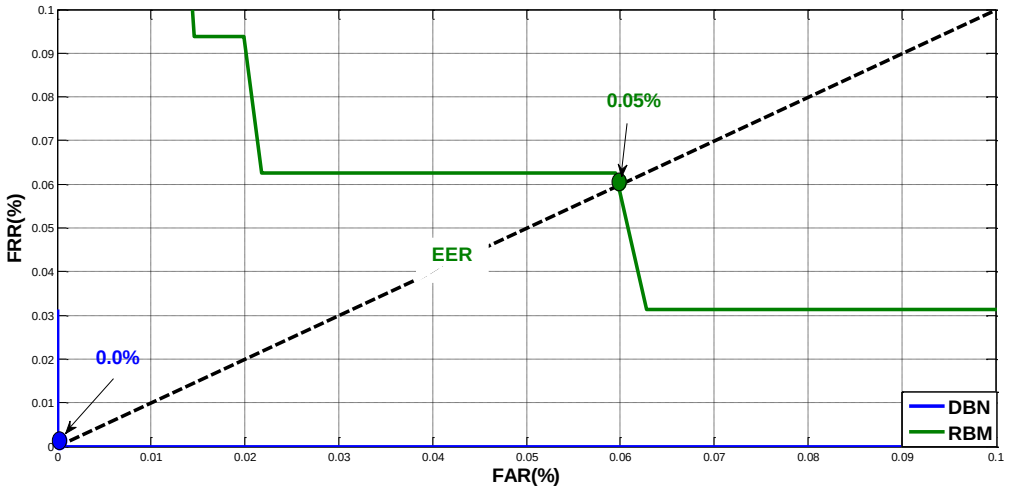

Figure III.8 : *performances des systèmes multi- échantillons ensemble ouvert*

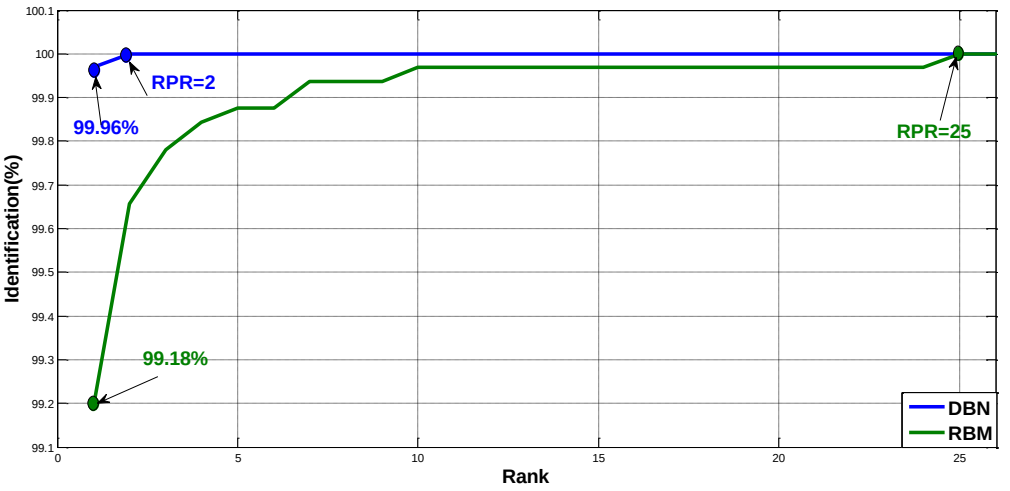

Figure III.9 : *performances des systèmes multi- échantillons ensemble fermé*

Discussion et analyse des résultats

Il est clair que la combinaison porte des améliorations considérables des performances par comparaison à celle offerte par le système unimodal. Cependant, cette fusion conduit à une erreur nulle (**EER = 0 %**) dans les deux cas des règles SUM et MUL par l'algorithme DBN. Ce résultat permet de confirmer l'efficacité de la fusion multimodale dans les systèmes d'identification biométrique.

Nous avons aussi testé les performances de la méthode DBN dans un système d'identification opérant en mode ensemble fermé. Dans le même Tableau sont représentées les performances d'un méthode DBN On constate sur ce tableau que pour la même combinaison,

le système donne le meilleur résultat avec un **ROR** égal à **99.96%** et un **RPR** égale à **2**et ceci avec règles SUM, MUL et MIN, WHT.

Dans la deuxième partie de cette section, nous allons exécuter une série des expériences pour examiner la performance de système multi-échantillons basé sur la méthode RBM. Dans le **tableau III.4**, on remarque une amélioration des résultats obtenus par rapport à ceux des systèmes unimodaux, Diminution un peu d'égalité d'erreur EER avec toutes les règles de la fusion utilisée (SUM, MUL, MIN et MAX) est très observée. A partir des résultats obtenus dans le **Tableau III.3** on remarque que dans le cas d'identification **ensemble ouvert**, la fusion entre deux bandes donne une valeur minimale d'erreur (EER) Alors que la meilleure erreur trouvée est (**0.06%**) avec la règle de fusion SUM. Dans le cas d'identification **ensemble fermé**, la meilleure valeur de **ROR** (**99.21%**) est obtenue avec les règle de fusion MUL et WHT.

À travers la comparaison entre les deux méthodes avec une fusion au niveau de score par le scenario multi-échantillons. Les résultats obtenus dans le **Tableau III.3** et le **Tableau III.4** On remarque que :

Dans l'ensemble ouvert (voir **figure III.8**), l'algorithme **DBN** est donné un résultat de **EER** moindre par rapport l'algorithme **RBM** dans tous les cas des règles. Ainsi que l'ensemble fermé (voire **figure III.9**) l'algorithme **DBN** montre un résultat du **RPR** et **ROR** mieux que le résultat qui donne par l'algorithme **RBM** et la performance de la méthode DBN est élevé comme il le montre la comparaison entre les deux tables.

La précision du système multimodal est meilleure que celle du système uni-modal dans les deux modes. Ces informations additionnelles aident au mieux de bien classifier cette méthode (DBN)

III.6.2 Système Multi-algorithmique

En vue d'améliorer en plus nos résultats, nous allons essayer de fusionner les différents scores des différentes méthode un système multimodal. De la même manière que précédemment, nous avons effectué la fusion entre les deux méthodes une fois pour la bande **NG** et autre fois pour la bande **NIR** comme indique les tableaux suivant et la **figure III.10** et **figure III.11.**

Mode	**Ensemble Ouvert**									
Règles	**SUM**		**MUL**		**MIN**		**MAX**		**WHT**	
	EER	T_0	EER	T_0	EER	T_0	EER	T_0	EER	T_0
NG (RBM.DBN)	0.031	0.83	0.031	0.70	0.031	0.80	0.04	0.89	0.031	0.83
NIR (RBM.DBN)	0	0.96	**0**	**0.93**	0.002	0.87	0.013	0.97	0.006	0.9
Mode	**Ensemble Fermé**									
Règles	**SUM**		**MUL**		**MIN**		**MAX**		**WHT**	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
NG (RBM.DBN)	99.59	21	99.59	21	99.65	37	98.93	17	**99.65**	**18**
NIR (RBM.DBN	99.96	2	99.96	2	99.84	8	98.65	4	**99.87**	**2**

Tableau III.5 : *Performance de système multi-algorithmique*

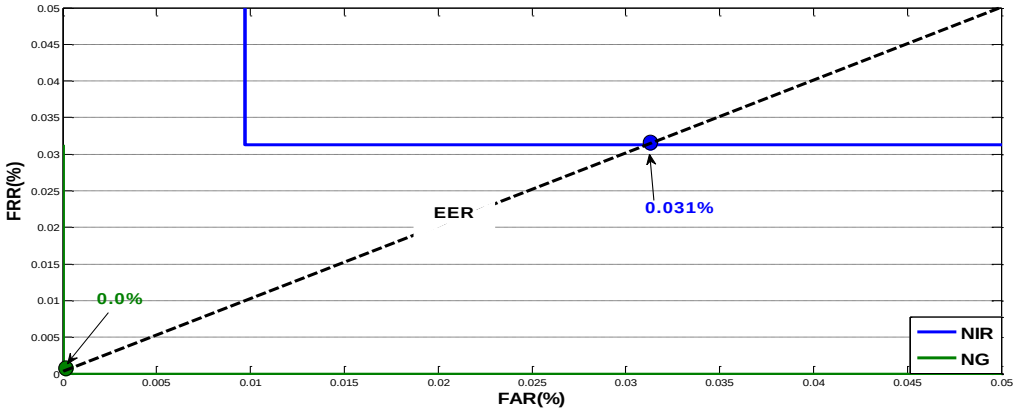

Figure III.10: *performances des systèmes multi- algorithmique ensemble ouvert*

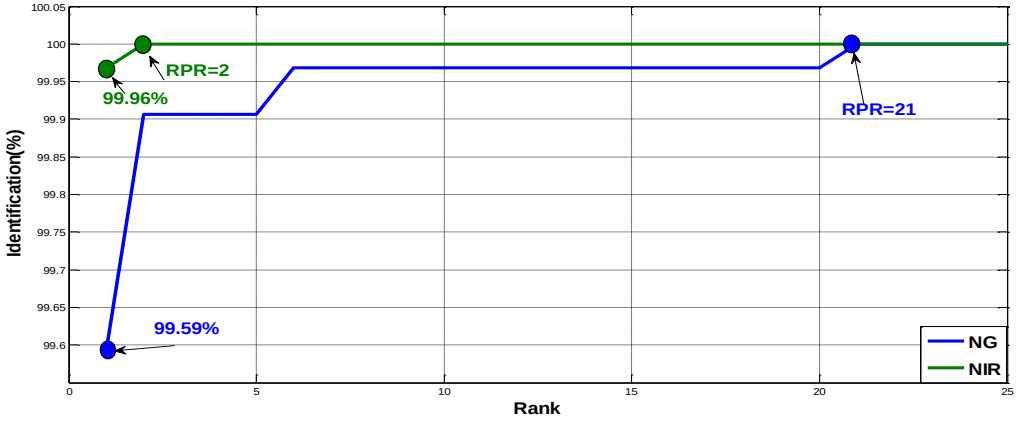

Figure III.11 : *performances des systèmes multi- algorithmique ensemble fermé*

Discussion et analyse des résultat

On est notée que la combinaison porte des améliorations considérables des performances par comparaison à celle offerte par le système unimodal. Ainsi que cette fusion conduit à une erreur nulle (**EER = 0 %**) dans les deux cas des règles SUM et MUL par la bande **NIR**. Par contre que la bande **NG** donne une erreur augment par rapport la bande **NIR**.

Nous avons aussi testé les performances de cette fusion dans un système d'identification opérant en mode ensemble fermé. Dans le même **Tableau III.5** sont représentées les performances d'un système multi-algorithmique. On constate sur ce tableau que pour la même combinaison, le système donne le meilleur résultat avec un **ROR**, **RPR** et ceci avec règle de WHT avec les deux bandes **NG** et **NIR**.

① **Pour la bande NG :** L'ensemble Ouvert noté que Le système donne le meilleur résultat avec un EER égal **0.031%** ceci avec tous les règle (SUM MUL MAX WHT). Ainsi que L'ensemble fermé montre que : Le système donne le meilleur résultat avec un ROR égal **99.59** ceci avec les règle (SUM, MUL). Cette bande possède la même résulta avec les règle (SUM.MUL) égal **ROR=99.59 RPR=21**

② **Pour la bande NIR :** L'ensemble Ouvert noté que Cette bande montre que la règle de fusion **SUM** et **MUL** donne des résultats parfaits **EER=0** Tandis que les autres règles donnent des résultats de **EER** entre **[0.002% ,0.013%].** On outre que L'ensemble fermé noté que Les résultats obtenus du **ROR** et du **RPR** sont très plausible et justifier ceux obtenus dans l'ensemble ouvert.

À travers la comparaison entre les deux méthodes avec une fusion au niveau de score par le scenario multi-algorithme. Les résultats obtenus dans le **Tableau III.6** On remarque que :

Dans l'ensemble ouvert (voir **figure III.10**), la bande **NIR** est donné un résultat de **EER** moindre par rapport la bande **NG** dans tous les cas des règles. Par contre que l'ensemble fermé (voire **figure III.11**) les deux bandes **NG** et **NIR** montre un résultat du **RPR** et **ROR** performant avec la règle **WHT**.

III.6.3 Système hybride

En combinant les systèmes multi-échantillon avec les systèmes multi algorithmiques. Ils permettent d'augmenter les performances de l'identification du point de vue taux d'identification. Dans le mode d'identification ensemble ouvert et fermé ouvert, le **tableau III.6**

présente les taux d'identification retenus pour les différents systèmes en respectant les différentes règles de fusion.

Hybride	**Ensemble Ouvert**									
	SUM		**MUL**		**MIN**		**MAX**		**WHT**	
	EER	T_0	EER	T_0	EER	T_0	EER	T_0	EER	T_0
	0.0006	**0.94**	0.0006	0.82	0.001	0.87	0.022	0.97	0.0007	0.93
Hybride	**Ensemble Fermé**									
	SUM		**MUL**		**MIN**		**MAX**		**WHT**	
	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR	ROR	RPR
	99.96	2	99.96	2	99.9	6	98.12	6	99.93	2

Tableau III.6 : *Performance de système hybride*

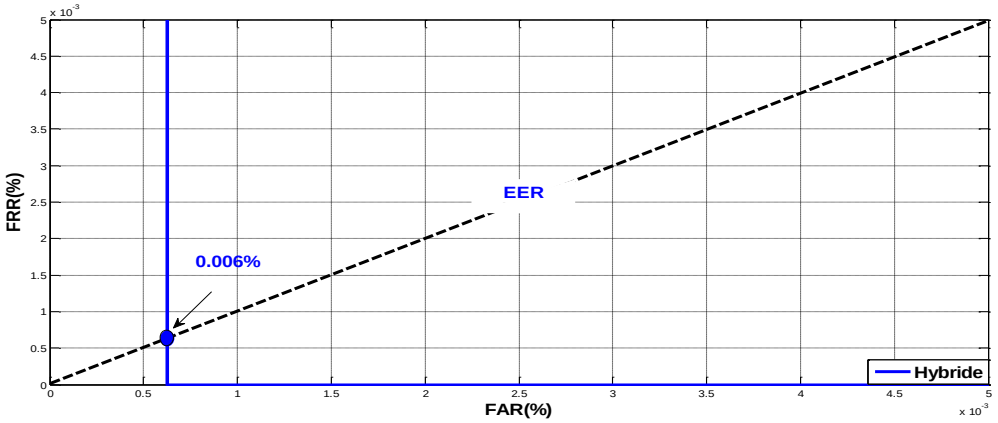

Figure III.12 : *performances des Hybride ensemble ouvert*

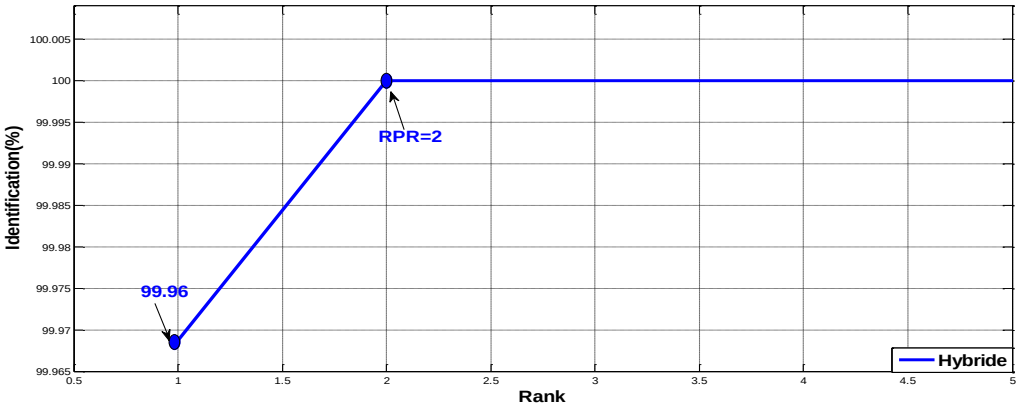

Figure III.13 : *performances des systèmes Hybride ensemble fermé*

Le **tableau III.6**, la **Figure III.12** et la **figure III.13**montre que les règle de fusion **SUM** et **MUL** donne un meilleur résulte par rapport les autres règles, soit avec l'ensemble ouvert (**EER = 0.0006%**), ou avec l'ensemble fermé (**ROR = 99.96%**). Tandis que les autres règles donnent des résultats de **EER** et **RPR** réductif (**EER=0.001, ROR=99.9**), MUL (**EER=0.022 ROR=98.12**), WHT (**EER=0.0007 ROR=99.93**)

III.7 Conclusion

Dans ce chapitre, les travaux biométriques présentés ont conduit à l'élaboration d'un système d'identification des personnes par reconnaissance d'empreintes palmaires. Pour ce faire, Nous avons proposé plusieurs systèmes biométriques. Outre le système uni modaux, nous avons exploré quelques systèmes multimodaux. Ces différents systèmes sont testés dans le but d'améliorer le taux d'identification des modalités dans les deux modes d'identification, ensemble ouvert et ensemble fermé. En validant ces systèmes sur une base de données de 400 personnes, nous avons dégagé une amélioration considérable du taux d'identification (99.96%).

Conclusion Générale

Conclusion générale

L'identification des individus par leurs empreintes palmaires (Palmprints), considérée comme nouveau membre de la famille des modalités biométriques, est devenue un domaine de recherche très actif durant ces dernières années. Les travaux réalisés, jusqu'à présent, se sont basés sur les techniques de représentation des images de Palmprints pour une meilleure classification.

Dans notre travail, nous nous sommes basés sur une démarche qui consiste à améliorer la performance de l'identification et vérification biométriques via l'empreinte palmaire par deux méthodes (RBM et DBN) avec ensembles d'opérations. Pour cela, nous avons fait la comparaison entre différentes méthodes d'extraction des caractéristiques, ce qui nous a permis d'en choisir celle qui est la mieux adaptée à notre problème. Suivant les résultats obtenus, nous avons opté pour le choix des méthodes RBM et DBN. Pour rendre notre système plus pratique avec ces deux algorithmes, nous avons utilisé le filtre Log-Gabor afin d'obtenir des vecteurs binaires suivi par une classification.

En fin, les résultats obtenus, sont très intéressants. En effet on est arrivé à un taux de reconnaissance idéal de 100 %, ce taux est très intéressant ce qui rend notre système fiable où il répond bien à l'objectif que nous nous sommes fixés au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus.

Notre futur travail est concentré sur l'évaluation de la performance dans les deux phases (vérification et identification) en utilisant une base de données de grande taille et de l'intégration d'autres traits biométriques pour obtenir les performances du système avec une grande précision.

Bibliographie

Bibliographie

[1] F.Perronnin, J. Dugelay, “An Introduction to Biometrics Audio and Video-Based Person Authentification ”. Volume 19 – n4,2002

[2] S.Boudjelial, " detection et identification d’individu par méthode biométrique ".UMMTO.2014

[3] M.Moulay, M.Arbaoui, "authentification des personnes par l’articulation du doigt "UNIVERSITE KASDI MERBAH OUARGLA.2015

[4] A.Murhula, " Conception et mise en place d'une plateforme de sécurisation par synthese et reconnaissance biométrique de documents de traffic ".

Polytechnique_INITELEMATIQUE_BURUNDI - Ingénieur Civil en Informatique et télécommunications 2015

[5] A.Meraoumia, "Modèle de Markov caché applique à la multi biométrie "USTHB. 2014

[6] A. Ross and A. K. Jain, "Information Fusion in Biometrics", Pattern Recognition Letters, Vol. 24, Issue 13, pp. 2115-2125, September, 2003.

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

[8] Y.Lee, K.Lee, Hyung keun Jee, Youn-Hee Gil, Woo-Yong Choi, Dosung Ahn, Sung Bum Pan, "Fusion for Multimodal Biometric Identification",5th International conference on Audio and video-based biometric person authentication-AVBPA, Hilton Rye Town, N.Y. USA, July 2005, pp. 1071-1079.

[9] S.Jidong, L.Xiaoming, "Fusion of Radar and AIS Data", 7th International Conference on Signal Processing-ICSP'04, Beijing, China, Vol.3, 2004, pp, 2604-2607.

[10] C.Berger ; M.Voltersen ; R.Eckardt ; Eberle, J. ; Heyer, T. ; Salepci, N. ; Hese, S. ; Schmullius,C. ; Tao, J. ; Auer, S. ; Bamler, R. ; Ewald, K. ; Gartley, M. ; Jacobson, J. ; Buswell, A. ; Du, Q. ;Pacifici, F., "Multi-Modal and Multi-Temporal Data Fusion", IEEE Journal

of Selected Topics in Applied Earth Observations and Remote Sensing, Jun 2013, Vol.6, N.3, pp.1324-1340

[11] Earprints, Forensic Evidence of. Dans: Encyclopedia of Biometrics. s.l.:Spring. 127, Champod, C., 2009.

[12] Forensic Applications, Overview. Dans: Encyclopedia of Biometrics. s.l.:Spring , Champod, C., 2009.

[13] P [Claus_Vielhauer]_Biometric_User_Authentication_for_IT_SECURITY Networked Society.

[14] Fedias Meriem., "Combinaisons de données d'espaces couleurs et de méthodes de vérification d‟identité pour l‟authentification de visages", Université Mohamed Khider – Biskra.

[15] DANG Hoang Vu., "Biométrie pour l‟Identification", Rapport final, Institut de la Francophonie pour l'Informatique, Hanoï, Vietnam, 07 – 2005.

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

[17] Alismail MohamedRaouf, Ourchani NorElhouda., "Fusion multimodale des scores pour la reconnaissancedes personnes", Université Mohamed Khider Biskra, 2011.

[18] Rose; Léo; Christelle., 'These-Romain-Giot-2012".

[19] Mébarka Belahcene., "Authentification et Identification en Biométrie", Université MohamedKhider – Biskra, 14 Janvier 2013.

[20] Amine Nait-Ali, Régis Fournier., "Traitement du signal et de l'image pour la biométrie", L'OUASIR, 2012.

[21] Melle Lorène ALLANO., "La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance", 2009.

[22] Hao, Anderson, and Daugman., "Combining crypto with biometrics efficiently", IEEE Transactions on Computers, 55, 2006.

[23] J. V. Kittler., "Combining classifiers A theoretical framework", IEEE Transactions on Pattern Analysis and Machine Intelligence, 1(1) :18–27, 1998.

[24] K. Nandakumar., "Integration of Multiple Cues in Biometric Systems", PhD thesis, Michigan State University, May 2005.

[25] Pierre Buyssens., "Fusion de différents modes de capture pour la reconnaissance du visage appliquée aux e transactions", Université de Caen Basse-Normandie, 2011.

[26] Boudjellal Sofiane., "Détection et identification de personne par méthode biométrique", Université Mouloud Mammeri de Tizi-Ouzou (UMMTO),

[27] T. Ojala, M. Pietikainen, and T. Maenpaa. Multiresolution., "gray-scale and rotation invariant texture classi_ cation with local binary patterns", IEEE Trans. PAMI, 24(7) :971_987, 2002.

[28] BETTAHAR Abdessettar, SABER Fathi., "Extraction des caractéristiques pour l'analyse biométrique d'un visage", UNIVERSITE KASDI MERBAH OUARGLA,2014.

[29] Nanni, L., Lumini, A., Brahnam, S.,"Local binary patterns variants as texture descriptors formedical image analysis", Artif. Intell. Med. 49(2), 117–125 (2010)

[30] V. Ojansivu and J. Heikkila., "Blur insensitive texture classification using local phase quantization", International Conference on Image and Signal Processing (ICISP08), pp. 236-243, 2008.

[31] J. Flusseret T. Suk.,"Degraded Image Analysis: An Invariant Approach. IEEE Trans", Pattern Analysis and Machine Intelligence, vol. 20, no. 590-603, 1998.

[32] Convolutional Deep Belief Networks for Scalable Unsupervised Learning of Hierarchical Representations

[33] C. Fiche. "Repousser les limites de l’identification faciale en contexte de vidéosurveillance". Docteur De L’université De Grenoble Spécialité : Signal - Images - Parole - Télécoms (SIPT), le 31/01/2012