République Algérienne Démocratique et Populaire
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
CENTRE UNIVERSITAIRE BELHADJ BOUCHAIB D'AÏN-TÉMOUCHENT

Institut des Sciences
Département des Mathématiques et de l'Informatique

MÉMOIRE

Pour l'obtention du Diplôme de Master en Informatique

Option : Réseaux et Ingénierie des Données (RID)

Présenté par :
Mme. Fatima Zohra AMARA

IDENTIFICATION BIOMÉTRIQUE PAR FUSION MULTIMODALE DE L'EMPREINTE DIGITALE

Encadrant :
Melle. Fatima BEDAD
Maitre Assistant "A" à C.U.B.B.A.T.

Soutenu en 2018

Devant le jury composé de :

Président :	M.BENOMAR Amine (M.C.B)	C.U.B.B.A.T.
Examinateurs :	Melle. BERRAKAM fatima (M.A.A)	C.U.B.B.A.T.
Encadrant :	Melle. Fatima BEDAD (M.A.A)	C.U.B.B.A.T.

Je dédie ce mémoire à ma famille
et à mes amis proches...

Remerciements

Je remercie tout d'abord Dieu le tout puissant et miséricordieux, qui nous a donné la force et la patience d'accomplir ce Modeste travail.

En second lieu, je remercie mon encadreur Mlle : BEDAD Fatima, son précieux conseil et son aide durant toute la période du travail.

Je souhaite remercier Dr BENOMAR Amine qui m'a fait l'honneur de présider le jury de cette mémoire. Je tiens aussi à remercier Dr MERAD BOUDIA Djalal pour avoir accepté d'examiner ce travail.

Je remercie très chaleureusement Dr Samia BENTAIEB pour son soutien sur le plan scientifique aussi bien que moral.

Je tiens à exprimer mes sincères remerciements à tous les professeurs qui m'a enseigné et qui par leurs compétences m'a soutenu dans la poursuite de mes études.

Les mots manquent pour remercier à leur juste valeur Jazia Bekradda et Meriem Ouafaa Bekkoucke pour leur énorme soutien.

Enfin, un très grand merci à toute ma famille qui m'a gratifié de son amour et fourni les motivations. Je leur adresse toute ma gratitude du fond du cœur.

Résumé :

Les systèmes biométriques unimodaux souffrent de plusieurs problèmes qui sont à l'origine de l'utilisation d'un seul trait biométrique susceptible au bruit, à la mauvaise capture, à la pauvreté en matière de points biométriques confidents et notamment à la détérioration de la qualité de l'entrée biométrique. L'introduction de systèmes biométriques multimodaux est une solution à ces problèmes.
Nous avons proposé un système d'authentification/identification automatique d'individus par instances multiples et répétées d'empreinte digitale, avec une fusion au niveau de score. Nous avons utilisé l'algorithme SURF pour l'extraction de caractéristiques, En profitant de sa robustesse grâces a l'invariabilité a l'échelle et à la rotation, de plus de sa rapidité.
Le processus de reconnaissance multimodal permet de renforcer les systèmes biométriques sur les plans de sécurité, fiabilité et pertinence. En effet. le taux de reconnaissance global pour la méthode proposée est de 100%, ce qui est beaucoup mieux que le système unimodale où le taux de reconnaissance est de 65%.

MOTS CLÈS :
reconnaissance,biométrie, fusion, multimodalité,SURF ,empreinte digitale.

Abstract :

The uni-modal biometric systems suffer from several problems which are due to
the origin of the use of a single biometric trait susceptible to noise, poor capture, poverty in terms of confidential biometric points and in particular the deterioration of the quality of the biometric entry. Introduction of biometric systems multi-modal is a solution to these problems.
We have proposed a system of authentication / identification automatic of individuals by multiple instances and repeated fingerprint, with a fusion at the score level.
We used SURF algorithm for the extraction of characteristics, taking advantage of its robustness thanks to the invariability, scale and the rotation, more of its speed.
The multi-modal recognition process makes it possible to strengthen the biometric systems under terms of security, reliability and relevance. Indeed, 100% were the overall recognition rate for the proposed method while the former mentioned system we're rated as 65%.

KEYWORDS :
recognition,biometrics, fusion, multimodality, SURF, fingerprint.

Table des matières

Table des figures

Liste des tableaux

Abreviation

CN :Crossing Number

Rank-1 RR : Rank-OneRecognition Rate

Rank-1 RR : Rank-OneRecognition Rate

CMC : Cumulative Match Characteristic

FAR : False Accept Rate

FRR : False Reject Rate

EER : Equal Error Rate

NMS : Non-Maximum Suppression

NN-DR :Nearest Neighbor Distance Ratio

VR@0.1FAR : Verification Rate at 0.1% FAR

ROC : Receiver Operating Characteristic

SVM : Support Vector Machine

SURF : Speeded-Up Robust Features

SIFT : Scale-Invariant FeatureTransform

LBP : Local Binary Pattern

FVC :Fingerprint Verification Competition

FFT :Transformée de Fourier Rapide

K-means :k-moyennes

Introduction génerale

Face à la fraude documentaire, au vol d'identité et nouvelles menaces telles que le terrorisme ou la cybercriminalité, de nouvelles solutions technologiques sont progressivement mises en œuvre. Parmi ces technologies : la biométrie.
Cette technologie s'est rapidement distinguée, car elle permet d'identifier et d'authentifier les personnes de manière fiable et rapide, en fonction de caractéristiques biologiques uniques.

La biométrie fait le lien entre identité physique et identité numérique d'une personne, permettant de réduire les risques de fraude à l'identité, elle facilite la vie des utilisateurs et offre une alternative simple aux mots de passe et aux codes PIN en matière d'authentification /identification en mesurant une de ses caractéristiques biométriques.

Il peut y avoir plusieurs types de caractéristiques biométriques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. D'autre part, ces caractéristiques sont loin d'être ni parfaites et ni précises, et l'on atteint très vite des limites pour ces techniques.

En effet, les systèmes biométriques mono-modaux souffrent de plusieurs problèmes qui les rendent inappropriés aux applications actuelles de la biométrie, exigeants de hauts degrés de fiabilité et de sécurité. Ces problèmes sont à l'origine de l'utilisation d'un seul trait biométrique susceptible au bruit, à la mauvaise capture, ou encore à la détérioration de la qualité de l'entrée biométrique. L'introduction de la biométrie multimodale s'avère une solution à ces problèmes.

L'objectif principal de notre travail est l'implementation d'un algorithme de reconnaissance par empreinte digitale assurant l'authentification/identification par instances répétées (plusieurs impressions du même doigt) et multiples (plusieurs doigts) d'empreintes digitales, afin de surmonter les limites de la modalité biométrique, en améliorant la précision de la reconnaissance, la vitesse de correspondance et la consommation de mémoire, en utilisant le descripteur SURF (Speeded Up Robust Feature) pour l'extraction des caractéristiques, avec une classification par le plus proche voisin et une fusion au niveau de score (score level).

Dans ce mémoire, nous allons essayer d'atteindre cet objectif à travers quatre chapitres, plusieurs notions et concepts de la biométrie et réalisation des systèmes de reconnaissance vont être abordés :
Dans le chapitre 1, nous allons mettre le point sur le concept et les bases de la reconnaissance automatique ainsi que sur les différentes modalités. Une étude détaillée d'un système biométrique uni-modal sera dressée, ainsi que ses domaines d'application, finaliser par ses limitations.
Le chapitre 2,est consacré à la fusion multi-modale. Dans ce chapitre plusieurs notions sur

la façon d'utiliser et de combiner plusieurs modalités seront abordées.
Dans le chapitre 3,Un résumé de travaux récents dans la reconnaissance biométrique par empreinte digitale sera présenté
Dans le chapitre 4, nous présenterons le processus général de la reconnaissance. Puis les résultats expérimentaux obtenus en analysent leurs performances .

Finalement, une conclusion générale est présentée, ainsi que quelques perspectives visées.

Chapitre 1

la Biometrie

1.1 Introduction

La biométrie est une technique qui permet d'établir l'identité d'une personne grâce à la reconnaissance automatique d'une ou de plusieurs caractéristiques biologiques et comportementales de cette personne préalablement enregistrées, telles que l'empreinte digitale, la signature, l'iris, la voix, le visage, la démarche [Firm, 1997] ...etc. Ces caractéristiques sont appelées « les modalités biométriques ».

Etymologiquement, le mot « biométrie » vient de la concaténation de deux termes grecs « bio » qui signifie la vie, et « metrie » qui se traduit par mesure [Gregory and Simon, 2008], c'est ainsi que John et al. [Woodward Jr et al., 2003] ont définit la biométrie comme « toutes caractéristiques physiques ou traits personnels automatiquement mesurables, robustes, et distinctives qui peuvent être utilisés pour identifier un individu ou pour vérifier l'identité prétendue d'un individu ».

Donc la biométrie représente ce que l'on est contrairement à ce que l'on possède (carte, badge, clé, etc.), ou ce que l'on sait (mot de passe, code PIN, etc.) permettant de surmonter les problèmes liés à ces deux derniers systèmes à savoir : la duplication, le vol, l'oubli, et la perte [Perronnin, 2002].

Ainsi, chaque caractéristique (physiologique et/ou comportementale) peut être considérée comme une modalité biométrique, si elle possède certaines propriétés bien déterminées [Newman, 2009; Maltoni et al., 2009].Elle doit être :

- Unique : généralement, deux personnes n'ont pas la même caractéristique
- performante : les caractéristiques ne doivent pas varier dans le temps
- Acceptable : l'acceptabilité du public lors de l'acquisition en tenant compte des conditions et contraintes de la capture de la modalité.
- mesurable : les caractéristiques doivent être facilement collectables et mesurables
- Universelle : elles existent chez tous les individus
- infalsifiables : impossible à dupliquer

Dans ce chapitre nous allons présenter une vue générale de la biométrie, Nous décrivons l'architecture d'un système biométrique ainsi que les technologies biométriques les plus courantes avec une comparaison entre elles, Nous présentons enfin les limitations des systèmes biométriques uni-modaux

1.2 Applications de la biométrie :

La biométrie est devenue un des thèmes de recherche les plus actifs dans le domaine de la vision par ordinateur, et de la reconnaissance des formes. Les applications biométriques

sont nombreuses et permettent de gérer l'accès à des ressources physiques tel que le contrôle des frontières dans les aéroports.

Le contrôle d'accès logique, tel que le commerce électronique, est un domaine d'application majeur de la biométrie.

La biométrie joue un rôle clé dans la sécurité publique et l'identification des personnes recherchées. L'utilisation des empreintes digitales comme système d'identification des suspects lors d'une enquête criminelle fut l'une des premières applications de la biométrie [Perronnin, 2002].
À noter qu'en Algérie, une base de données nationale et centralisée pour les empreintes et autres informations personnelles et techniques des citoyens a été créée. Le passeport biométrique informatisé (autrement appelé : e-passeport) contient un module électronique qui renferme des informations sur le titulaire du passeport. La puce en question utilise la technologie RFID (Radio Frequency IDentification). Plus de 12 millions de passeports et 7 millions de cartes d'identité biométriques ont été remis depuis le lancement de l'opération. [1]
Les premiers permis de conduire biométriques ont été mis en circulation à partir de la fin du mois de janvier 2018.

1.3 Fonctionnement des systèmes biométriques

Un système biométrique peut être un système d'identification (reconnaissance) ou un système d'authentification (vérification) [Mohammed, 2010], qui sont définis comme suit :

1.3.1 L'identification

L'identification effectue un appariement d'un à plusieurs (1 : N) entre un nouvel échantillon biométrique capturé, et les modèles biométriques stockés dans une base de données biométrique afin de tenter de déterminer l'identité d'une personne inconnue.

1.3.2 L'authentification

L'authentification effectue une correspondance un à un (1 : 1) entre un nouvel échantillon biométrique capturé, et un modèle biométrique spécifique stocké dans une base de données biométrique, pour tenter de vérifier que la personne est bien la personne qu'elle prétend être.

1. http ://www.aps.dz/algerie/67632-plus-de-12-millions-de-passeports-et-7-millions-de-cartes-didentite- biometriques-delivres-bedoui.

1.3.3 l'enrôlement

Les systèmes identification/authentification comprennent deux phases principales comme le montre la Figure 1.1 : l'enrôlement ou l'apprentissage et la reconnaissance. La phase enrôlement est commune à l'authentification et l'identification. C'est une phase préliminaire de tout système biométrique qui se fait off-line. L'enrôlement consiste à représenter les caractéristiques physiques ou comportementales d'un utilisateur dit "référence" sous forme d'un modèle biométrique appelé "signature" puis enregistrer ses informations dans une base de données.

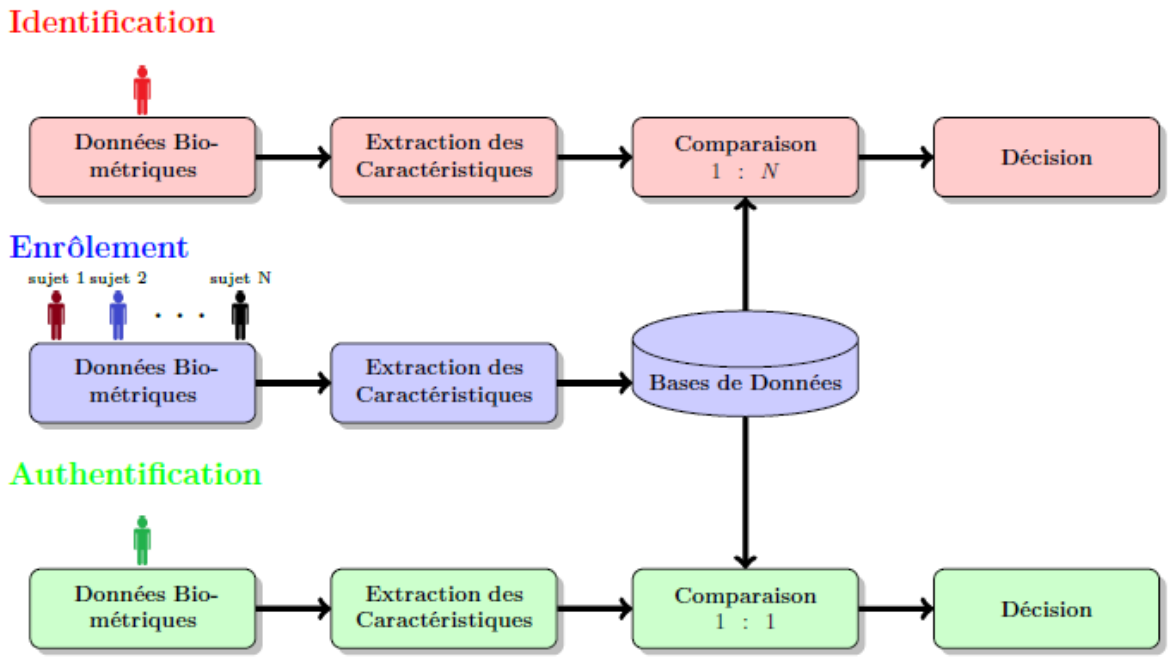

FIGURE 1.1 – Structure des systèmes biométriques.

1.4 Principaux Modules d'un Système biométrique

Un système biométrique comprend 4 modules dont certains sont communs à la phase d'enrôlement et à celle d'authentification/identification : l'acquisition, l'extraction des caractéristiques, la comparaison et la décision [YADDADEN, 2010].

1.4.1 Le module de capture :

sert a faire une mesure de la caractéristique biométrique en se servant d'un capteur

1.4.2 Le module d'extraction de caractéristiques :

:pour Extraire les traits fondamentaux et les caractéristiques des données acquises, en permettant d'obtenir une signature biométrique de l'individu, généralement sous forme d'un vecteur.

1.4.3 Le module de correspondance :

compare le vecteur de caractéristique avec le modèle enregistré dans la base de données du système et détermine le degré de similitude entre les deux.

1.4.4 Le module de décision :

Le module de décision sert ensuite à prendre une décision à partir de la sortie du module de comparaison qui correspond à un score de similarité entre les deux signatures .

1.5 Les modalités biométriques

On distingue trois catégories de technologies biométriques : les mesures morphologiques,les mesures biologiques, et les mesures comportementales.

1.5.1 Les mesures morphologiques

sont les modalités qui utilisent une partie du corps humain, ont l'avantage d'être stables dans la vie d'un individu. Ce sont surtout les empreintes digitales, la forme de la main, du doigt, le réseau veineux, l'œil (iris et rétine), ou encore la forme du visage.

1. **Empreintes digitales** Une signature que nous laissons derrière nous à chaque fois que nous touchons un objet [Firm, 1997] C'est le dessin formé par les lignes de la peau des doigts, et composé de lignes localement parallèles constituant un motif unique, universel et permanant. Même les vrais jumeaux ont des empreintes digitales différentes.

   Les crêtes sont les lignes en contact avec une surface au touché et les vallées sont les creux entre deux crêtes [Belguechi, 2015].

   A l'intérieur de ce motif, il y a un très grand nombre d'éléments qui nous différencient les uns des autres. Ces caractéristiques sont formées par le flux des crêtes formant l'empreinte. La figure 1.2 illustre un exemple de ces caractéristiques [Belguechi, 2015].

FIGURE 1.2 – Quelques caractéristiques des empreintes digitales.

Ces éléments sont à leur tour découplés en deux familles : les minuties et les singularités.

La minutie est un point qui se situe sur le changement de continuité des lignes papillaires. En effet, une strie peut bifurquer (la minutie s'appelle alors la bifurcation), s'arrêter soudainement (on parle alors de la terminaison), se déchirer au milieu pour former une sorte de trou (c'est le lac)... La figure 1.3 illustre les différents types de minuties

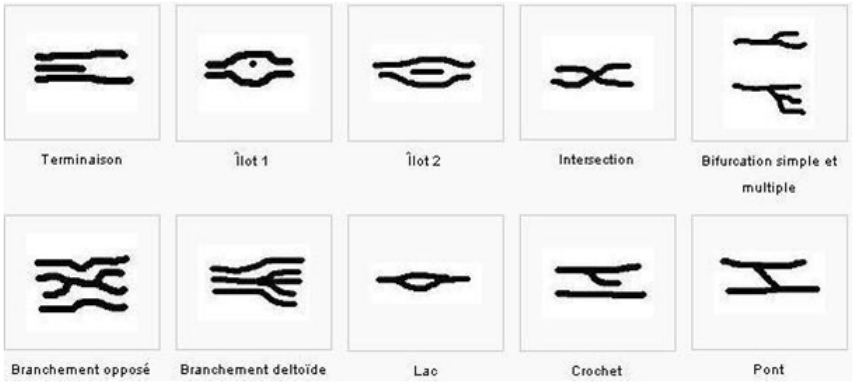

FIGURE 1.3 – les différents types de minuties.

En différencie deux points de singularités (voir figure 1.4) le core et le delta. Le core est le point de courbure maximale. Le delta est localisé à la confluence de trois différentes crêtes.

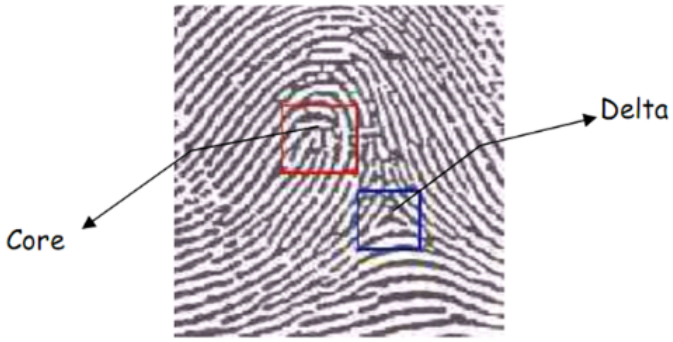

FIGURE 1.4 – les singularités dans une empreinte.

Selon le nombre et la localisation des points delta et core, nous pouvons regrouper les empreintes en trois catégories principales comme le montre la figure 1.5

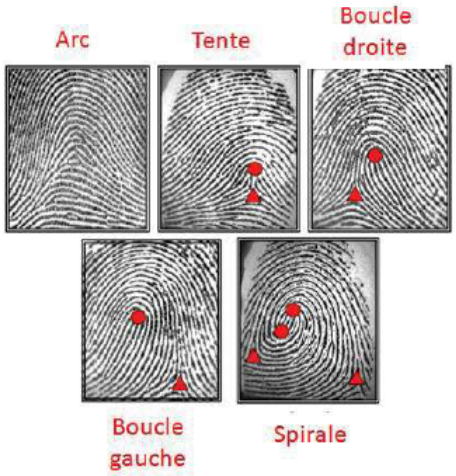

FIGURE 1.5 – Différents types d'empreintes digitales.

- Les arcs ou les tentes.
- Les boucles à droite ou à gauche (loop).
- Les spirales (whorl).

Nous pouvons observer d'autres caractéristiques en haute résolution qui sont hautement discriminées, à savoir les pores, comme le montre le figure 1.6

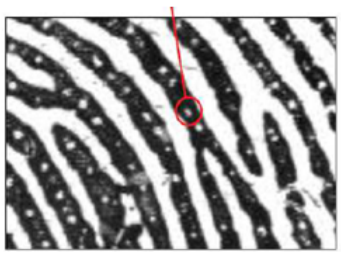

FIGURE 1.6 – les pores de la peau.

Les caractéristiques visible sur une grande résolution de 1000 dpi : les pores de la peau.

L'empreinte digitale est une modalité biométrique populaire qui est largement utilisée dans de nombreuses applications pour l'authentification des personnes. Elle offre une haute diversité et une performance acceptable [Chouaib, 2014].

2. **Visage (reconnaissance faciale)**

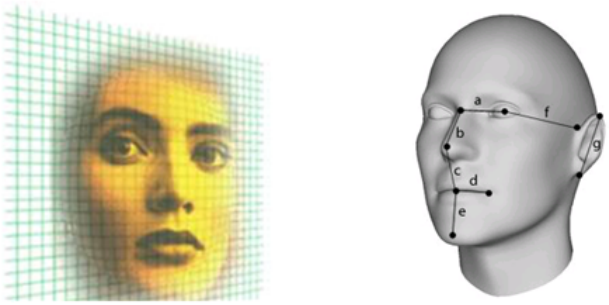

FIGURE 1.7 – Reconnaissance faciale.

Les systèmes de reconnaissance faciale sont des systèmes automatisés capables d'identifier des individus en fonction des caractéristiques de leur visage telles que l'écartement des yeux, des arêtes du nez, des commissures des lèvres, des oreilles, menton, etc.
Cette méthode doit pouvoir tenir compte de certains changements de la physionomie (lunettes, barbe, chirurgie esthétique) et de l'environnement (conditions d'éclairage, variation de pose et d'expression). Il est impossible de différencier deux jumeaux [BENTAIEB, 2018].
La reconnaissance du visage est utilisée comme système de surveillance ou d'identification par les autorités ou les corps policiers principalement dans les lieux publics, tel que les aéroports. Elle est parmi les techniques les plus acceptables, mais elle nécessite un arrière plan simple et fixe pour que le résultat soit précis [Jain et al., 2006].

3. **La reconnaissance de l'iris**

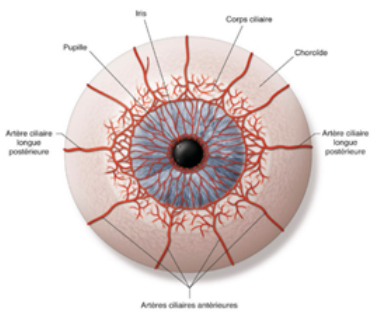

FIGURE 1.8 – Reconnaissance de l'iris .

La biométrie par l'iris est plus récente mais offre l'avantage d'être beaucoup plus fiable. Elle occupe actuellement plus de 10% du marché [Nadia, 2009]. L'iris est la zone colorée située entre le blanc de l'œil et la pupille [DJILI, 2016], c'est le seul organe interne humain visible de l'extérieur, qui se compose de vaisseaux sanguins disposés différemment d'un individu à un autre. Chaque œil est unique et stable durant la vie d'une personne.
Une fois que l'image de la configuration des vaisseaux sanguins est obtenue par le système biométrique, le fonctionnement est quasi identique à celui du système analysant l'empreinte digitale. La grosseur des vaisseaux, leur positionnement et les bifurcations qui les caractérisent font partie des éléments, les minuties.
Le point faible de ce type de système utilisant l'œil à des fins d'authentification/identification ou de vérification est qu'il éprouve beaucoup de difficultés à lire l'image de l'œil d'une personne aveugle ou d'un individu ayant un problème de cataracte [BENCHENNANE, 2015].

4. **La reconnaissance de la rétine :**

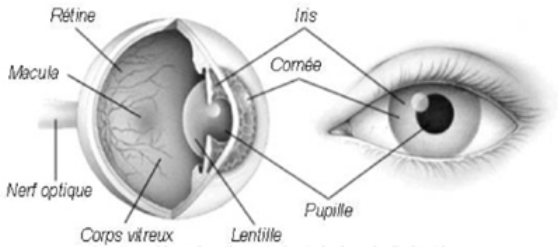

FIGURE 1.9 – Reconnaissance de la retine .

La rétine est située dans le fond de l'œil. Elle est la paroi interne qui reflète les images que nous percevons. Cette paroi très mince est tapissée par une multitude de vaisseaux sanguins (dit réseau veineux rétinien).
La disposition de ces veines est stable et unique.
La biométrie par la rétine procure également, un haut niveau en matière de reconnaissance. Cette technologie est bien adaptée pour des applications de haute sécurité (sites militaires et nucléaires, salles de coffres forts, etc.), mais parfois considérée comme intrusive à cause de l'acquisition qui se fait assez proche de l'œil.
En outre, hormis son coût élevé, les risques pour la santé ne seraient pas nuls, ce qui en limite d'autant son déploiement dans le secteur privé.
Enfin, l'exposition de la rétine aux blessures est beaucoup plus faible comparativement à toute autre partie du corps en contact direct avec l'extérieur [BENCHENNANE, 2015].

5. **Géométrie de la main**

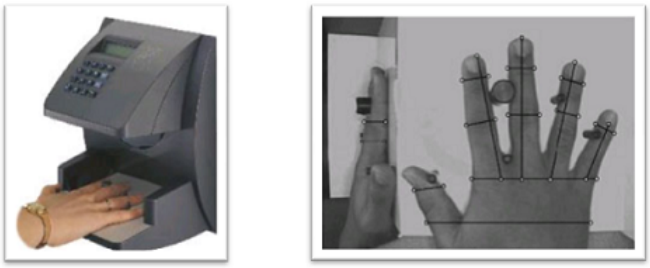

FIGURE 1.10 – Géométrie de la main .

La biométrie par la forme de la main est simple à mettre en œuvre, elle est très bien acceptée. L'utilisateur place sa main sur une platine possédant des guides pour positionner les doigts.
Le système prend une photo de la main et examine les caractéristiques, y compris la forme tridimensionnelle de la main, de la longueur et de la largeur des doigts et de la forme des articulations [Sanchez-Reillo et al., 2000].
Les blessures, l'humidité et la propreté des doigts n'affectent pas le contrôle.
Les fichiers gabarit présentent en outre l'avantage d'être de taille réduite (une dizaine d'octets).
Mais elle a un faible pouvoir discriminant et les systèmes peuvent être facilement trompés par de vrais jumeaux ou même par des personnes de la même famille, elle est toutefois sujette aux modifications de la forme de la main liées au vieillissement[GHACHOUA, 2017]

1.5.2 Les mesures biologiques

En matière de mesures biologiques, on trouve le plus souvent l'ADN, le sang, la salive, ou l'urine utilisés dans le domaine médical, pour des investigations criminelles ou même dans le domaine du sport pour des contrôles de dopage.

(a) **Analyse de l'ADN**

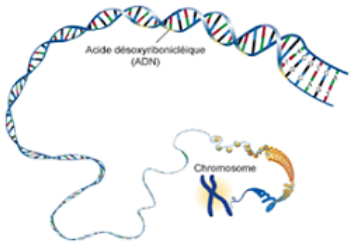

FIGURE 1.11 – Exemple de l'ADN .

L'analyse des empreintes génétiques est la façon la plus précise pour déterminer l'identité d'une personne, issue directement de l'évolution de la biologie molé-

culaire. Il est impossible de trouver deux personnes qui ont le même ADN car aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'acide désoxyribonucléique (ADN).

1.5.3 Les mesures comportementales

Contrairement à la biométrie physiologique (caractéristiques physiques figées), cette biométrie est liée à des caractéristiques comportementales dynamiques.
Les caractéristiques comportementales quant à elles sont directement liées à la façon d'agir de la personne. Elle concerne l'étude des actions répétitives et usuelles des personnes.
Les traits les plus répandues sont la reconnaissance vocale, la dynamique des signatures, la dynamique de frappe au clavier d'un ordinateur, la façon d'utiliser des objets, la démarche, le bruit des pas, la gestuelle [YADDADEN, 2010].

(a) **La dynamique de la frappe (au clavier)**

FIGURE 1.12 – La dynamique de la frappe.

La dynamique de la frappe est propre à chaque individu. Il s'agit en quelque sorte de la graphologie des temps modernes, car nous écrivons plus souvent avec un clavier qu'avec un stylo.
Les éléments analysés sont : la vitesse de la frappe, la suite de lettres, le temps de frappe, les pauses.[Giot et al., 2012].

(b) **La signature dynamique**

FIGURE 1.13 – La signature dynamique.

La vérification d'identité par la signature manuscrite devient très importante, vu l'utilisation répandue et la grande acceptabilité de cette modalité. Ce système inclue habituellement un crayon lecteur et une tablette à digitaliser.
Il ya plusieurs systèmes concurrents dans ce domaine analysant les caractéristiques spécifiques d'une signature comme la précision géométrique, l'inclinaison du stylo, la vitesse et l'accélération de l'écriture, la pression exercée, le nombre de fois que le stylo soi soulevé, le temps écoulé entre deux lettres..., etc.
Ces informations sont stockées sous forme de fichier pour être comparées lors de la reconnaissance. Certains systèmes ne font qu'enregistrer l'image statique de la signature pour comparaison [Toufik, 2016].

Le tableau suivant résume les avantages et les Inconvénients de tout les modalités décrite précédemment[BENCHENNANE, 2015] :

TABLE 1.1 – Avantages et inconvénients des technologies biométriques.

Modalité	Avantages	Inconvénients
Empreinte digitale	• Faible coût • Petite taille du lecteur • facilité de mise en place	• mauvaise réputation (aspects criminels) • possibilité d'attaque (rémanence de l'empreinte....)
Visage	• bonne acceptabilité •(peu intrusive), • pas de contact physique. • utilisation facile.	• vulnérabilité aux attaques • Sensibilité à la variation de l'éclairage •moins efficaces si les expressions du visage varient
Iris	• Grande quantité d'information. • haute presision	• Acceptabilité très faible • contrainte d'éclairage
Retine	• C'est une modalité caché , donc elle est peu exposée aux blessures (coupure, brûlure) • Plus précise • Invariant par rapport au temps • impossible à imiter(Haute sécurité.)	• Système intrusif ,L'œil est un organe sensible, acceptabilité faible • Coût plus important que d'autres technologies •installation difficile
la Géométrie de la main	• Le résultat est indépendant de l'humidité et de l'état de propreté des doigts. • Simplicité d'utilisation • bonne acceptabilité	• Système encombrant • La non unicité pour des jumeaux ou des membres d'une même famille.
ADN	• ADN a une très grande précision. • Il est standardisé	• Lente pour obtenir les résultats • cout important.
la dynamique de la frappe	•Non intrusif. • geste naturel pour un individu •Permet d'identifier une personne , à distance à partir de son ordinateur.	• Dépend de l'état (physique, émotion, fatigue...). Sensibilité à la différence entre les claviers
La signature dynamique	• technique qui repose sur un geste « naturel » facile à faire .	• La signature n'est pas parfaitement reproductible, elle est susceptible d'être affectée par l'état émotionnel de l'individu, notamment la fatigue.

1.6 Comparaison entre les modalités biométriques

Le choix d'une caractéristique biométrique est trés délicat car chacune d'elles possède ses avantages et ses inconvénients, le Groupe International de la Biométrie IBG (International Biometric Group) a procédé à une comparaison des différentes technologies biométriques appelée Analyse Zéphyr. Les résultats de cette comparaison sont illustrés sur la figure 1.14. Cette comparaison est basée sur quatre (04) critères principaux [Mohammed, 2010]

(a) **l'effort (Effort) :** l'effort fourni par l'utilisateur lors de la vérification par le système biométrique.

(b) **l'intrusion (Intrusiveness) :** niveau de l'acceptation du test par l'utilisateur.

(c) **le coût (Cost) :** coût de la technologie (capteurs, lecteurs...).

(d) **la précision (Accuracy) :** efficacité de la méthode.

L'exemple le plus explicite est l'utilisation de l'iris, ses avantages est sa précision et sa fiabilité ,par contre le capteur utilisé pour son acquisition est très couteux et son utilisation occasionne une certaine gène à l'utilisateur dans la mesure ou' il doit se tenir à une certaine distance du capteur afin que ce dernier puisse prendre une mesure de bonne qualité. Il est donc important de souligner que le choix d'une caractéristique biométrique est régi par plusieurs paramètres dont il faut impérativement tenir compte afin d'avoir un bon compromis qualité/prix.

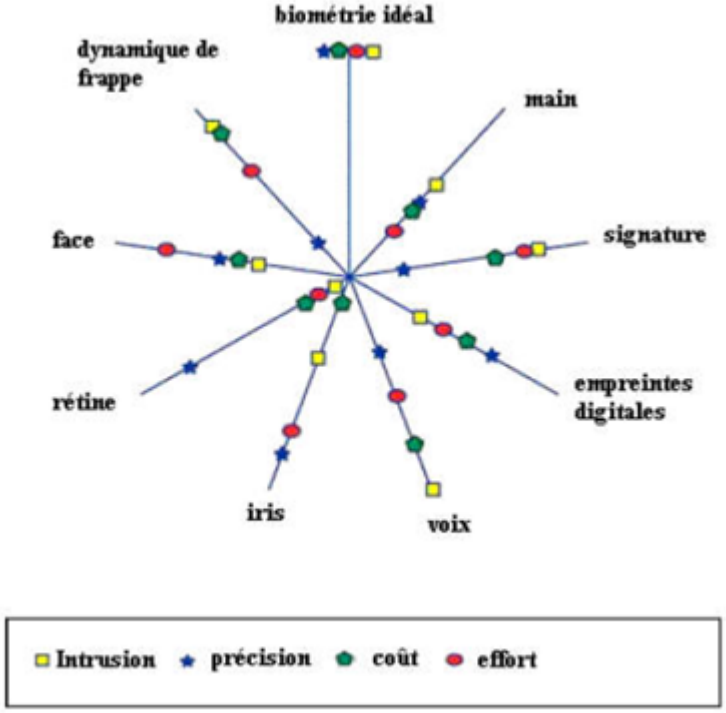

FIGURE 1.14 – Comparaison de différentes modalité biométrique.

1.7 Les limitations des systèmes biométriques unimodaux

Malgré les avantages des systèmes biométriques uni-modaux par rapport aux systèmes traditionnels, leur utilisation souffre de plusieurs limitations qui peuvent dégrader considérablement leur fonctionnalité et intérêt. En effet, ces systèmes sont souvent affectés par les problèmes suivants :

(a) **La non-universalité des biométries** signifie que certaines modalités biométriques ne peuvent pas être utilisées par une certaine catégorie de la population. Par exemple certaines personnes ont des empreintes digitales contenant trop peu d'information pour servir de moyen d'identification. Le NIST (National Institute of Standards and Technology) a publié dans une étude qu'environ 2% de la population ne peut pas utiliser l'empreinte digitale comme moyen d'identification.

De la même manière, des personnes souffrant d'anormalités des yeux ou de maladies oculaires ne peuvent fournir des images d'iris, ou de rétine, de bonne qualité pour une reconnaissance automatique
Pour toutes ces personnes, certains systèmes biométriques ne sont pas accessibles et ceci risque alors de les exclure de certaines utilisations si aucune alternative ne leur est proposée [Mohammed, 2010].

(b) **La variabilité lors de la capture**

La déformation physique lors de la capture signifie que 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.
Ces variations peuvent être dues

- à une mauvaise interaction de l'utilisateur avec le capteur (changements de pose)
- à l'utilisation de différents capteurs.
- à des changements de conditions de l'environnement ambiant (tel que l'éclairage, le bruit ...)
- ou encore à des changements inhérents à la modalité biométrique (apparition de rides, présence de cheveux, présence de cicatrices, etc.)

(c) **La sensibilité aux attaques**

Une autre limitation des systèmes biométriques est la sensibilité aux attaques (possibilité de fraude).
Il est possible de reproduire certaines modalités biométriques, comme la reproduction d'une signature ou l'imitation de la voix d'une personne ou même la fabrication de fausses empreintes digitales en gomme et de les utiliser pour contrer un système biométrique. (Les modalités biométriques comportementales sont plus sensibles à ce genre d'attaque)

(d) **La non-unicité des biométries**

C'est la variabilité entre les modalités de plusieurs Individus. Cependant, les caractéristiques extraites à partir de données biométriques d'individus différents peuvent être relativement semblable. Par exemple, une certaine partie de la population peut avoir une apparence faciale pratiquement identique due à des facteurs génétiques (ex : père et fils, vrais jumeaux). Ce manque d'unicité accroît le taux d'erreur d'un système biométrique (accepter des personnes non enregistrées dans la base des données) [BENAGGA Abderahmane, 2016].

1.8 Conclusion

Les quelques notions et définitions de base liées à la biométrie abordées dans ce chapitre montrent des inconvénients dans les systèmes uni-modaux.
Pour éviter ces inconvénients l'utilisation de plusieurs modalités biométriques au sein d'un même système (système biométrique multimodal) est la meilleure solution.
Dans le chapitre suivant nous allons présenter le système multimodal .

Chapitre 2

les systèmes biométriques multimodaux

2.1 Introduction

La multimodalité est l'utilisation de plusieurs systèmes biométriques au sein d'un même système. La combinaison de plusieurs systèmes a pour objectif de diminuer les limitations vues au système monomodal.

En effet, l'utilisation de plusieurs systèmes a pour but d'abord d'améliorer les performances de reconnaissance. En augmentant la quantité d'informations discriminante de chaque personne, on augmente le pouvoir de reconnaissance du système.

De plus, le fait d'utiliser plusieurs modalités biométriques réduit le risque d'impossibilité d'enregistrement et augmente la robustesse aux fraudes.

Alors, les Systèmes biométriques multimodaux sont ceux qui utilisent plusieurs caractéristiques physiologiques ou comportementales pour inscription, vérification ou identification [DJILI, 2016].

Nous exposerons d'abord les différentes formes de multi modalité possibles, et les niveaux de fusion puis les bases de données multimodales existantes, et enfin, les métriques utilisées pour évaluer les performances d'un système biométrique

2.2 Différentes formes de multi-modalité

On peut différencier 5 types de systèmes multimodaux selon les systèmes qu'ils combinent (Figure 2.7).

2.2.1 Multi-capteurs :

lorsqu'ils associent plusieurs capteurs pour acquérir la même modalité, par exemple un capteur optique et un capteur capacitif pour l'acquisition de l'empreinte digitale [Marcialis and Roli, 2004].

2.2.2 Multi-instances :

Lorsqu'ils associent plusieurs instances différents de la même modalité, par exemple deux empreintes de l'articulation de doigt différents [AlMahafzah et al., 2012] ,ou les deux iris (droite + gauche). Dans ce cas les données sont traitées par le même algorithme mais nécessitent des références différentes à l'enregistrement.

2.2.3 Multi-algorithmes :

Dans ce genre de système plusieurs algorithmes sont utilisés, dans la phase d'extraction de caractéristiques et/ou dans la phase de la mise en comparaison pour traiter la même la même image acquise, exemple l'utilisation des algorithmes pour analyser la texture et les minuties de l'empreinte digitale afin d'extraire des caractéristiques pouvant améliorer la performance du système [Ross and Jain, 2003].

2.2.4 Multi-echantillons :

il s'agit d'utiliser un seul capteur pour extraire des échantillons du même caractère biométrique, afin d'obtenir plusieurs variations de ce trait en enrichissant le modèle biométrique de l'individu. Par exemple l'acquisition de plusieurs images de visage en changeant la pose, l'expression, et/ou l'illumination, ou plusieurs images de d'empreinte digitale comme [Cheng et al., 2011].

2.2.5 Multi-biometries :

lorsque l'on combine différents traits biométriques d'un individu par exemple le visage et l'iris, le visage et l'empreinte digitale etc [DJILI, 2016],[Ross et al., 2006].

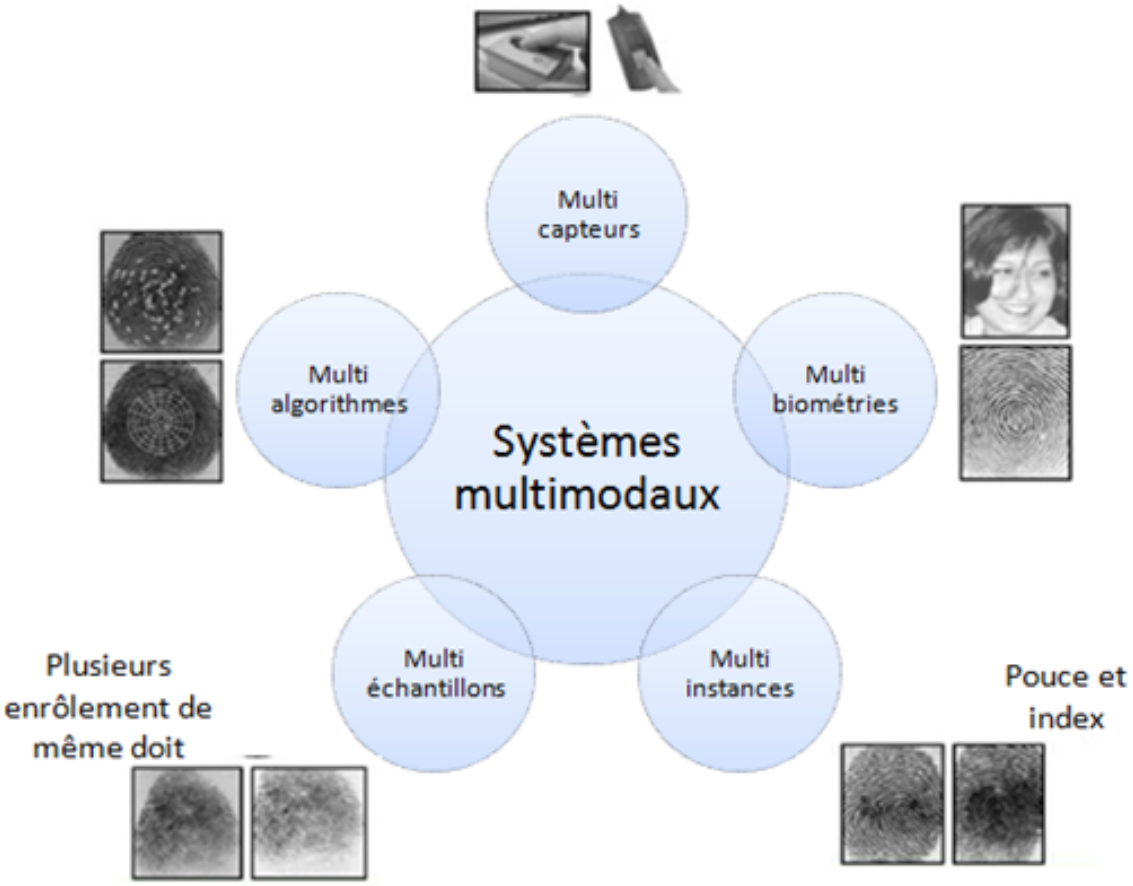

FIGURE 2.1 – les différents systèmes biométriques multimodales.

2.3 Niveau de Fusion

La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents : au niveau des données, au niveau des caractéristiques extraites, au niveau des scores issus du module de comparaison ou au niveau des décisions. comme montre la Figure 2.2

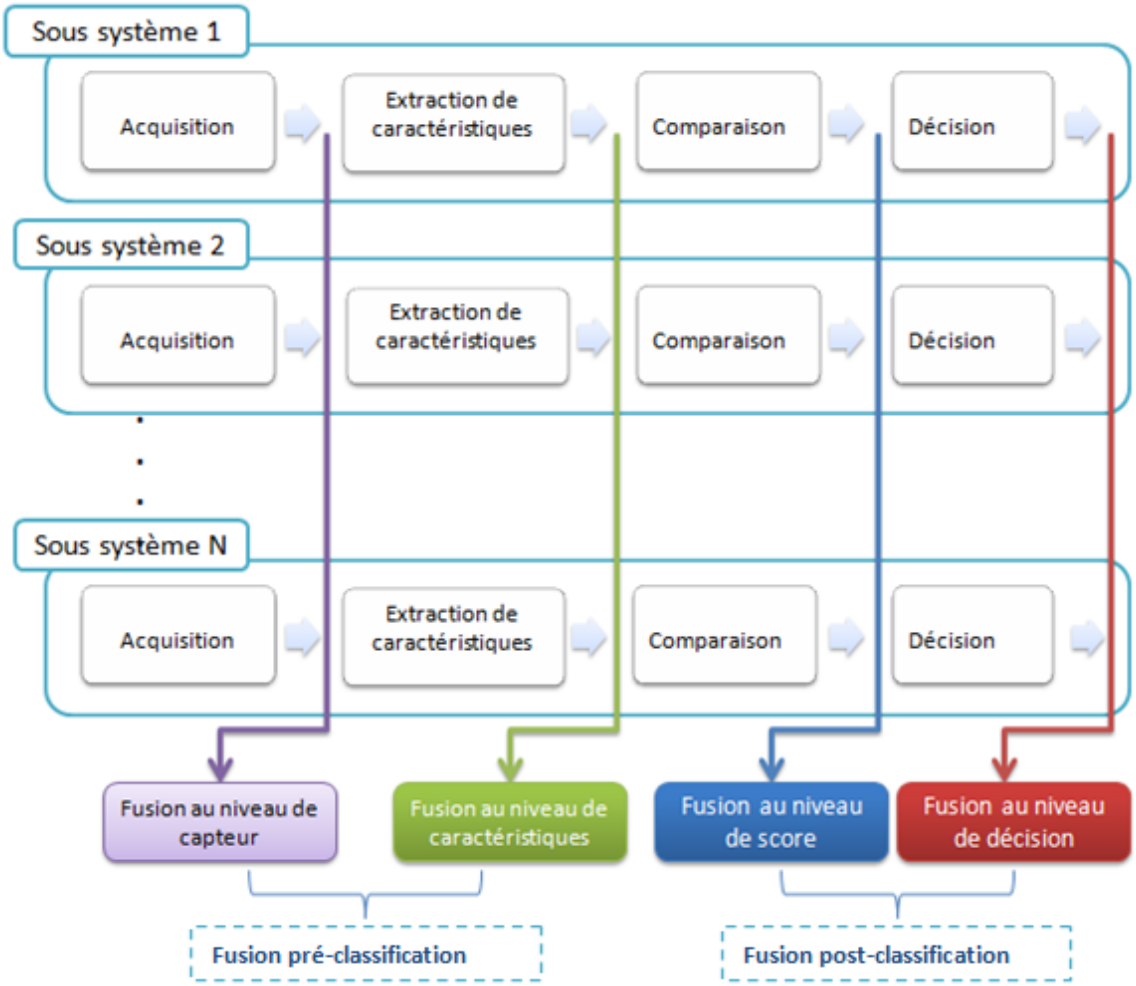

FIGURE 2.2 – les différents niveaux de la fusion.

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) [Sanderson and Paliwal, 2002].

2.3.1 La fusion pré-classification

La fusion pré-classification correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques [Allano, 2009].

Niveau de capteur(Sensor Level) Il s'agit ici de fusionner les données brutes ("raw data") qui proviennent de plusieurs capteurs * pour obtenir une nouvelle donnée de même trait biométrique. Ce type de fusion est peu utilisé car il nécessite une homogénéité des informations acquises [Iyengar et al., 1995].

il y a deux méthodes principales pour y parvenir : la sommation pondérée et la construction en mosaïque.

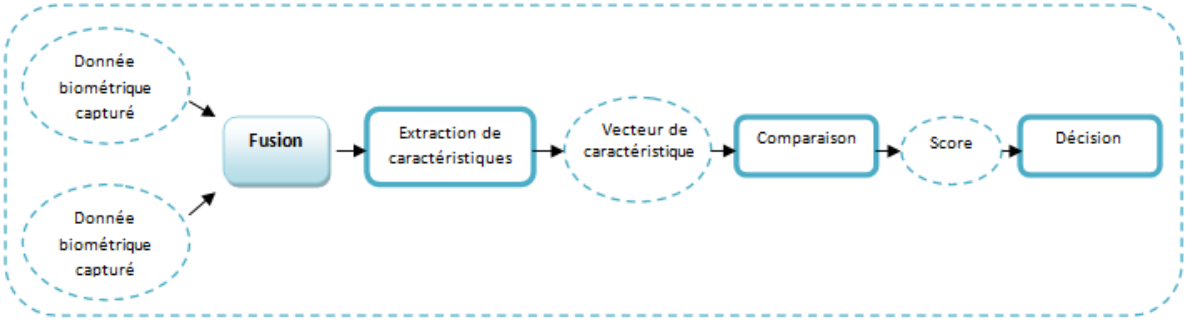

FIGURE 2.3 – Fusion au niveau Capteur.

FUSION AU NIVEAU DES CARACTERISTIQUES (FEATURE LEVEL) Dans cette architecture, les informations extraites des différents capteurs sont combinées dans un vecteur de caractéristiques commun, qui est ensuite comparé à un modèle préenregistré (qui est lui-même un vecteur de caractéristique commun stocké dans une base de données) et assigné un score correspondant comme dans un seul système (voir la figure 2.4) [Bubeck, 2003].

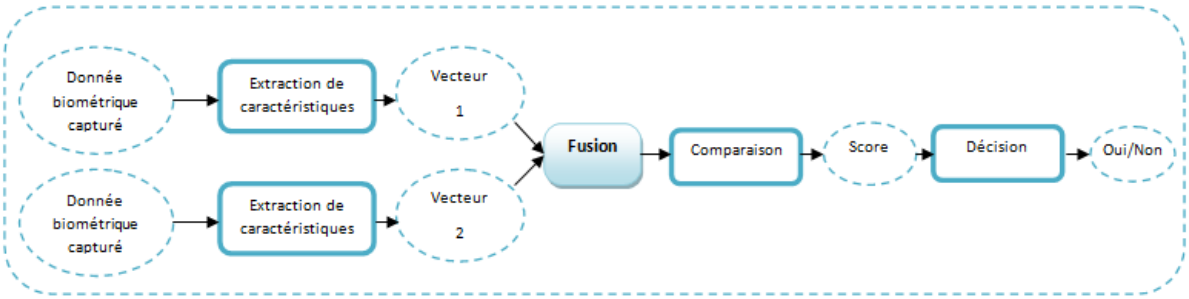

FIGURE 2.4 – Fusion au niveau des caractéristiques.

Contrairement à la fusion au niveau capteur, cette fusion est moins limitée par la nature des données biométriques. Donc si les vecteurs de caractéristiques en entrée sont homogènes, le vecteur de caractéristique résultant est calculé comme une somme pondéré de ces vecteurs. Lorsque les vecteurs de caractéristiques à fusionner sont hétérogènes, leur concaténation est souvent le moyen utilisé pour créer un nouveau vecteur. Mais la concaténation pose le problème de la dimension de l'espace de classification qui lorsqu'il augmente, rend plus difficile la tache de classification.
Les méthodes de fusion pré-classification sont assez peu utilisées car elles posent un

certains nombre de contraintes qui ne peuvent être remplies que dans certaines applications très spécifiques, tels que le coût de l'application, la dimension gigantesque du vecteur de caractéristiques obtenu par la concaténation des vecteurs entrants, ce qui conduit les chercheurs à s'intéresser à la fusion après matching [Mohammed, 2010].

2.3.2 La fusion post-classification

La fusion post-classification peut se faire au niveau des scores issus des modules de comparaison ou au niveau des décisions.

Fusion au niveau de score Dans un système multibiométrique construit sur cette architecture, des vecteurs de caractéristiques sont créés indépendamment pour chaque capteur, puis comparés aux modèles enregistrés, Basé sur la proximité du vecteur de caractéristiques et du modèle, chaque sous-système calcule son propre score de correspondance. Ces scores individuels sont finalement combiné en un score total, qui est remis au module de décision [Jain et al., 2005] [Ross and Jain, 2003]. L'ensemble du processus est illustré à la figure 2.5 :

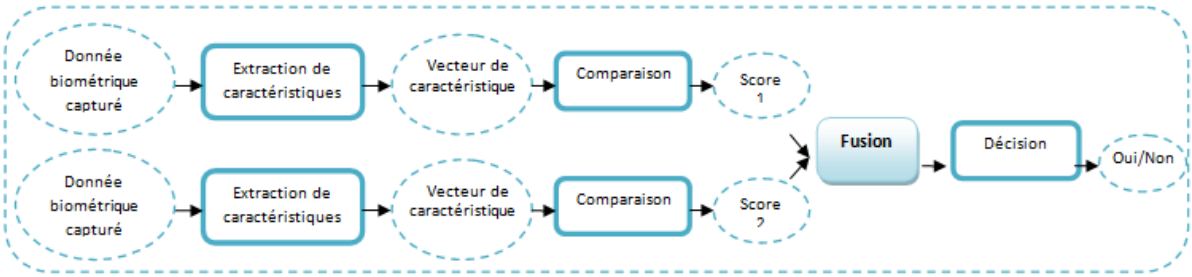

FIGURE 2.5 – Fusion au niveau de score.

Une étape de normalisation est généralement nécessaire avant que les scores bruts provenant de différents classificateurs puissent être combinés dans l'étape de fusion. En effet, les scores provenant de chaque système peuvent être de nature différente (scores de similarité, scores de distances ....).

- **Les méthodes de normalisation** :

  les trois méthodes de normalisation les plus connues en occurrence la méthode Min-Max, la méthode Z-score et la méthode TanH[Ahmed, 2014].

  - **Normalisation par la méthode Min-Max** : Cette méthode normalise les scores bruts tout en conservant leurs distributions à un facteur d'échelle près et transforme tous les scores dans l'intervalle [0,1] selon :

$$E_{iNorm} = \frac{E_i - E_{max}}{E_{max} - E_{min}} \tag{2.1}$$

– **Normalisation par la méthode Z-score :** Cette méthode transforme les scores en une distribution avec une moyenne égale à 0 et un écart type égal à 1 selon :

$$E_{iNorm} = \frac{E_i - \mu}{\sigma} \tag{2.2}$$

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

– **Normalisation par la méthode tangente hyperbolique Tanh :** Cette méthode est parmi les techniques statistiques les plus solides. Elle met chaque score normalisé dans l'intervalle [0, 1] selon :

$$E_{iNorm} = 0.5[Tanh(0.01 * (\frac{E_i - \mu}{\sigma})) + 1] \tag{2.3}$$

- **Les méthodes de combinison des scores**

Après avoir introduit les techniques de normalisation les plus utilisées, nous allons presenter des méthodes de fusion par combinaisons des scores.

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.

– Combiner les scores par **la moyenne** consiste à calculer s tel que :

$$S = \frac{1}{N} * \sum_{i=1}^{n} S(i) \tag{2.4}$$

– Combiner les scores par le produit consiste à calculer s tel que :

$$S = \prod_{i=1}^{n} S(i) \tag{2.5}$$

– Combiner les scores par le minimum consiste à calculer s tel que :

$$S = \min(S_i) \tag{2.6}$$

– Combiner les scores par le maximum consiste à calculer s tel que :

$$S = \max(S_i) \tag{2.7}$$

– Combiner les scores par la médiane consiste à calculer s tel que :

$$S = med(S_i) \tag{2.8}$$

– Toutes ces méthodes sont des méthodes simples qui ne nécessitent aucune adaptation. Il existe également des méthodes un peu plus évoluées de combinaison qui nécessitent le réglage de paramètres comme la somme pondérée :

$$S = \sum_{i=1}^{n} \omega S(i) \tag{2.9}$$

La somme pondérée permet de donner des poids différents à chacun des sous-systèmes en fonction de leur performance individuelle ou de leur intérêt dans le système multimodal. [Toufik, 2016]
parmi les stratégies utilisés dans la combinaison : La règle de somme, Arbre de décision, L'analyse discriminante linéaire. [Bubeck, 2003].

La fusion au niveau des scores est l'approche la plus utilisée, car elle offre le meilleur compromis entre la richesse d'information et la facilité d'implémentation.
Ce niveau de fusion peut être appliqué à tous les types de systèmes [Mohammed, 2010]

FUSION AU NIVEAU DE DÉCISION (DECISION LEVEL) Dans cette stratégie de fusion, une décision d'authentification distincte est prise pour chaque trait biométrique. Ces décisions sont ensuite combinées en un vote final, comme le montre la figure 2.6

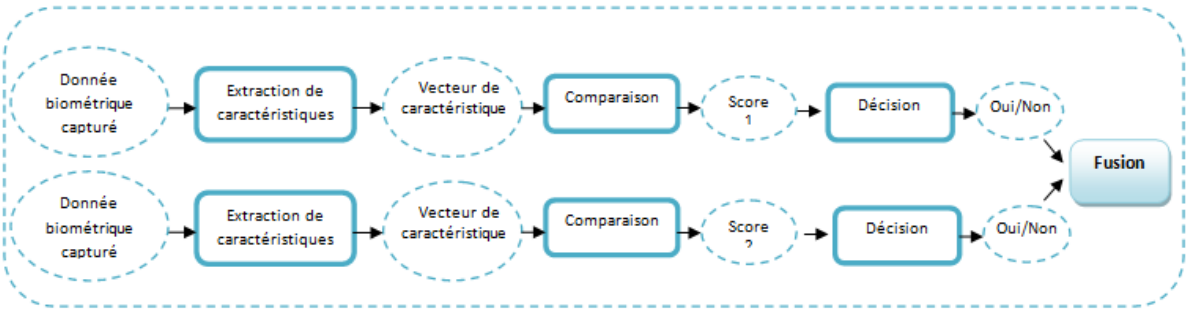

FIGURE 2.6 – Fusion au niveau de décision.

De nombreuses stratégies différentes sont disponibles pour combiner les décisions distinctes dans une décision d'authentification finale, les plus utilisées sont le majority voting [Lam and Suen, 1997](si la majorité des systèmes ont décidé 1 alors la décision finale est "accepté"), les règles ET (si tous les systèmes ont décidé 1 alors la décision finale est "accepté") et OU (si un système a décidé 1 alors la décision finale est "accepté").

Ces méthodes de fusion sont souvent utilisée pour sa simplicité mais utilisent très peu d'information [Sanderson and Paliwal, 2002].

2.4 Les bases de données de reference

La communauté scientifique a mis à disposition plusieurs bases de données des différentes modalités biométriques, afin de permettre aux chercheurs d'évaluer leurs systèmes biométriques ainsi que la comparaison entre les différents systèmes.
Certaines de ces bases de données contiennent une seule modalité alors que d'autres sont multimodales.
Nous décrivons quelque bases de données les plus utilisées :

2.4.1 PolyU-MSP

PolyU base de donnée contient 500 individus créés par des chercheurs de l'université polytechnique de Hong Kong en 2003. Les images des empreintes palmaires ont été assemblées en utilisant un dispositif de capture d'images, ensuite elles ont été prises dans deux périodes différentes séparées par un intervalle de temps d'environ deux mois. Chaque individu devait prendre au moins six images de ses des empreintes palmaires durant une période précise [Charfi, 2017].

2.4.2 CASIA-Iris :

CASIA-Iris de L'Académie chinoise des sciences - Institut d'Automation (CASIA) base de données d'image de l'œil contient 756 images de l'œil avec 108 niveaux de gris yeux et 7 images différentes de chaque œil unique.
les Images sont prises à partir de deux sessions avec un mois d'intervalle entre les sessions. Les images ont été capturées en particulier pour la recherche de reconnaissance de l'iris en utilisant l'optique numérique.
La base de données multi-représentation se compose de six images d'iris images par personne avec un total de 100 personnes [Phillips et al., 2007].

2.4.3 XM2VTSDB

La base de données XM2VTS (M2VTS étendu) a été acquise dans le cadre du projet M2VTS (Vérification multimodale des applications de téléservices et de sécurité), c'est une partie intégrante du programme ACTS de l'UE, dont Le but est d'améliorer l'efficacité de la reconnaissance en combinant des modalités uniques, à savoir des fonctionnalités de visage et de voix.

XM2VTSDB contient quatre enregistrements de 295 sujets pris sur une période de quatre mois.
Elle est disponible à l'achat auprès de l'Université de Surrey, elle a été distribuée à plus de 100 institutions [Messer et al., 1999].

2.4.4 BiosecurID

BIOSECUR-ID est un projet jOint financé par le Ministère espagnol de la Science Y Tecnologfa, La base de données comprend huit traits biométriques unimodaux, à savoir : parole, iris, visage (images fixes, vidéos de visages), signature manuscrite et texte manuscrit (signaux dynamiques en ligne, images numérisées hors ligne), empreintes digitales (acquises avec deux capteurs), la main (palmprint, contour-geometry) et la frappe.
La base de données comprend 400 sujets et présente des caractéristiques telles que : répartition équilibrée des sexes et des populations, disponibilité des informations sur des groupes démographiques particuliers (âge, sexe, faiblesse), et compatibilité avec autres bases de données existantes. Toutes ces caractéristiques le rendent très utile dans la recherche et le développement de systèmes biométriques unimodaux et multimodaux. La base de données était prête pour la recherche d'ici la fin de 2006 [Fierrez et al., 2010].

2.4.5 BioSec

Une base de données multimodale, acquise dans le cadre du projet intégré FP6 EU BioSec. Plus de 20 partenaires de neuf pays européens participent au projet, y compris de grandes entreprises, des producteurs biométriques de matériel / logiciels, des universités prestigieuses et des PME. ATVS est responsable des activités de base de données effectuées au sein de BIOSEC.

Biosec comprend des images d'empreintes digitales acquises avec trois capteurs différents, des images de visage, des images d'iris ,et des énoncés vocaux. BioSec comprend de vraies données multimodales de 200 individus dans 2 sessions d'acquisition. La base de données etait mise à la disposition du public à des fins de recherche d'ici la mi-2006 [Fierrez et al., 2007].

2.4.6 MYIDEA

La base de données MYIDEA est en cours d'acquisition dans le cadre d'une collaboration entre l'Université de Fribourg en Suisse, l'Ecole d'ingénieurs de Fribourg en

Suisse et le Groupe des Ecoles des Télécommunications à Paris. La base de données MYIDEA comprend la géométrie du visage, de l'audio, des empreintes digitales, de la signature, de l'écriture manuscrite et de la main. Suite à l'acquisition indépendante de chaque modalité, deux enregistrements synchronisés sont effectués : face-voix et écriture-voix.
Les spécifications générales de MYIDEA sont les suivantes : contient 104 sujets, qualité différente des capteurs, divers scénarios d'acquisition réalistes [Humm et al., 2005].

2.4.7 SDUMLA-HMT

SDUMLA-HMT [Yin et al., 2011] a été collecté durant l'été 2010 à l'Université de Shandong, Jinan, Chine. 106 sujets, dont 61 hommes et 45 %femmes âgés de 17 à 31 ans, ont participé au processus de collecte de données, dans lequel les 5 traits biométriques - visage, veine digitale, démarche, iris et empreintes digitales - sont collectés pour chaque sujet.
Par conséquent, il y a 5 sous-bases de données incluses dans SDUMLA-HMT, c'est-à-dire, une base de données de visage, une base de données de veines de doigt, une base de données de démarche, une base de données d'iris et une base de données d'empreinte digitale multi-capteur. Il est à noter que dans les 5 sous bases de données, tous les traits biométriques avec la même identité de personne sont capturés à partir du même sujet.
Le tableau 2.1 résume les bases de données decrit ci-dessus

TABLE 2.1 – Description de bases de données biométriques.

Base de données	Année	Utilisateurs	Sessions	Modalités	Visage	ED	M	Ms	I	Fc	S	V x	Vn	D
Poly msp	2003	500	2	1			X							
Casia	2005	100	2	1					X					
XM2VTSDB	1999	295	4	2	X							X		
Biosec	2007	250	4	4	X		X		X			X		
BiosecureID	2007	400	4	8	X		X	X	X	X	X	X		
Sdumla	2010	106		5	X	X			X				X	X
Myidea	2004	104	3	6	X	X	X	X			X	X		

ED :Empreinte, digitale, M :Main, Ms :Manuscrite, I :Iris, Fc :Frappe au clavier ,S :Signature ,Vx :Voix ,Vn :Veine ,D :Demarche

2.5 Fiabilité des systèmes biométriques

Il existe dans la littérature de nombreuses métriques pour quantifier la performance d'un système biométrique. On ne s'intéressera dans cette section qu'aux mesures des taux d'erreur et aux courbes de performance, selon les deux scénarios :

- E**n mode identification :** Le problème d'identification peut être formellement posé comme suit : étant donné N références d'entrée R1, ...,RN et une identité revendiquée (dite également probe) représentée par le vecteur Q, le système biométrique doit déterminer l'identité de Q à partir de R1, ...,RN. Les mesures suivantes sont utilisées pour mesurer la fiabilité d'un système biométrique avec un scénario d'identification :

  - **Rank-One Recognition Rate(Rank-1 RR) :** est le pourcentage de probes correctement identifiés. On dit qu'un système reconnaît un probe au rang 1 lorsqu'il choisit le plus proche modèle de la galerie comme résultat. Un système reconnaît un probe au rang 2, lorsqu'il choisit le plus proche modèle parmi deux modèles de la galerie et ainsi de suite.

  - **Cumulative Match Characteristic (CMC) :** cette courbe donne le pourcentage de personnes reconnues en fonction du rang k.

- **En mode authentification :** Le problème de vérification peut être formellement posé comme suit : étant donné le vecteur caractéristique d'entrée R et une identité revendiquée représentée par le vecteur Q, le système biométrique doit déterminer si l'identité proclamée Q est acceptée ou rejetée. Les mesures suivantes sont utilisées pour mesurer la fiabilité d'un système biométrique avec un scénario d'authentification :

  - **False Accept Rate (FAR),** ou taux de fausses acceptations : exprime le pourcentage d'utilisateurs acceptés par le système alors qu'ils devraient être rejetés.

  - **False Reject Rate (FRR)**, ou taux de faux rejets : exprime le pourcentage d'utilisateurs rejetés alors qu'ils devraient être acceptés par le système.

  - **Equal Error Rate (EER),** calculé à partir des deux premiers critères, il corres pond à l'endroit où FAR = FRR. C'est le meilleur compromis entre les faux rejets et les fausses acceptations.

$$TFA = \frac{FA}{NI} \tag{2.10}$$

et

$$TFR = \frac{FR}{NL} \tag{2.11}$$

avec
FR : nb faux rejets.
FA : nb fausses acceptations.
NL : nb total légitimes.
NI : nb total imposteurs.

– **Verification Rate at 0.1 % FAR :** correspond au taux de reconnaissance obtenu lorsque le FAR est de 0.1 %.

– **Receiver Operating Characteristic (ROC)** : la courbe ROC est une démonstration visuelle du compromis entre le FAR et le FRR par rapport à un seuil variable.

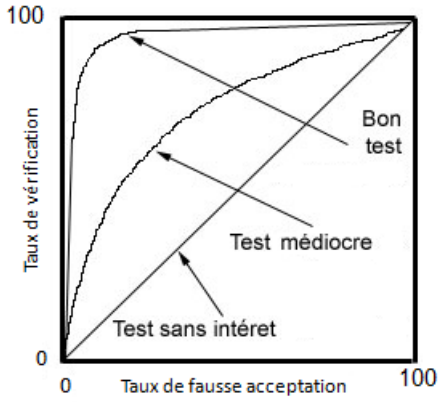

FIGURE 2.7 – Principes d'une Courbe ROC.

2.6 Conclusion

Nous avons présenté des systèmes biométriques multimodaux qui combinent les informations issues de différentes sources biométriques, ainsi que les différentes facettes que comporte la fusion de données. Il existe plusieurs topologies et niveaux de fusion dont le choix dépend de la nature des sources et de l'information.
Dans la fin de ce chapitre, nous avons présenté les bases de données les plus utilisées dans la recherche d'évaluation des systèmes biométriques et les principales techniques utilisées pour l'évaluation de ces systèmes.

Dans le chapitre suivant nous allons présenter un aperçu de quelques travaux dans le domaine de la biométrie multimodale.

Chapitre 3

État de l'art de la Reconnaissance d'empreinte digitale

3.1 Introduction

La reconnaissance d'empreinte digitale est la méthode la plus ancienne d'identification biométrique. Les premières traces d'utilisation d'empreintes digitales ont été découvertes en Egypte et datent de plus de 4000 ans. L'empereur chinois Qin Shi Huangdi (259 – 210 av. J.¬C.) fut le premier souverain à utiliser la marque des empreintes digitales dans l'argile comme sceau servant à authentifier les documents. Entre 618 et 907 ap. J.¬C., le papier et la soie connurent leur essor en Chine. Les paumes des mains et les empreintes digitales étaient imprimées sur les documents pour en attester l'authenticité.

En 1684, le morphologiste anglais Nehemiah Grew a publié le premier article scientifique rapportant une étude systémique sur la structure des crêtes, sillons et pores au niveau de l'empreinte digitale. En 1788, Mayer a pu fournir une description détaillée de la formation anatomique de l'empreinte digitale. En 1823, Purkinje a réussi à proposer la première classification des empreintes digitales.

C'est en 1856 que l'anglais William Hershel, après avoir utilisé les empreintes en guise de signature sur la population indienne qu'il dirigeait, commença à comprendre que les empreintes étaient uniques et constantes dans le temps. En 1888 le britannique Francis Galton publia une étude sur les empreintes digitales où il établit leurs caractéristiques (unicité, invariance, minuties, classification) et en 1901 la technique d identification au moyen de empreintes fut adoptée officiellement en Angleterre dans le système judiciaire.

De nos jours les empreintes sont toujours largement utilisées et reconnues comme méthode d'identification fiable. En 2013, le premier smartphone avec lecteur d'empreinte digitale a été deploye sur le marche par Apple avec l'Iphone 5S.

Les approches de reconnaissance par empreintes digitales peuvent être classées en deux catégories : les approches basées sur la mono-modalité et les approches locales basées sur la multi-modalité de l'empreinte digitale. Dans ce chapitre, nous passons en revue les approches les plus significatives et les plus représentatives suivant ces deux catégories.

3.2 Approches basées sur la mono-modalité

Le système uni-modal est un système qui utilise d'un seul doigt.Un tel systéme ne possède pas généralement un taux d'erreur très élevé le rendant inapplicable pour des entreprises ou des personnes particulières.

Dans [Masmoudi and Masmoudi, 2010], Masmoudi et al. ont proposé un système de reconnaissance d'empreinte digitale en utilisant un descripteur de modèle binaire local (LBP) appliqué aux champs de minutie et d'orientation. Avec un classificateur basé sur des réseaux neuronaux, le système proposé a été implémenté sur la plate-forme connue sous le nom de FPGA et optimisé en fonction de l'occupation des ressources matérielles. Les résultats expérimentaux de la base de données d'empreintes digitales, FVC (Fingerprint Verification Competition) ont montré des taux de reconnaissance élevés.

Deux nouvelles méthodes de mis en correspondance utilisant Scale Invariant Local Features (SIFT) pour la reconnaissance des empreintes digitales ont été etudiées dans [Trung, 2011]. Dans la première méthode, l'association entre les points détectés par SIFT et les points minuties est utilisée tandis que dans la deuxième méthode, la mise en correspondant les point d'intérêt de SIFT seulement est adoptée. Pour évaluer les performance de ces deux méthodes, une collection d'environt 306 empreintes digitales collectées à partir de 34 étudiants de l'université de CAN THO est utilisée atteignant un taux de reconaissance de 92.6%pour la première et 93.4%pour la deuxième méthode.

Un algorithme basé sur la corrélation d'un sous-ensemble de minuties (les terminaisons et les bifurcations) a été proposé dans [Asha and Chellappan, 2014] pour la correspondance des empreintes digitales. Pour le prétraitement, trois étapes ont été appliquées : une amélioration avec légalisation d'histogramme, la transformée de Fourrier, une binarisation par seuillage local adaptatif et une segmentation pour la localisation de la région d'intérêt avec des méthodes de la morphologie mathématique. Pour l'extraction des minuties une approche de numéro de passage (Crossing number), a été mise en œuvre. La distance entre deux minuties est calculée en utilisant la distance Euclidienne. Cet algorithme a été évalué sur la base de données FVC2004 montrant une amélioration des performances de reconnaissance de 0.32 à 0.12% en taux d'erreur après application de l'algorithme des sous-ensembles de minuties. De plus, les résultats expérimentaux ont montré que la méthode proposée offre un bon compromis entre vitesse et précision.

Dans [Garg et al., 2014], une méthode pour La reconnaissance d'empreintes digitales utilisant une combinaison de la Transformée de Fourier Rapide (FFT) et des filtres de Gabor pour le réhaussement de l'image a été proposée. La méthode consiste à combiner le filtre de Gabor et le filtrage dans le domaine des fréquences pour améliorer l'empreinte digitale. Avec huit différentes orientations du filtre de Gabor, les caractéristiques de l'empreinte digitale sont combinées. Dans le filtrage dans le domaine des fréquences, l'image de l'empreinte digitale est subdivisée en32×32 petits blocs puis les caractéristiques sont extraites de ces blocs dans le domaine fréquenciel. L'em-

preinte digitale finale améliorée est obtenue grâce aux résultats du filtre de Gabor et du filtrage dans le domaine fréquentiel. La binarisation et l'amincissement suivent, où l'empreinte digitale améliorée est convertie en image binaire et les crêtes sont amincies à une largeur de 1 pixel, permettant d'extraire les minutiaes (bifurcation des crêtes et terminaisons des crêtes). Le taux global de reconnaissance de la méthode proposée est de 95%.
Hany et Akter [Hany and Akter, 2015] ont étudié et évalué une approche de reconnaissance d'empreintes digitales par une méthode locale d'extraction et d'appariement des caractéristiques. Dans cette approche, les caractéristiques locales sont d'abord extraites à l'aide de l'algorithme SURF (Speeded-Up Robust Feature). Ensuite, les caractéristiques de l'image d'empreinte digitale de test sont comparées à ceux de l'image de la galerie. Deux caractéristiques correspondent lorsque la distance entre elles ,est inférieure au seuil correspondant. Les résultats expérimentaux indiquent son efficacité et ses performances grâce à l'invariabilité de détecteur surf à l'échelle et de rotation. Evaluée sur une base de données comprenant, l'approche proposée atteint un taux de reconnaissance de 88.3%.

Un système d'authentification pour les petits capteurs d'empreinte digitale grâce à l'intégration des nouveaux capteurs d'empreinte digitale dans les Smartphones, on comparant entre deux descripteurs SIFT et HARRIS a été développé dans [Bourjot, 2017]. Pour simuler le processus d'acquisition d'un petit capteur, une image de taille 70×70 pixels est découpée dans chaque acquisition. Ce format correspond à une surface de de taille 5×5 mm pour un capteur de 350dpi, soit de l'ordre de grandeur de ceux du marché des smartphones. Pour extraire une image centrée sur l'empreinte, l'algorithme K-means est utilisé afin de séparée le fond de l'image de celle de l'empreinte.

Dans Manickam et al. [2018], un système d'identification des empreintes digitale a eté presenté. D'abord, une étape d'amélioration du contraste d'empreintes digitales est appliquée, ensuite l'algorithme SIFT est utilisé pour l'extraction de caractéristiques. Les scores de similarités sont calculés en utilisant la distance euclidienne. Les auteurs ont évalué leur algorithme, en utilisant une base de FVC-2004. Les résultats expérimentaux indiquent que l'approche proposée donne de meilleurs résultats que les approches basées sur les minuties.

3.3 Approches basées sur la multi-modalité

Les humains se reconnaissent entre eux à partir de plusieurs modalités biométriques physiques et/ou comportementales. Chaque modalité en soi ne peut pas toujours être utilisée de manière fiable pour effectuer la reconnaissance. Cependant, la fusion d'in-

formation présentées par les diférentes modalités permet d'améliorer de manière significative sa performance, conduisant à une reconnaissance précise de l'identité.

Plusieurs limitations inhérentes des systèmes uni-modaux peuvent être observées. D'abord, au niveau de l'acquisition, le bruit cause une dégradation des performances. Ensuite, la modalité elle-même peut présenter une grande variabilité intra-classes ou une petite variabilité interclasses.

Des études menées à la fin des années 1990 ont montré qu'une meilleure reconnaissance est atteinte lorsque la fusion de plusieurs sources d'information est utilisée plutôt qu'une seule source. Cette revue de littérature porte principalement sur la fusion à partir des informations provenant de plusieurs doigts d'une même personne, puisqu'il s'agit de l'une des plus couramment utilisées et recommandées pour les systèmes d'identification automatique. Cependant, la fusion à l'aide des informations provenant de plusieurs échantillons du même doigt est également abordée dans le cadre de cette étude, puisque plusieurs enrôlements sont également effectués.

Prabhakar et Jain [Prabhakar and Jain, 2002] ont montré que si différents algorithmes de comparaison d'empreintes digitales sont combinés (quatre algorithmes ont été utilisés), la performance globale serait alors plus importante. Ils ont montré également que la combinaison d'empreintes multiples ou de doigts multiples améliore considérablement les performances de vérification du système de reconnaissance d'empreintes digitales. Ils ont procédé à une enrôlement multiple en combinant deux échantillons d'empreintes digitales du même doigt ou de doigts différents pour vérifier l'efficacité du système qu'ils proposent. Leurs expériences ont été réalisées sur une base de données de 167 individus (quatre empreintes pour quatre doigts, $167 \times 4 \times 4$ produisant 2672 empreintes digitales) à l'aide de l'appariement par minuties et par filtres de GABOR ainsi que de la fusion au niveau décision. Leurs résultats ont montré que lorsque des empreintes multiples ou des doigts multiple sont combinés, l'exactitude de la reconnaissance s'améliore de plus de 4%.

Dans [Simon-Zorita et al., 2003], Simon-Zorita et all. ont proposé le stockage de trois échantillons d'empreintes digitales du même doigt au moment de l'enrôlement. La vérification est ensuite effectuée en comparant l'échantillon des empreintes digitales de référence avec les trois échantillons stockés et en choisissant le score maximum pour être le score de fusion.

Marcialis et Roli ont fusionné dans leurs recherches plusieurs capteurs d'empreintes digitales pour la vérification des empreintes digitales [Marcialis and Roli, 2004]. Chaque

capteur a été soumis à des doigts dont les images d'empreintes digitales sont capturées, traitées et des caractéristiques distinctes (minuties) extraites. Les ensembles de caractéristiques extraites sont appariés et deux scores d'appariement (chacun résultant de chaque capteur) sont générés. Ces deux scores sont ensuite combinés pour obtenir un score final d'appariement.

Yang et Zhou ont réalisé une étude comparative de la combinaison de plusieurs échantillons enregistrés pour la vérification des empreintes digitales [Yang and Zhou, 2006]. De nombreux schémas ont été étudiés qui ont montré une plus grande amélioration de la performance de la reconnaissance lorsqu'un enrollement multiple était appliquée. Ils ont en outre proposé leur propre schéma qui combinait les niveaux de fusion de caractéristiques et de décision tout en utilisant des empreintes multiples pour obtenir une meilleure performance de reconnaissance. Les bases de données utilisées pour les expériences étaient THU (avec 827 doigts et 8 empreintes par doigt donnant 6616 empreintes digitales), FVC2002 DB1 et FVC2002 DB2. Une grande amélioration des performances globales en termes de FRR et de FAR ont été observée avec le schéma combiné proposé.

Stelvio et Gamassi propose un approche de reconnaissance des empreintes digitales à inscriptions multiples qui améliore la précision de la reconnaissance, la vitesse de correspondance et la consommation de mémoire et permet l'implémentation de méthodes non minutieuses basée sur un filtre de Gabor, Les auteurs de [Cimato et al., 2008] utilisent une fusion au niveau de caractéristiques, en utilisant deux bases de données d'empreintes digitales; FVC 2000-DB1-A et FVC 2006-DB2- A. Une amélioration de EER attient 0.13% par rapport a 0.75% avec la première base de données et de 6,14% à 1,75% avec la deuxième base Les résultats de l'expérimentation et les évaluations montrent que les inscriptions multiples dans leur ensemble sont supérieures à l'inscription unique.

Dans [Ren et al., 2009], les auteurs ont proposé dans leur recherche une méthode qui met en œuvre la fusion au niveau du score en utilisant des empreintes digitales multiples. Plusieurs échantillons du doigt d'un même utilisateur sont enregistrés et stockés comme modèles. Au moment de la vérification, la distance par rapport à l'empreinte digitale test et le centroïde des empreintes digitales de référence (modèles stockés) est calculé dans un espace multidimensionnel. Les bases de données FVC2000 DB1, FVC2000 DB2, FVC2002 DB2 et FVC2002 DB3 (de 100 personnes ayant chacune 8 empreintes)ont été utilisées. Les résultats montrent qu'une plus grande précision de reconnaissance est obtenue lorsque l'enrôlement multiple avec fusion a été appliqué.

Pour améliorer la précision de la reconnaissance et réduire les erreurs de classification dans les systèmes biométriques, les auteurs de [Uhl and Wild, 2009] ont combiné plusieurs instances d'une même biométrie, à savoir les empreintes digitales et le doigt propre, et les ont comparées aux instances uniques. Les caractéristiques (Minuties et doigt propre) sont extraites et stockées comme modèles de référence. Pour les minuties, l'appariement des modèles stockés est suivi d'une exécution par paires qui génère un score d'appariement pour chaque comparaison effectuée. Pour l'appariement avec le doigt propre, le classifieur à base de la distance de Mahattan convertit les distances propes en scores de similarité. les scores des minuties et des doigts propres sont ensuite fusionnée pour obtenir le résultat final. Deux bases de données A (86 individus et 443 échantillons) et B (31 individus et 63 images) ont été utilisées. Une grande amélioration de la performance de reconnaissance a été observée dans les expériences multi-instances.

Dans [Mane et al., 2011], Mane et al. ont combiné les scores d'appariement générés à partir de multiples instances du même doigt acquises en utilisant le même capteur d'empreintes digitales. Ils ont utilisé la technique de fusion au niveau du score pour obtenir une précision de reconnaissance finale. Les bases de données FVC2000 DB1, FVC2002 DB1, FVC2004 DB1 ont été utilisées. La méthode d'appariement est basée sur des modèles où un point de référence et une région d'intérêt sont d'abord déterminés. L'appariement se fait ensuite après filtrage de la région d'intérêt et calcul de l'écart absolu moyen. Leurs résultats montrent qu'il y a eu une plus grande amélioration dans l'exactitude de la reconnaissance lorsque un enrollement multiple est appliqué.

Dans [Cheng et al., 2011], Cheng et al. ont développé un système biométrique multi-échantillon des empreintes digitale, basé sur l'extraction de minuties, en utilisant une combinaison au niveau de score lors de test, c.-à-d le système biométrique a acquis deux modèles de test et peut créer un score de correspondance combiné, en faisant la moyenne de deux scores à partir des correspondances entre ces modèles et le modèle enregistré. Les expériences effectuées sur les quatre bases de données d'empreintes digitales FVC2002 : DB1, DB2, DB3 et DB4, chacune contenant 110 personnes différentes avec huit images différentes pour la même empreinte digitale d'une personne. Les résultats montrent que l'utilisation des scores entre les modèles de test peut améliorer les performances des méthodes de combinaison utilisées.

Bian et Busch [Yang et al., 2011]proposent un système d'authentification de l'empreinte digitale basés sur des minuties ,en utilisant les pseudonymes. Ils démontrent l'influence sur la performance biométrique de la fusion au niveau de la décision dans différents scénarios de fusion (multi échantillons, multi instances, multi capteurs et multi algorithmes) sur une base de données d'empreintes digitales multi-capteurs. la fusion

dans ce niveau présente non seulement la moindre complexité de fusion, mais aussi l'interopérabilité maximale entre différentes caractéristiques biométriques.

Dans [Singh et al., 2012], un système biométrique multimodèle efficace basé sur 4 images d'empreintes digitales est proposé. Le système utilise un lecteur d'empreintes digitales à 4 touches pour collecter simultanément les empreintes de plusieurs doigts sur une main et utilise une combinaison au niveau de score. Le système a été testé sur deux bases de données d'empreintes digitales, à savoir IITK-student et IITK-rural contenant respectivement 1007 et 991 sujets. Les deux bases de données sont acquises en 2 sessions. Le taux de reconnaissance correct obtenu est de 91% pour la base de données IITK-rural et de 99.64% pour la base de données ITKstudent.

Cheng et Tulyakov étudient la question de la combinaison des résultats de correspondance multi-échantillons obtenus lors de tentatives répétées d'authentification basée sur les empreintes digitales [Cheng et al., 2013],en utilisant l'extraction de minuties, Les expériences sont effectuées sur des bases de données d'empreintes digitales FVC2002. Le résultat montre que le système proposé est capable de surpasser le système. Le rapport de vraisemblance (Likelihood ratio) et le perceptron multicouche sont utilisés comme méthodes combinées.

Dans [Ilugbusi and Adetunmbi, 2017], Ilugbusi présente un système d'authentification par empreintes digitales multi-instances, qui résiste aux divers problèmes rencontrés dans les systèmes unimodaux. Des caractéristiques uniques des empreintes digitales ont été extraites en utilisant la technique du nombre de croisements (CN) qui acquiert la fin des arêtes et la bifurcation à partir d'une seule image en examinant le voisinage local de chaque pixel en utilisant une fenêtre 3 par 3. L'authentification nécessite deux empreintes digitales demandées, à partir desquelles les entités sont ensuite extraites et comparées avec celles du modèle de base de données respectivement pour déterminer un score de correspondance pour chacune. Chaque score est ensuite fusionné en utilisant une règle de somme pondérée. Le score fusionné est ensuite comparé pour effectuer le match final. Le résultat expérimental montre une durée d'exécution moyenne de 3,82 secondes pour la vérification des sujets et une précision de 98,67%.

Dans [Sedighi and Analoui, 2017], Elham et Analoui proposent un système de vérification des empreintes digitales ,avec une fusion multi-échantillons au niveau de score qui offre une simplicité et haute performance, en utilisant la machine à vecteurs de support, Les résultats expérimentaux de la base de données des empreintes digitales de l'Université d'Iran montrent des taux de reconnaissance élevés :0.997% pour la précision et 0,129% pour un taux d'erreur

Shancymol Sojan et khjh développent un système d'authentification de l'empreinte digitale, cité dans [Sojan and Kulkarni, 2017], en explorant la possibilité de combiner des caractéristiques du même trait biométrique (empreintes digitales), c'est-à-dire en le maintenant unimodale tout en offrant la même sécurité que celle de la biométrie combinée. En utilisant les fonctions de minutie et d'orientation de deux empreintes différentes, un nouveau modèle unique d'empreintes digitales mixtes est généré.Une fonctionnalité de Gabor du modèle mixte est extraite avant la correspondance afin de réduire le taux d'erreur, Le test des modèles se fait à l'aide de deux méthodes, à savoir : basé sur les corrélations et les minuties. Ces deux méthodes ont été efficaces pour identifier les modèles avec précision. Le FAR = 0,08% et le FRR = 0,1%.

3.4 Conclusion

De nos jours les empreintes digitales sont toujours largement utilisées et reconnues parmi les méthodes de reconnaissance les plus fiables. Dans ce chapitre un état de l'art sur la reconnaissance d'empreinte digitale a été présenté. Un résumé de travaux récents dans la reconnaissance biométrique par empreinte digitale est présenté. Le point est mis sur les deux types de systèmes biométriques mono-modaux et multi-modaux par cette modalité.
Dans le chapitre suivant nous présenterons le processus général de notre système ainsi que les résultats obtenus

Chapitre 4

Conception et réalisation du système multimodal

4.1 Introduction

Après avoir abordé l'aspect théorique dans les chapitres précédents, nous passons à la conception et à l'implémentation de notre application pour la reconnaissance des individus par l'empreinte digitale.
Nous analyserons plus en détail les étapes de conception du notre système multi-biométrique pour cela on a met en place la méthode locale SURF (Speeded Up RobustFeature) qui est inspirée de la méthode SIFT (Scale Invariant Feature Transforme). Nous présenterons par la suite des méthodes utilisées pour fusionner les scores obtenues. Finalement, nous conclurons le chapitre par une analyse et discussion des résultats expérimentaux.

4.2 Architecture du système proposé

L'architecture de notre système de reconnaissance biométrique multimodale est illustrée dans la figure 4.1

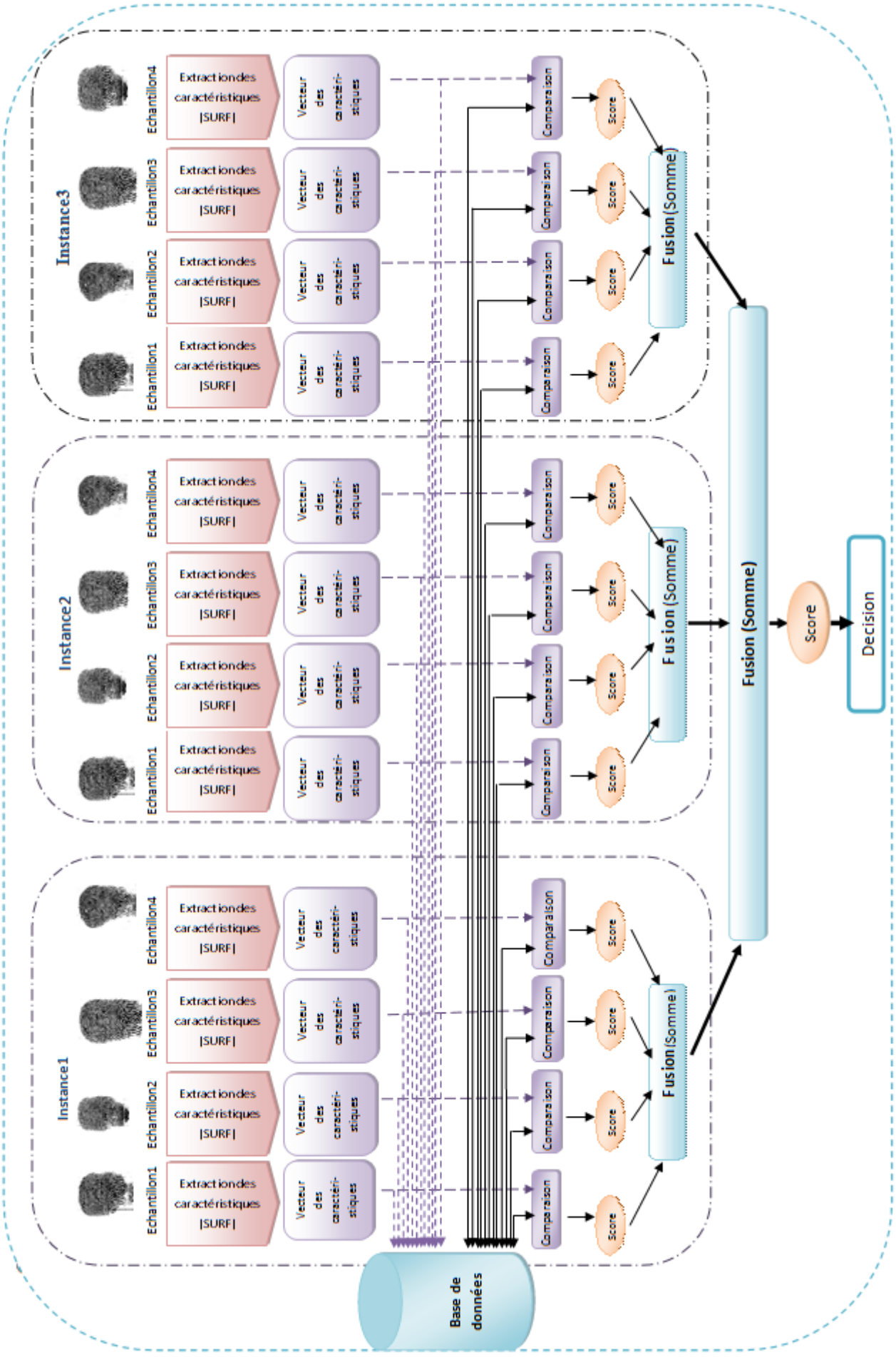

FIGURE 4.1 – Architecture du systeme proposé en utilisant le descripteur SURF.

Description d'architecture du notre système

4.2.1 Module d'acquisition

L'image dans cette étape est dans un état brut ce qui provoque des problèmes qui peuvent diminuer les performances du système, La qualité de la biométrie est affectée par le dispositif de capture. Dans ce paragraphe, nous présentons un résumé des facteurs affectant notre étude :

1. **Qualité des crêtes et clarté des crêtes :**
   La mauvaise qualité d'image capturée impacte directement la performance de système surtout si l'image capturée comme la figure ci-dessous (Figure 4.2).

FIGURE 4.2 – la qualité et la clarté des crêtes.

2. **La position de l'image capturée :**
   La probabilité d'erreur est élevé, lorsqu'on compare une traces laissées partielles et une empreinte bien positionné. (Figure 4.3).

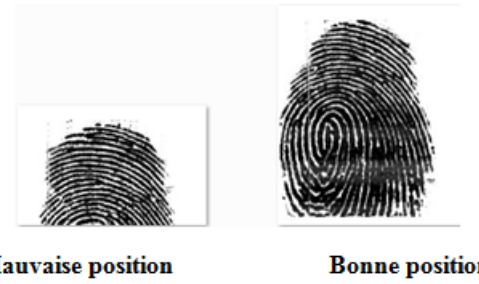

FIGURE 4.3 – Différentes positions des empreintes.

3. **La distorsion de l'image :**
   Les images biométriques détériorées présentent un sérieux problème. Dans la majorité des cas ces images sont supprimées de la base ou remplacées par d'autres captures de bonne qualité.

FIGURE 4.4 – Exemples d'images d'empreinte d'détériorées.

Solutions envisagées

- Stockage de multiples instances et répétés du même trait biométrique représentant la variabilité de ce trait.
- Mise à jour des instances dégradées et remplacement des images détériorées par de bonnes captures.
- Sélection d'images à base leurs qualité pour être utiliser dans le test

4.2.2 Module d'extraction des caractéristiques

Dans notre travail en extraction des caractéristiques de l'empreinte digitale nous avons utilisé la méthode SURF qui nous a donné le meilleurs taux de reconnaissance dans un temps raisonnable Par rapport au Gabor [Fogel and Sagi, 1989] et LBP[Ojala et al., 1994], sur la même base d'image, grâce à l'invariabilité à l'échelle et de rotation.

TABLE 4.1 – Comparaison entre Gabor et LBP et surf au niveau de précision.

Algorithme	Gabor	LBP	surf
Taux de reconnaissance	68%	74%	100%

4.2.2.1 Aperçu de SURF

L'algorithme SURF (Speeded Up Robust Features), que l'on peut traduire par caractéristiques robustes accélérées, développé par [Bay et al., 2008], est un détecteur et descripteur de caractéristique, présenté par des chercheurs de l'ETH Zurich et de l'université catholique de Leuven pour la première fois en 2006, il présente l'avantage majeur d'être à la fois invariant aux rotations et aux changements d'échelle. De plus qu'il est simple et rapide SURF est partiellement inspiré par le descripteur SIFT [Lowe, 2004], qu'il surpasse en rapidité, Le détail de la méthode est présenté par la suite.

4.2.2.2 L'algorithme SURF

La mise en œuvre de l'algorithme SURF passe par plusieurs étapes : La première consiste à détecter des points d'intérêt sur l'image et la seconde consiste à décrire ces points d'intérêt à l'aide d'un vecteur de 64 caractéristiques. comme montre la figure suivante :

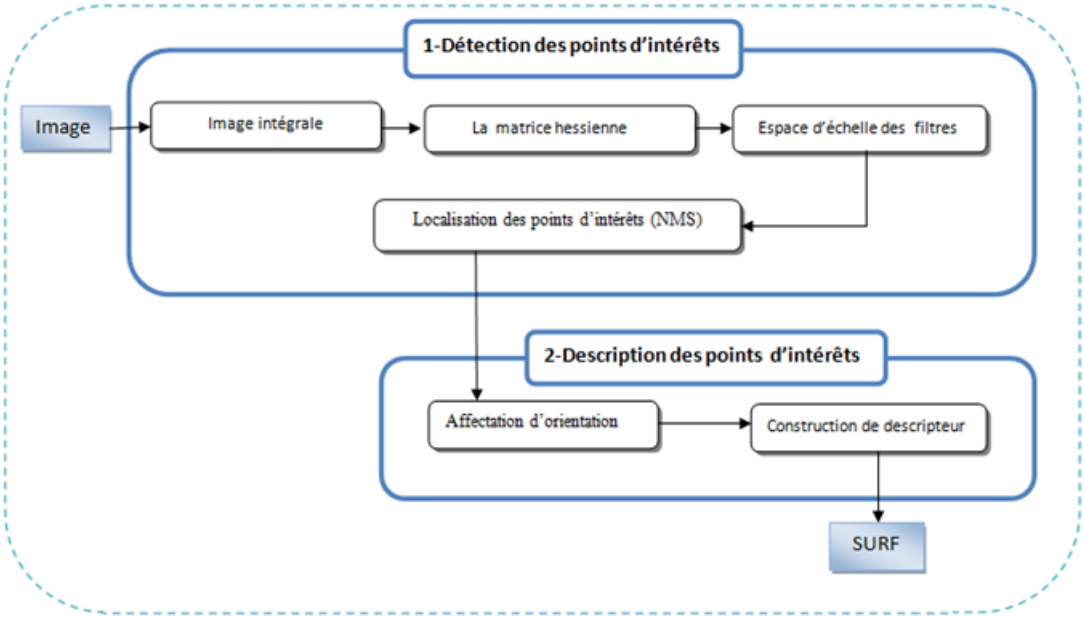

FIGURE 4.5 – Description de l'algorithme Surf.

Détection des points d'intérêts :

Image intégrale

Une grande partie de l'augmentation des performances de SURF peut être attribuée à l'utilisation d'une représentation intermédiaire de l'image appelée image intégrale. Étant donné I, notre image de départ, $I(x, y)$ représente la valeur d'un pixel de l'image aux coordonnées x et y. L'image intégrale, notée I_Σ est une image de même taille que l'image d'origine, calculée à partir de celle-ci. Chaque pixel de l'image intégrale contient la somme des pixels situés au dessus et à gauche de ce pixel dans l'image d'origine :

$$I_\Sigma(x, y) = \sum_{x'<=x, y'<=y} I(x', y') \tag{4.1}$$

Une fois l'image intégrale calculée, l'évaluation de toute région rectangulaire quelconque délimitée par les sommets A, B, C et D, comme dans la Figure 4.6, est réduite à quatre opérations. La somme des intensités de pixels est calculée par :

$$\Sigma = A + D - (C + D) \tag{4.2}$$

et s'effectue donc en temps constant indépendamment de la position et la taille de la région.

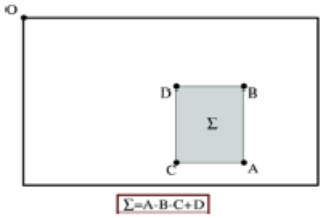

FIGURE 4.6 – Représentation de l'image intégrale où la somme des pixels dans la zone Σ est directement calculée par $A + D - (C + B)$).

La Hessienne

On recherche les zones de fort changement d'intensité des pixels dans l'image on utilisant la matrice Hessienne, cette dernière basée sur le calcul des dérivées partielles d'ordre deux, elle est définie comme suit :

$$H(X,\sigma) = \begin{bmatrix} L_{xx}(X,\sigma) & L_{xy}(X,\sigma) \\ L_{xy}(X,\sigma) & L_{yy}(X,\sigma) \end{bmatrix} \tag{4.3}$$

où

$$L_{xx}(X,\sigma) = I(X) * \frac{\delta^2}{\delta x^2} * g(\sigma) \tag{4.4}$$

et

$$L_{xy}(X,\sigma) = I(X) * \frac{\delta^2}{\delta xy} * g(\sigma) \tag{4.5}$$

L_{xx}est la convolution de la dérivée du second ordre de la Gaussienne avec l'image I au point X et de même pour L_{yy} et L_{xy}. Ces dérivées sont connues sous le nom de Laplacien des Gaussiens.

Afin de gagner en rapidité, ces gaussiennes sont approximées par un filtre moyenneur sur des voisinages pondérés appelée box filter.

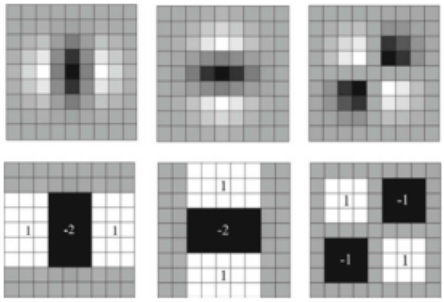

FIGURE 4.7 – Approximation des dérivées partielles du second ordre des Gaussiennes par des boîtes de filtres. De gauche à droite sont $L_{xx}, L_{yy} et L_{xy}$.

Le déterminant approximé est donné par l'expression suivante :

$$det(H_{approx}) = D_{xx}D_{yy} - (0.9D_{xy})^2 \tag{4.6}$$

Espace d'échelle

Pour trouver un point clé à différentes échelles, nous devons créer un espace d'échelle d'image qui peut généralement être atteint par une pyramide, mais en conservant la taille originale de l'image, l'espace de l'échelle est calculé en changeant la taille du filtre [Zhang et al., 2012].

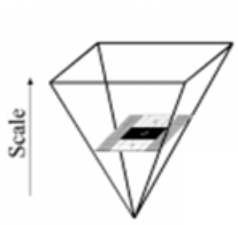

FIGURE 4.8 – espace d'échelle.

Cette étape apporte une invariance des points d'intérêts par rapport à la mise à l'échelle.

La localisation des points d'intérêt :

Les points d'intérêt sont localisés en appliquant une suppression non maximale de det(Happrox) dans un 3×3×3 voisinage. Tout d'abord, les déterminants sont seuillés de sorte que toutes les valeurs au dessous d'un seuil prédéfini soient supprimées.
Après le seuillage, une suppression non maximale est effectuée pour trouver un ensemble de points candidats. Pour ce faire, chaque pixel de l'espace échelle est comparé à ses 26 voisins, composés de des 8 points de l'échelle courant et des 9 points de chacun des échelles au-dessus et au-dessous. La Figure 4.9 illustre l'étape de suppression non maximale. À ce

stade, nous avons un ensemble d'intérêts points dont la résistance minimale est déterminée par la valeur seuil et qui sont également locaux maxima/minima dans l'espace échelle.

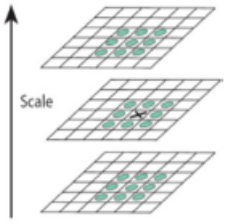

FIGURE 4.9 – Suppression Non-Maximale. Le pixel marqué "X" est sélectionné comme maximum s'il est plus grand que les pixels environnants sur son échelle et ses échelles au-dessus et au-dessous.

L'algorithme comporte ensuite des étapes destinées à apporter plus de précision dans leur localisation.

La description des points d'intérêts

Affectation d'orientation

Une fois les points d'intérêt extraits, la seconde étape de SURF consiste à calculer le descripteur correspondant. Le descripteur SURF décrit l'intensité des pixels dans un voisinage autour de chaque point d'intérêt.et donc permet d'apporter l'invariance par rapport à la rotation. Une orientation est tout d'abord assignée à chaque point extrait. Pour cela, les réponses des ondelettes du Haar du premier ordre en x et en y(figure 4.11) sont calculées dans un voisinage circulaire de rayon 6σ ou σest l'échelle du point considéré [Hoogstoel, 2011].

Les réponses sont alors accumulées horizontalement et verticalement dans une fenêtre d'orientation glissante de taille

$\pi/3$ pour donner un vecteur d'orientation local, et le vecteur le plus long sur toutes les fenêtres définit l'orientation dominante du point clé comme montre la figure 4.10

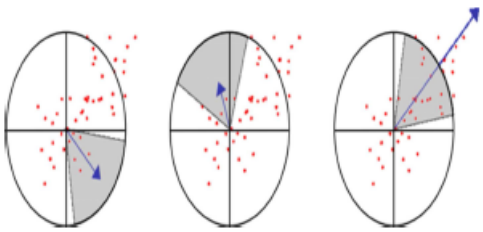

FIGURE 4.10 – Détermination de l'orientation principale.

FIGURE 4.11 – Filtre horizontal et vertical de Haar waar wavelet filters.

Construction de descripteur SURF

Le calcule du descripteur se fait sur un voisinage carré de coté 20σ et orienté selon l'orientation majoritaire du point. Cette zone est subdivisée en sous-zones 4×4 qui sont décrites par les valeurs d'une réponse d'ondelette de Haar horizontales et verticales. ces valeurs d'intérêt sont pondérées par un gaussien ($\sigma = 2.5s$) pour donner une certaine robustesse aux déformations [Pedersen, 2011], Chaque sous-zones est alors caractérisée par un vecteur de quatre composantes :

$$v = \{\sum d_x, \sum d_y, \sum |x|, \sum |y|\} \tag{4.7}$$

La concaténation de ces vecteurs conduit au descripteur SURF de 64 composantes.
Donc, le résultat de l'extraction d'une image, est un ensemble des points d'intérêts, chacun est caractérisé par son position (x, y), ainsi que l'´echelle σ(de filtre utilisé) et leur orientation θ comme montre la figure suivante :

$$Y(I) = \{ki = (x_i, y_i, \sigma_i, \theta_i, v_i) | i = 1 : N(I)\}$$

FIGURE 4.12 – Résultat de l'algorithme SURF.

4.2.3 Module de comparaison (Matching)

4.2.3.1 La méthode de comparaison

Dans cette étape, on cherche à trouver des correspondances entre les Surf de l'image requête et les Surf des images de la base, le but est de former les couples des plus proches descripteurs.
L'image I est ainsi caractérisée par l'ensemble

$Y(I) = \{ki = (x_i, y_i, \sigma_i, \theta_i, v_i) | i = 1 : N(I)\}$ avec : N(I) le nombre de points d'intérêt détectes dans I; (xi, yi) la position du point d'intérêt i dans I; (σ_i, θ_i) l'´echelle et l'orientation du point d'intérêt i; et v_i le vecteur de descripteurs du point d'intérêt i. La vérification entre deux images I1 et I2 correspond au calcul du nombre d'associations entre les deux ensembles Y (I1) et Y (I2).
Une association est définie par une double mise en correspondance entre deux points d'intérêt, Pour le point d'intérêt x de l'image I1, nous recherchons le point d'intérêt y de I2 le plus proche parmi l'ensemble de points d'intérêt de I2. Nous regardons également si le second point d'intérêt y' le plus proche est suffisamment loin de x au moyen d'une valeur seuil C :

$$d(x, y) = min_{\{z \in Y(I_2)\}} d(x, z) \tag{4.8}$$

et

$$d(x, y) = C * d(x, y') \tag{4.9}$$

avec

$$d(x, y') = min_{\{z \in Y(I_2), d(x,z) > d(x,y)\}} d(x, z) \tag{4.10}$$

La correspondance entre x et y est accepté si le ratio $\frac{d(x,y')}{d(x,y)}$ est inferieur à un seuil C. Cela met en avant que « x » doit ressembler beaucoup à « y» mais peu à tous les autres descripteurs de la base.
La distance d(.,.) est une distance euclidienne calculée entre les deux descripteurs normalises correspondant aux points d'intérêt. Si ces deux conditions ne sont pas remplies, alors le point x n'est pas mis en correspondance avec le point y [Oyallon and Rabin, 2015].cette methode prend le nom "NN-DR " pour Nearest Neighbor Distance Ratio

4.2.3.2 la fusion

Nous avons choisis la fusion au niveau score car elle donne le meilleur compromis entre la richesse d'information et la facilité d'implémentation.
nous avons appliqué les deux méthodes de fusion(multi échantillon afin de prendre en compte les variations de la pose (pour prendre en compte la qualité d'image acquise) et multi instance de 3 doigts De la main gauche pour ajouté plus de sécurité et réduire le taux d'erreur comme nous avons vu déjà dans le deuxième chapitre concernant les bien fait de la multi modalité).

Lors de test on va fusionner les quatre scores des échantillons de la même instance, après

en combine les trois scores de trois instances, en sortant avec un score global, en utilisant une simple méthode; la somme pondérée qui est décrite dans 2.3.2 avec un poids équilibré égal a un.

4.2.4 Module de décision

dans cette étape nous avons en entré une matrice de similarité qui contient touts les scores fusionnés, et le système accepte le client s'il possède un score maximal (nombre maximal de couple du point d'intérêt).

4.3 résultat expérimental

4.3.1 Matériel utilisé et recommandé

TABLE 4.2 – Description du matériel utilisé et du matériel recommandé pour l'application de la fusion d'empreintes.

Matériel utilisé			
Modèle	Processeur	Mémoire vive	Système d'exploitation
LENOVO Idealpad Z570	Intel®Core (TM)i7-2670QM CPU@2.20ghz	6.00 Go	Windows 7 Professionnel
Matériel recommandé			
	Tout processeur INTEL ou AMD * x86 supportant les instructions SSE2	1.00Go	Windows xp Service pack2

4.3.2 Langage de programmation utilisé

Matlab est une abréviation de MATrix LABoratory [Radi, 2018], Une traduction littérale nous amène à voir MATLAB comme un laboratoire pour manipuler des matrices.
En effet, Matlab est très performant dans la manipulation de vecteurs ou de matrices : il est alors dans l'intérêt du programmeur d'´eviter un maximum les boucles habituelles dans d'autres langages. Matlab est un environnement puissant et facile à utiliser destiné au calcul scientifique.il apporte aux ingénieurs, chercheurs et à tout scientifique un system interactif intégrant calcul numérique et visualisation.
Ce langage comprend de nombreuses fonctions prédéfinies pour le calcul matriciel, specifique à des domaines, regroupées dans des TOOLBOX (que l'on peut traduire par "boîte à outils"). Ces toolbox sont des extensions évidemment payantes utiles, voire nécessaires, pour des développements de niveau professionnel. On peut citer les extensions :

- OPTIMIZATION pour l'optimisation.
- image processing pour le traitement d'image. Les domaines couverts sont très varié et comprenant notamment.
- le calcul numérique dans le corps des réels ou des complexes.
- le calcul de probabilités ou les statistiques.
- le calcul intégral ou la dérivation.
- le traitement du signal.
- l'optimisation.
- l'automatisme.
- le traitement d'image.

C'est un environnement performant, ouvert et programmable qui permet de remarquables gains de productivité et de créativité.

Quelles sont les particularités de Matlab ?

Matlab permet le travail interactif soit en mode commande, soit en mode programmation ;tout en ayant toujours la possibilité de faire des visualisations graphiques. Considéré comme un des meilleurs langages de programmation(C ou fortran), Matlab possède les particularités suivantes par rapport à ces langages :

- La programmation facile ;
- La continuité parmi les valeurs entières, réelles et complexes ;
- La gamme étendue des nombres et leurs précisions ;
- La bibliothèque mathématique très compressive ;
- L'outil graphique qui inclut les fonctions d'interface graphique et les utilitaires ;
- La possibilité de liaison avec les autres langages classiques de programmation(C ou Fortran)

Notons enfin que MATLAB peut être exécuté sur les plates-formes les plus courantes : linux, mac os X ou Windows.

Versions utilisées :

MATLAB R2013a et MATLAB R2017a,ce dernier offre plus de fonctionnalités, mais nessecite une confuguiration puissante de PC.

4.3.3 Base de données utilisée

Nos expériences ont été menées sur la sous base de données d'empreinte digitale de SDUMLA-HMT [Yin et al., 2011](mentionné dans le chapitre 2 : 2.4.7. Elle comprend des images acquises par 5 capteurs différents sur 1 personne. Pour chaque personne, 6 doigts sont enregistrés : le pouce, l'index et le majeur de chacune des mains; chacun des doigts est acquis 8 fois (Tableau 5.1), nous avons sélectionné les 3 doigts de la main gauche.
Nous avons choisi les images prises du capteur AuthenTec AES2501, qui est un capteur de type capacitif utilisant la méthode de capture de balayage. ce qui nous donne des meilleures résultats.

De cette base, nous avons sélectionné 100 personnes, totalisant 2400 images. Il s'agit de données labellisées puisque les acquisitions sont rangées par dossier selon les individus avec un sous dossier par doigt. Le tableau 4.x donne une description de notre base.

Tableau 4.3 : Description de la base d'empreintes digitales

TABLE 4.3 – Déscription de la sous-base de données d'empreinte digitale.

Année	**Sujet**				capteurs	instances	échantillon	obs
	nombre	homme	femme	âge				
2010	106	61	45	17-31	5	6	8	Réel

Répartition de la base de données

Répartition de la base de données Afin de développer une application de reconnaissance, 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, notre base a été scindée de la façon suivante (Figure 4.13) :

- **Images d'apprentissages** : La première, la troisième, la cinquième, et la Septième image de chaque personne servent pour la phase d'apprentissage (4/8).
- **Images de Tests** : Les 4 images restantes de chaque individu nous ont servi pour la réalisation des différents tests.

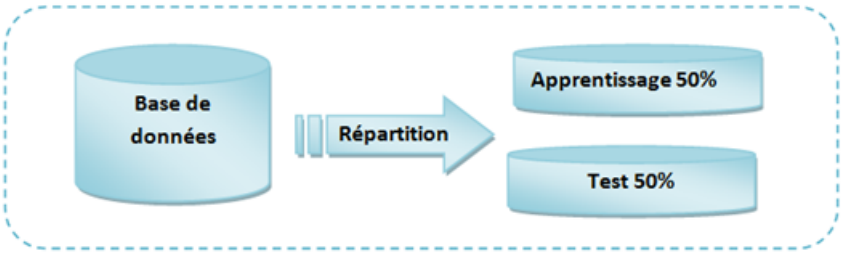

FIGURE 4.13 – Repartition de la base de données.

4.3.4 Présentation de l'application

FIGURE 4.14 – Interface Principale de l'application.

Interface Apprentissage (Ajouter une personne)

FIGURE 4.15 – Interface d'enrôlement.

1. Sélection d'un sujet

2. Sélection d'instance
3. Sélection d'échantillon
4. l'extraction des caractéristiques
5. Enregistrement dans la base de données
6. Vider tout les champs
7. Enregistrement automatique de 100 sujets avec 3 instances et 4 échantillons

- Apres l'ajout d'un individu dans la base de données, une boite d'information s'affiche (figure 4.16).

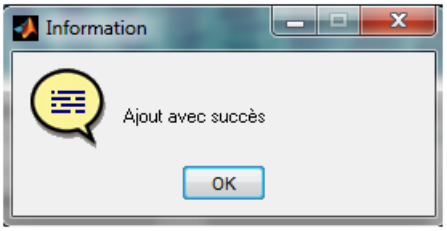

FIGURE 4.16 – Enregistrement avec succès.

Interface Identification

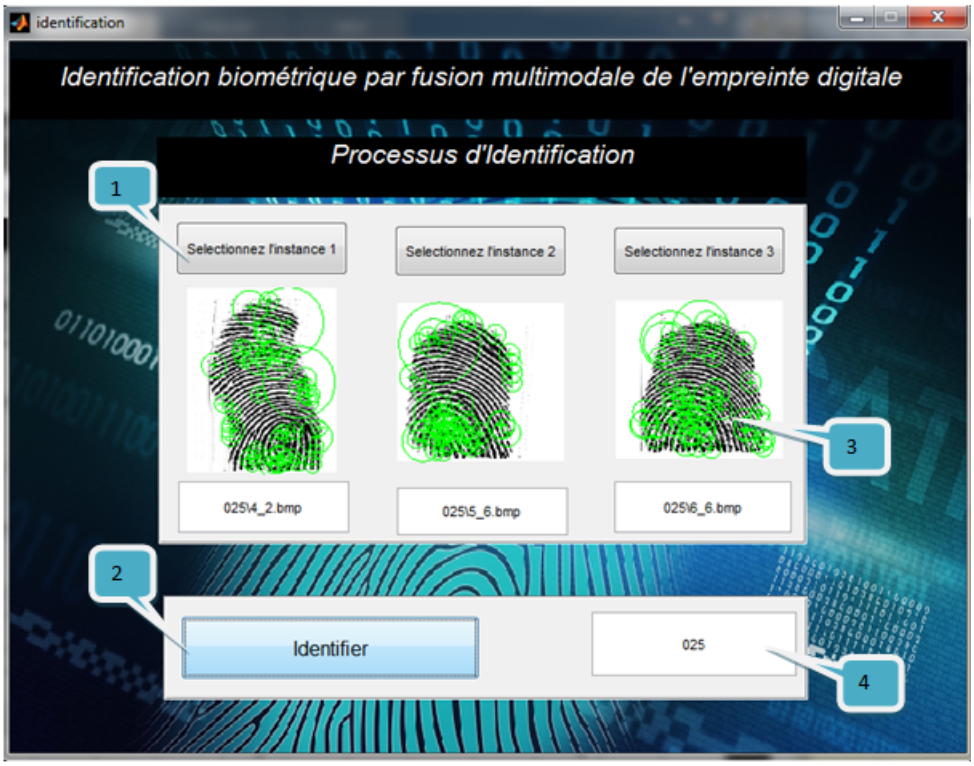

FIGURE 4.17 – Interface d'identification.

1. Sélection de l'instance
2. Lancement de processus d'identification
3. Affichage des points clé après l'extraction
4. Affichage de résultat

Interface d'authentification

FIGURE 4.18 – Interface d'authentification.

1. Sélectionner les instances.
2. Entrer le pseudonyme pour la vérification.
3. Lancer la vérification

On a 3 cas :

1. Le cas d'un client accepté :

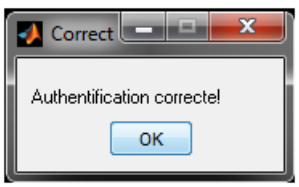

FIGURE 4.19 – Client.

2. Dans le cas d'un imposteur :

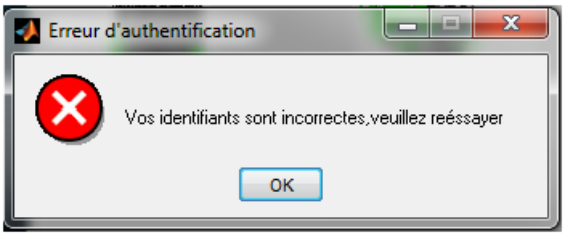

FIGURE 4.20 – Imposteur.

4.4 Evaluation de performance

Dans cette section, nous présentons les résultats des expériences menées sur la base de données SDUMLA HMT.

Dans le scénario d'identification, la performance de l'approche proposée est présentée sous forme de taux de reconnaissance et de courbes CMC. Dans le scénario d'authentification, la performance de l'approche proposée est présentée sous forme de taux de vérification (VR) et de courbes ROC.

1. **Taux de classification**

   L'algorithme SURF détecte un nombre variable de points d'intérêts pour les empreintes de la galerie et les empreintes test, ce qui forme un dictionnaire.
   Sa taille a un impact direct sur la performance de reconnaissance, un dictionnaire de petite taille accélère le calcul, mais cela entraîne une dégradation importante des performances de reconnaissance.
   Il peut exister entre 800 et 1500 points d'intérêts retournés par le détecteur SURF sur chaque empreinte. Cela rend le dictionnaire grand et augmente ainsi le coût de calcul de l'approche proposée.
   L'effet de la taille du dictionnaire (nombre de points) sur la performance de l'approche proposée pour la reconnaissance des empreintes est étudié.

   Nous évaluons expérimentalement ce nombre dans la tâche de classification en augmentant le nombre de points progressivement et en calculant le taux de classification correct.
   la précision de reconnaissance augmente considérablement avec l'augmentation de la taille du dictionnaire, comme le montre la figure 4.4

Ainsi, nous remarquons clairement l'amélioration du taux de reconnaissance de notre système par rapport systeme uni-modale.

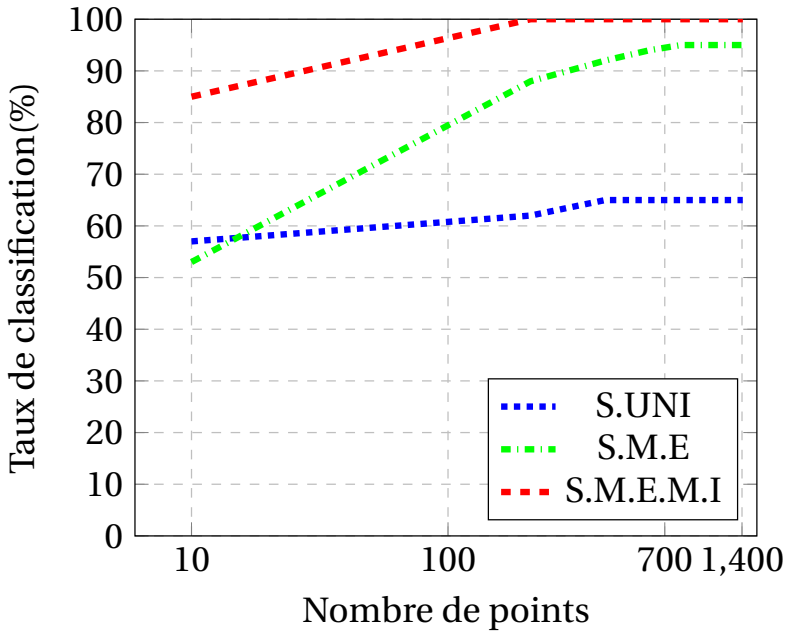

FIGURE 4.21 – Èvalution du taux de classification en fonction du nombre de points utilisés dans les trois systemes :uni-modal,multi-échantillon et multi-instance multi-échantillon.

En outre, nous avons comparé trois systèmes en changeant que le nombre de doigts, Les résultats ulistré dans la figure 4.22démontrent l'utilité de la fusion pour améliorer la précision,avec 3 doigts en a obtenu un taux ideal 100%

2. **la courbe CMC**

Afin d'évaluer la performance de notre approche, nous allons choisie la courbe CMC (Cumulative Match Caractéristique), Cette courbe affiche le taux d'identification cumulé en fonction de rang de la distribution. Ceci fournit une indication du degré de proximité pour obtenir la correspondance correcte si la correspondance au rang-1 est incorrecte.
Comme le montre la figures 4.4, notre approche donne des meilleurs résultats par rapport au deux autres systèmes(systeme uni-modale et systeme multi-échantillon), nous avons pu améliorer le taux de reconnaissance au rang1 de 65 %dans le système uni-modale a 86% en utilisant plusieur echantillon,et enfin, à 100% en utilisant l'instance répété et multiple comme montre la figure 2.

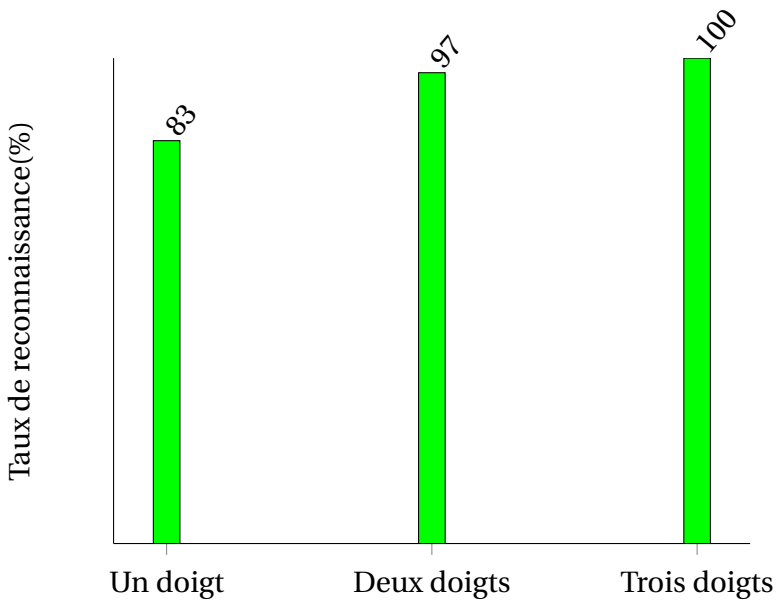

FIGURE 4.22 – La performance de l'approche proposée vs le nombre de doigts.

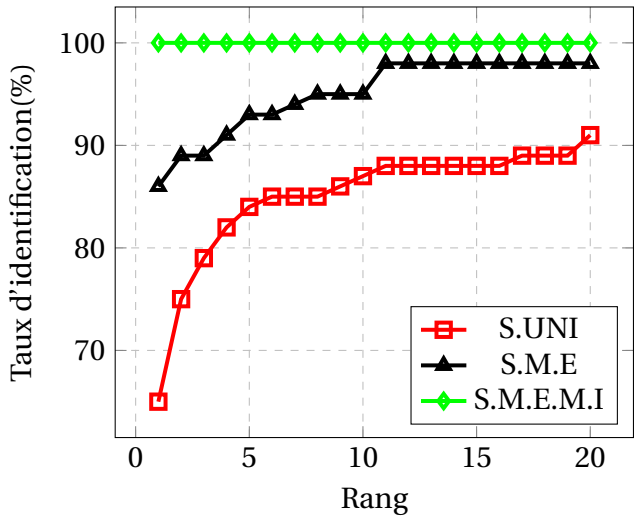

FIGURE 4.23 – Comparaison entre les courbes CMC :Notre approche Vs systeme uni-modale et systeme multi-echantillon.

3. **la courbe ROC**
   Une approche efficace devrait idéalement avoir des taux de vérification (VR) élevés associés à des faibles taux de fausse acceptation (FAR). On peut voir à partir de la figure 4.4 que le VR@0.1%FAR atteint 100% par notre approche par rapport a 65% par un système uni-modale.

La figure 4.4 justifie notre choix de trois doigts.

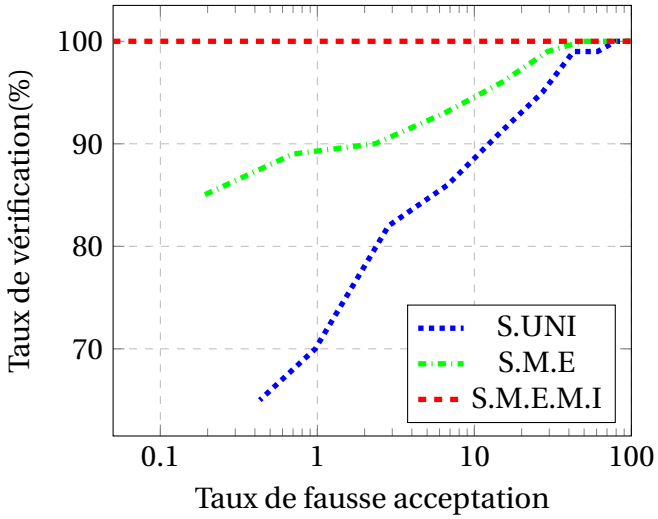

FIGURE 4.24 – Comparaison entre les courbes ROC :Notre approche Vs systeme uni-modal et Systeme multi-echantillon.

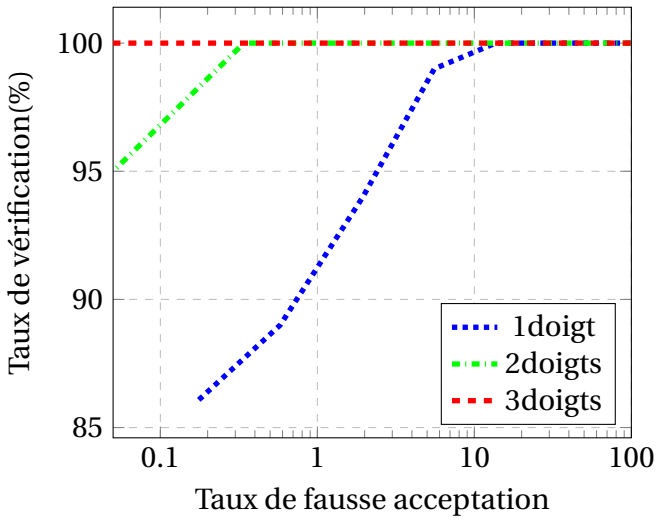

FIGURE 4.25 – Comparaison entre les courbes ROC :3 instances Vs 2 instances Vs 1 instance.

4.5 Conclusion

Dans ce chapitre, nous avons vu les étapes de conception d'une plateforme biométrique multimodale.
Sa représentation modulaire ainsi que la méthode utilisée pour extraire les informations nécessaires à partir des instances multiples et répétées pour chaque individu avec la modalité « empreinte digitale ».
Par la suite on a exposé les résultats obtenu lors de la phase de test d'évaluation de notre système on utilisant les courbes CMC et ROC.
Enfin, nous remarquons à travers les expériences effectuées, que la fusion multiple/répété au niveau de score des empreintes digitales donne un système multimodal performant comparé aux systèmes uni modaux, comme on a pu arriver à augmenter la fiabilité de la reconnaissance tout en maintenant un taux de reconnaissance idéal de 100% avec une solution simple, rapide et précise.

Conclusion générale

La biométrie, définit comme l'étude quantitative des caractéristiques biologiques, morphologiques ou comportementales de l'humain, est un champ de recherche très actif. A l'heure actuelle, les technologies biométriques sont basées le plus souvent sur la modalité d'empreinte digitale, qui est pour l'instant réputée parmi les plus fiables en contrepartie de leur caractère intrusif.

Les systèmes biométriques unimodaux souffrent de plusieurs problèmes qui sont à l'origine de l'utilisation d'un seul trait biométrique susceptible au bruit, à la mauvaise capture, à la pauvreté en matière de points biométriques confidents et notamment à la détérioration de la qualité de l'entrée biométrique. L'introduction de systèmes biométriques multimodaux est une solution à ces problèmes.

L'étude présentée dans ce mémoire traite l'authentification/identification automatique d'individus par instances multiples et répétées d'empreinte digitale, combinés au niveau de score,En profitant des avantages de l'algorithme SURF qui est invariant a l'échelle et la rotation, de plus de sa rapidité.

Aprés avoir introduit les concepts généraux en biométrie, nous avons détaillé les différents niveaux et techniques de fusions possibles dans un système biométrique multimodal, présenté un état de l'art en reconnaissance de l'empreinte digitale. Ensuite, nous avons implémenté et testé notre système afin dévaluer leur performance et avoir une vision claire de la robustesse de la phase de fusion.

Le processus de reconnaissance multimodal permet de renforcer les systèmes biométriques sur les plans de sécurité, fiabilité et pertinence. En effet, les tests que nous avons effectués ont montré l'intérêt de la fusion.
En perspective, il est souhaitable d'ajouter un module pour contrôler la qualité des données biométriques acquises pendant la phase d'enrôlement. Ainsi d'intégrer un module destiné à la sécurisation des données biométriques.

Bibliographie

Mr HADJAR Ahmed. Identification des individus par la biométrie multimodale. Master's thesis, UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE D'ORAN MOHAMED BOUDIAF, 2014.

Lorène Allano. *La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles*. PhD thesis, Evry, Institut national des télécommunications, 2009.

Harbi AlMahafzah, Mohammad Imran, and HS Sheshadri. Multibiometric : Feature level fusion using fkp multi-instance biometric. *arXiv preprint arXiv :1210.0818*, 2012.

S Asha and C Chellappan. Partial fingerprint matching using minutiae subset. In *Intelligent Computing, Networking, and Informatics*, pages 445–452. Springer, 2014.

Herbert Bay, Andreas Ess, Tinne Tuytelaars, and Luc Van Gool. Speeded-up robust features (surf). *Computer vision and image understanding*, 110(3) :346–359, 2008.

Rima Ouidad Belguechi. *Sécurité des systèmes biométriques : révocabilité et protection de la vie privée*. PhD thesis, Ecole nationale Supérieure en Informatique Alger, 2015.

TELIB Lina BENAGGA Abderahmane. Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt. 2016.

Ibtissam BENCHENNANE. *Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus*. PhD thesis, Université des sciences et de la technologie à Oran, 2015.

Samia BENTAIEB. *Reconnaissance de Visages en 3D*. PhD thesis, Mohamed Boudiaf, 2018.

Régis et Mainguet Jean-François Bourjot, Mathilde et Perrier. Etude d'algorithmes d'authentification pour petits capteurs d'empreinte digitale. In *CORESA 2017*, 2017.

Uwe M Bubeck. Multibiometric authentication. *Term Project CS*, 574, 2003.

Nesrine Charfi. *Biometric recognition based on hand schape and palmprint modalities*. PhD thesis, Ecole nationale supérieure Mines-Télécom Atlantique, 2017.

Xi Cheng, Sergey Tulyakov, and Venu Govindaraju. Multiple-sample fusion of matching scores in biometric systems. In *CVPR Workshops*, pages 120–125, 2011.

Xi Cheng, Sergey Tulyakov, and Venu Govindaraju. Minutiae-based matching state model for combinations in fingerprint matching system. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pages 92–97, 2013.

Moujahdi Chouaib. Protection des systèmes de sécurité biométriques : Contributions à la protection des modèles biométriques. 2014.

Stelvio Cimato, Marco Gamassi, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti. Privacy-aware biometrics : Design and implementation of a multimodal verification system. In *Computer Security Applications Conference, 2008. ACSAC 2008. Annual*, pages 130–139. IEEE, 2008.

Djamel Eddine DJILI, Abdellah et MAHDADI. Reconnaissance de personnes utilisant la multi-représentation de l'iris. 2016.

Julian Fierrez, Javier Ortega-Garcia, Doroteo Torre Toledano, and Joaquin Gonzalez-Rodriguez. Biosec baseline corpus : A multimodal biometric database. *Pattern Recognition*, 40(4) :1389–1392, 2007.

Julian Fierrez, Javier Galbally, Javier Ortega-Garcia, Manuel R Freire, Fernando Alonso-Fernandez, Daniel Ramos, Doroteo Torre Toledano, Joaquin Gonzalez-Rodriguez, Juan A Siguenza, Javier Garrido-Salas, et al. Biosecurid : a multimodal biometric database. *Pattern Analysis and Applications*, 13(2) :235–246, 2010.

Larousse Firm. *Grand usuel Larousse : dictionnaire encyclopédique*, volume 2. Larousse, 1997.

Itzhak Fogel and Dov Sagi. Gabor filters as texture discriminator. *Biological cybernetics*, 61 (2) :103–113, 1989.

Bindu Garg, Arjun Chaudhary, Kunal Mendiratta, and Vijay Kumar. Fingerprint recognition using gabor filter. In *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on*, pages 953–958. IEEE, 2014.

Ibrahim GHACHOUA, Abdelatif et KAHLAOUI. Reconnaissance de personnes en utilisant l'empreintes apprentissage l'sur basésmultispectral palmaires profondipa. 2017.

Romain Giot, Christophe Rosenberger, and Bernadette Dorizzi. Reconnaissance du genre par analyse de dynamique de frappe au clavier sur texte libre. In *7ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR-SSI 2012)*, pages 111–118, 2012.

Peter Gregory and Michael A Simon. *Biometrics for dummies*. John Wiley & Sons, 2008.

Umma Hany and Lutfa Akter. Speeded-up robust feature extraction and matching for fingerprint recognition. In *Electrical Engineering and Information Communication Technology (ICEEICT), 2015 International Conference on*, pages 1–7. IEEE, 2015.

Marine Campedel Oudot ; Pierre Hoogstoel. *Sémantique et multimodalité en analyse de l'information.* Lavoisier, 2011.

Andreas Humm, Rolf Ingold, Dijana Petrovska, Catherine Pugin, and Didier Von Rotz. Myidea-sensors specifications and acquisition protocol. *Pattern Recognition*, 2005.

AA Ilugbusi and OA Adetunmbi. Development of a multi-intance fingerprint based authentication system. In *Computing Networking and Informatics (ICCNI), 2017 International Conference on*, pages 1–9. IEEE, 2017.

Sundararaja S Iyengar, Laksham Prasad, and Hla Min. *Advances in Distributed Sensor Integration ; Application and Theory.* Prentice Hall PTR, 1995.

Anil Jain, Karthik Nandakumar, and Arun Ross. Score normalization in multimodal biometric systems. *Pattern recognition*, 38(12) :2270–2285, 2005.

Anil K Jain, Ruud Bolle, and Sharath Pankanti. *Biometrics : personal identification in networked society*, volume 479. Springer Science & Business Media, 2006.

Louisa Lam and SY Suen. Application of majority voting to pattern recognition : an analysis of its behavior and performance. *IEEE Transactions on Systems, Man, and Cybernetics-Part A : Systems and Humans*, 27(5) :553–568, 1997.

David G Lowe. Distinctive image features from scale-invariant keypoints. *International journal of computer vision*, 60(2) :91–110, 2004.

Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. *Handbook of fingerprint recognition.* Springer Science & Business Media, 2009.

Arjun V Mane, Yogesh S Rode, and KV Kale. Novel multiple impression based multimodal fingerprint recognition system. *International Journal of Computer Applications*, 27(8) : 26–31, 2011.

Adhiyaman Manickam, Ezhilmaran Devarasan, Gunasekaran Manogaran, Malarvizhi Kumar Priyan, R Varatharajan, Ching-Hsien Hsu, and Raja Krishnamoorthi. Score level based latent fingerprint enhancement and matching using sift feature. *Multimedia Tools and Applications*, pages 1–21, 2018.

Gian Luca Marcialis and Fabio Roli. Fingerprint verification by fusion of optical and capacitive sensors. *Pattern Recognition Letters*, 25(11) :1315–1322, 2004.

Alima Damak Masmoudi and Dorra Sellami Masmoudi. Implementation of a fingerprint recognition system using lbp descriptor. *Journal of Testing and Evaluation*, 38(3) :369–382, 2010.

Kieron Messer, Jiri Matas, Josef Kittler, Juergen Luettin, and Gilbert Maitre. Xm2vtsdb : The extended m2vts database. In *Second international conference on audio and video-based biometric person authentication*, volume 964, pages 965–966, 1999.

Tlili et Classe'A MC et Smaine Mazouzi et Bachir Boucheham et Mohammed Redjimi Mohammed, Benmohammed et Yamina. Systèmes multimodaux pour l'identification et l'authentification biométrique. 2010.

Hamrouni Nadia, Feddaoui et Kamel. Reconnaissance de l'iris par filtrage de gabor et deux variantes de descripteurs de texture, 2009.

Robert Newman. *Security and access control using biometric technologies*. Cengage Learning, 2009.

Timo Ojala, Matti Pietikainen, and David Harwood. Performance evaluation of texture measures with classification based on kullback discrimination of distributions. In *Pattern Recognition, 1994. Vol. 1-Conference A : Computer Vision & Image Processing., Proceedings of the 12th IAPR International Conference on*, volume 1, pages 582–585. IEEE, 1994.

Edouard Oyallon and Julien Rabin. An analysis of the surf method. *Image Processing On Line*, 5 :176–218, 2015.

Jacob Toft Pedersen. Study group surf : Feature detection & description. *Department of Computer Science, Aarhus University*, 2011.

Jean-Luc Perronnin, Florent et Dugelay. Introduction à la biométrie-authentification des individus par traitement audio-vidéo. *Traitement du signal*, 19(4), 2002.

P Jonathon Phillips, Kevin W Bowyer, and Patrick J Flynn. Comments on the casia version 1.0 iris data set. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(10) : 1869–1870, 2007.

Salil Prabhakar and Anil K Jain. Decision-level fusion in fingerprint verification. *Pattern Recognition*, 35(4) :861–874, 2002.

Abdelkhalak Radi, Bouchaïb et El Hami. *Méthodes numériques avancées sous Matlab® 1 : Approximation des fonctions et résolutions des systèmes linéaires*, volume 6. ISTE Editions, 2018.

Chunxiao Ren, Yilong Yin, Jun Ma, and Gongping Yang. A novel method of score level fusion using multiple impressions for fingerprint verification. In *Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on*, pages 5051–5056. IEEE, 2009.

Arun Ross and Anil Jain. Information fusion in biometrics. *Pattern recognition letters*, 24(13) : 2115–2125, 2003.

Arun A Ross, Karthik Nandakumar, and Anil K Jain. *Handbook of multibiometrics*, volume 6. Springer Science & Business Media, 2006.

Raul Sanchez-Reillo, Carmen Sanchez-Avila, and Ana Gonzalez-Marcos. Biometric identification through hand geometry measurements. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, 2000.

Conrad Sanderson and Kuldip K Paliwal. Information fusion and person verification using speech and face information. *Research Paper IDIAP-RR*, pages 02–33, 2002.

Elham Sedighi and Morteza Analoui. Combination of score level fusion methods in receiver operating characteristic space. In *Pattern Recognition and Image Analysis (IPRIA), 2017 3rd International Conference on*, pages 96–101. IEEE, 2017.

Danilo Simon-Zorita, Javier Ortega-Garcia, Marta Sanchez-Asenjo, and Joaquin Gonzalez-Rodriguez. Facing position variability in minutiae-based fingerprint verification through multiple references and score normalization techniques. In *International Conference on Audio-and Video-Based Biometric Person Authentication*, pages 214–223. Springer, 2003.

Nishant Singh, Kamlesh Tiwari, Aditya Nigam, and Phalguni Gupta. Fusion of 4-slap fingerprint images with their qualities for human recognition. In *Information and Communication Technologies (WICT), 2012 World Congress on*, pages 925–930. IEEE, 2012.

Shancymol Sojan and RK Kulkarni. Gabor feature extraction of mixed fingerprint template. In *Electrical, Instrumentation and Communication Engineering (ICEICE), 2017 IEEE International Conference on*, pages 1–5. IEEE, 2017.

Hafs Toufik. *Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne*. PhD thesis, UNIVERSITE BADJI MOKHTAR-ANNABA, 2016.

BUI Thanh Trung. Reconnaissance des empreintes digitales par lalgorithme sift. Master's thesis, Université de CAN THO ,Faculté de technologie de l'information et de la communication, 2011.

Andreas Uhl and Peter Wild. Single-sensor multi-instance fingerprint and eigenfinger recognition using (weighted) score combination methods. *International Journal of Biometrics*, 1(4) :442–462, 2009.

John D Woodward Jr, Christopher Horn, Julius Gatune, and Aryn Thomas. Biometrics : A look at facial recognition. Technical report, RAND CORP SANTA MONICA CA, 2003.

Amina YADDADEN, Yacine et SERIR. Authentification et/ou identification biométriques. 2010.

Bian Yang, Christoph Busch, Koen de Groot, Haiyun Xu, and Raymond NJ Veldhuis. Decision level fusion of fingerprint minutiae based pseudonymous identifiers. In *Hand-Based Biometrics (ICHB), 2011 International Conference on*, pages 1–6. IEEE, 2011.

Chunyu Yang and Jie Zhou. A comparative study of combining multiple enrolled samples for fingerprint verification. *Pattern Recognition*, 39(11) :2115–2130, 2006.

Yilong Yin, Lili Liu, and Xiwei Sun. Sdumla-hmt : a multimodal biometric database. In *Chinese Conference on Biometric Recognition*, pages 260–268. Springer, 2011.

Yanning Zhang, Zhi-Hua Zhou, Changshui Zhang, and Ying Li. *Intelligent Science and Intelligent Data Engineering : Second Sino-foreign-interchange Workshop, IScIDE 2011, Xi'an, China, October 23-25, 2011, Revised Selected Papers*, volume 7202. Springer, 2012.