الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

UNIVERSITE BADJI MOKHTAR - ANNABA
BADJI MOKHTAR – ANNABA UNIVERSITY

جامعة باجي مختار – عنابـــــــــة

Faculté : Sciences de l'Ingéniorat
Département : Electronique
Domaine : Sciences et Technologie
Filière : Télécommunications
Spécialité : Réseaux et télécommunications

Mémoire
Présenté en vue de l'obtention du Diplôme de Master
Thème :

Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus

Présenté par : *KHERICI LOUBNA et SADOKI NESRINE*

Encadrant : BOULMAIZ Amira *Grade* *MCB* Université de Badji Mokhtar, Annaba

Jury de Soutenance :

BOUTERAA Nadia	MCA	UBM Annaba	Président
BOULMAIZ Amira	MCB	UBM Annaba	Encadrant
MESSADEG Djemil	Professeur	UBM Annaba	Examinateur

Année Universitaire : 2019/2020

Résumé

Les systèmes biométriques multimodaux établissent l'identité sur la base de plus d'un trait biométrique. En tant que tels, ils sont aujourd'hui considérés comme une technologie de pointe, principalement en raison de leur capacité à fournir des niveaux accrus de précision et de sécurité.

Dans ce mémoire, nous proposons une solution utilisant les empreintes digitales et les veines des doigts, qui est robuste au déplacement des doigts. Tout d'abord, les images d'empreintes digitales sont améliorées au moyen d'un filtrage adaptatif où le filtre de Gabor joue le rôle le plus important. D'autre part, les images des veines des doigts nécessitent que le rectangle de délimitation soit détecté avec précision afin de se concentrer uniquement sur le motif biométrique utile. Au stade de l'extraction, les caractéristiques de niveau 2 sont extraites des empreintes digitales à l'aide de la fonction SURF. Les caractéristiques SIFT sont utilisées dans le cas de motifs de veines de doigts.

La solution que nous proposons, a obtenu des résultats légèrement meilleurs que les systèmes basés sur un seul module. Néanmoins, un système biométrique multimodal entièrement automatisé, interopérable au niveau des capteurs et invariant les rotations et les échelles, utilisant les empreintes digitales et les veines des doigts avec un taux de reconnaissance global de 95%, ainsi que son évaluation, peut être considéré comme une contribution au domaine de la biométrie.

Mots clé : Système Biométrique Multimodale, Empreintes digitales, Veine de doigts, filtre de Gabor, SURF, SIFT

Abstract

Multimodal biometric systems establish identity on the basis of more than one biometric trait. As such, they are now considered a state-of-the-art technology, mainly because of their ability to provide increased levels of accuracy and security.

In this brief, we propose a solution using fingerprints and finger veins that is robust to finger movement. First, fingerprint images are enhanced by means of adaptive filtering, where the Gabor filter plays the most important role. Secondly, finger vein images require that the boundary rectangle is accurately detected in order to focus only on the useful biometric pattern. At the extraction stage, the Level 2 features are extracted from the fingerprints using the SURF function. SIFT features are used for finger vein patterns.

The solution we offer has achieved slightly better results than systems based on a single module. Nevertheless, a fully automated multimodal biometric system, interoperable at the sensor level and invariant to rotations and scales, using fingerprints and finger veins with an overall recognition rate of 95%, as well as its evaluation, can be considered as a contribution to the field of biometrics.

Keywords: Multimodal Biometric System, Fingerprints, Finger vein, Gabor filter, SURF, SIFT

ملخص:

تحدد أنظمة القياسات الحيوية متعددة الوسائط الهوية على أساس أكثر من سمة بيومترية واحدة. على هذا النحو ، فهي تعتبر الآن تقنية حديثة ، ويرجع ذلك أساسًا إلى قدرتها على توفير مستويات متزايدة من الدقة والأمان.

في هذا الموجز ، نقترح حلاً باستخدام بصمات الأصابع وعروق الأصابع التي تكون قوية لحركة الأصابع. أولاً ، يتم الدور الأكثر أهمية. ثانيًا ، Gabor تحسين صور بصمات الأصابع عن طريق التصفية التكيفية ، حيث يلعب مرشح تتطلب صور وريد الإصبع أن يتم اكتشاف المستطيل الحدودي بدقة من أجل التركيز فقط على نمط المقاييس الحيوية المفيد. تُستخدم .SURF في مرحلة الاستخراج ، يتم استخراج ميزات المستوى 2 من بصمات الأصابع باستخدام وظيفة لأنماط وريد الإصبع SIFTميزات.

حقق الحل الذي نقدمه نتائج أفضل قليلاً من الأنظمة القائمة على وحدة واحدة. ومع ذلك ، يمكن اعتبار نظام المقاييس الحيوية متعدد الوسائط مؤتمت بالكامل ، وقابل للتشغيل البيني على مستوى المستشعر وغير متغير مع التدوير والمقاييس ، باستخدام بصمات الأصابع وعروق الأصابع بمعدل التعرف الإجمالي بنسبة 95٪ ، بالإضافة إلى تقييمه ، كمساهمة في المجال من القياسات الحيوية.

الكلمات الرئيسية :نظام المقاييس الحيوية المشروط ، بصمات الأصابع ، وريد الأصابع ، مرشح غابور ، SURF، SIFT.

Remerciement

Ce travail est l'aboutissement d'un long cheminement au cours duquel nous avons bénéficié de l'encadrement, des encouragements et du soutien de plusieurs personnes à qui nous tenons à dire profondément et sincèrement merci.

Tout d'abord, nous tenons à remercier le bon dieu le tout puissant de nous avoir donné la force et le courage de mener à bien ce modeste travail, également nous remercions nos parents pour leur encouragement et leur patience.

Tous nos infinis remerciements à notre encadreur Mm : ***Boulmaiz Amira*** *pour son aide, sa patience, ses conseils et ses remarques qui nous ont permis de présenter notre travail dans sa meilleure forme.*

Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre recherche en acceptant d'examiner notre travail de l'enrichir par leurs propositions.

Nous tenons à exprimer nos sincères remerciements à tous les enseignants du département ***d'Electronique*** *qui nous ont enseigné et qui par leurs compétences nous ont soutenu dans la poursuite de nos études.*

Enfin nous remercions tous nos proches, nos amis et tous ceux qui ont contribué de prés ou de loin à l'élaboration de notre travail trouvant ici l'expression de notre profonde gratitude et profonds respects.

Merci à tous et à toutes.

Dédicaces

A ma mère qui a toujours su m'écouter et pris le temps de m'entendre, sa tendresse est sa volonté ont toujours mérité mon plus profond respect.

A la mémoire de mon père, nous prions constamment le bon dieu, afin qu'il t'accorde sa miséricorde et t'accueille en son vaste paradis inchallah. Repose en paix inchallah.

A mon cher frère et mes chères sœurs.

A toute ma famille, mes oncles et mes tantes, mes cousins et cousines.

Tous mes amis en particulier.

Tous mes collègues pour lesquels j'ai gardé de bons souvenirs.

A ma chère binôme Loubna et toute sa famille.

Nesrine

Dédicace

Je dédie ce modeste travail

A ma très chère mère

A mon cher père

Qui ont beaucoup sacrifié pour moi durant toutes mes années d'études et sans lesquels je n'aurais Jamais réussi.

A mes frères et mes très chères sœurs

A toute ma famille

A mes ami(e)s, tout particulièrement ma chère binôme Nesrine qui m'ont toujours poussé et encouragé.

A tous mes enseignants du département d'Electronique durant mes années d'études avec lesquels j'ai beaucoup appris.

Liste des Tableaux

Liste des Figures

Liste des abréviations

Code PIN : Personal Identification Number

2D : Deux Dimensions

CCD : Dispositif Couplé Chargé

3D : Trois Dimensions

ROI : Region Of Interest

SURF : Speeded Up Robust Features

SIFT : Scale-Invariant Feature Transform

Rank-1 RR : Rank-One Recognition Rate

CMC : Cumulative Match Characteristic

FAR : False Accept Rate

FRR : False Reject Rate

EER : EqualError Rate

FR : Faux Rejets

FA : Fausses Acceptations

NL : Total légitimes

NI : Total imposteurs

ROC : Receiver Operating Characteristic

CED : Canny Edge Detector

MATLAB : MATrixLABoratory

URU4000 : optical finger print scanner

ZY202-B : optical finger print scanner

FT2BU : capacitance finger print scanner

FPR620 : optical finger print scanner

Liste des Symboles

θ : L'orientation du filtre.

f : La fréquence.

λ : Longueur d'onde.

σ_x, σ_y:Les écarts types de la courbe gaussienne.

x Et y : Le long des axes.

O : L'image d'orientation.

F : L'image de fréquence.

G : Le filtre de Gabor.

N : L'image normalisée de l'empreinte digitale.

w_x, w_y : Indiquent la largeur et la hauteur du masque filtrant de Gabor.

$\mathbb{L}_{ij}(x, y, \sigma)$: La dérivée seconde.

I : L'image de départ.

t : Le point de fonctionnement de référence.

$r1$ Et $r2$: Les bords gauche et droit de la région.

Table des matières

Chapitre II: Conception et réalisation d'un système de reconnaissance biométrique multimodal

Chapitre III: Simulations et résultats

Introduction générale

Introduction générale

De nos jours, on constate un intérêt accru dans les sociétés modernes avec le développement et le déploiement des technologies de l'internet et du web pour des méthodes permettant de vérifier ou d'identifier l'identité d'un utilisateur qui accède à distance. Les systèmes de sécurité traditionnels comme les serrures à clé ou les cartes d'identification sont également la cible d'une modernisation qui peut améliorer la sécurité des lieux critiques tels que les distributeurs automatiques de billets, les banques, les centrales nucléaires, etc. Ces scénarios et d'autres encore poussent au développement de systèmes plus sophistiqués basés sur des informations biométriques, étant donné l'impossibilité pour un individu malveillant de reproduire ces informations.

Ces systèmes sont généralement connus sous le nom de systèmes d'identification biométriques. Les systèmes par reconnaissance de formes peuvent identifier un individu par une caractéristique biométrique unique. Théoriquement, la caractéristique biométrique idéale pour l'identification humaine devrait inclure : être facile à extraire d'un individu, difficile à accéder par le grand public et difficile à reproduire par quelqu'un d'autre. Les systèmes d'identification biométrique sont largement répandus, depuis la sécurité de ces systèmes est prouvée. Ces systèmes présentent un grand nombre d'avantages par rapport aux autres systèmes traditionnels d'identification.

Bien que les techniques biométriques montrent leur puissance, ils ne peuvent pas garantir actuellement un taux de reconnaissance de 100% avec les systèmes biométriques uni-modaux basés sur une donnée biométrique ou signature unique. En outre, ces systèmes sont souvent affectés par les problèmes suivants: le bruit généré par le capteur, non universalité, la sensibilité aux attaques. Pour remédier à ces inconvénients, la solution est l'utilisation de plusieurs modalités biométriques au sein du même système; qui est appelé système biométrique multimodal qui est l'objectif principal de ce mémoire.
Il existe cinq types des systèmes multimodaux: multi-capteur, multi-instance, multi-algorithme, multi-échantillon et multi-biométries. Ces différents types de systèmes multimodaux pourraient réduire plusieurs problèmes rencontrés dans les systèmes uni-modaux.

Dans ce mémoire nous utilisons deux principales technologies biométriques à savoir l'empreinte digitale et les veines des doigts pour implémenter un système biométrique multimodal.

La première modalité : **la reconnaissance d'empreintes digitales**. Les empreintes digitales sont des traits anatomiques qui consistent en un motif de crêtes et de vallées. Ils sont considérés comme des identificateurs très anciens et fiables.

La deuxième modalité : **la reconnaissance par les veines des doigts**. La reconnaissance du dessin des veines du doigt est basée sur l'utilisation des motifs des vaisseaux sanguins à l'intérieur de son doigt afin de procéder à l'authentification de son identité. Cela a suscité un grand intérêt ces dernières années, car elle présente de nombreux avantages, tels que la facilité d'utilisation.

Notre mémoire sera structurée en trois grands chapitres :

CHAPITRE I : dans le premier chapitre, nous présentons les différentes notions de base de la biométrie à savoir la présentation générale des systèmes biométriques et les différentes modalités, les caractéristiques, et un aperçu sur la multi-modalité et leurs différentes architectures, à la fin de ce chapitre nous présentons les différents niveaux de fusion possibles et les techniques associées.

CHAPITRE II : le deuxième chapitre consiste à investir l'identification à base de l'empreinte digitale et de veines des doigts en utilisant différentes techniques, afin de sélectionner celle qui soit adéquate en temps de réponse et en taux de reconnaissance et aussi les techniques de fusions de scores issus des deux modalités sélectionnées.

CHAPITRE III : le troisième chapitre présente les résultats de simulations, une description sur la base de données utilisée et à la fin la discussion des résultats obtenue.
Et enfin nous terminons ce travail par une conclusion.

CHAPITRE I

La biométrie

I.1. Introduction :

Avec nos progrès vers une société de l'information mondialisée, la vie de l'individu moyen est en même temps menacée par des actes criminels qui peuvent avoir lieu n'importe où dans le monde. Les horreurs peuvent se propager dans le monde entier en un instant, augmentant et intensifiant le risque. Ainsi, les systèmes biométriques, qui sont très précis et utilisent une partie du corps, sont devenus la réponse idéale à ces besoins de sécurité accrus et sont déjà adoptés dans le monde entier.

La première question à laquelle il nous faut répondre est la suivante : *qu'est-ce que la biométrie?* Le mot biométrie désigne dans un sens très large l'étude quantitative des êtres vivants, mais dans notre contexte plus précis de reconnaissance et d'identification d'individus, il existe deux définitions principales qui se complètent:

- La biométrie est la science qui étudie à l'aide de mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé;
- Toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier l'identité qu'un individu affirme. [1]

La biométrie, est la science qui porte sur l'analyse des caractéristiques physiques ou comportementales propres à chaque individu, permettant l'authentification de son identité. Au sens littéral et de manière plus simplifiée, la biométrie signifie la « mesure du corps humain ». [2]

Les technologies biométriques sont des méthodes automatisées d'identification des individus basées sur la mesure statistique de caractéristiques physiologiques et/ou comportementales humaines uniques. Les caractéristiques physiologiques font référence aux traits héréditaires qui se forment dans les premiers stades embryonnaires du développement humain. La sécurité et la fiabilité sont élevées car les caractéristiques biométriques sont difficiles à reproduire et ne peuvent être volées.

I.2. Les modalités biométriques :

Il existe plusieurs modalités qui ont été utilisées dans divers systèmes biométriques. Dans cette section, nous allons mettre l'accent sur les modalités comportementales et morphologiques.

Figure I.1. Différentes modalités biométriques.

2.1.Les modalités morphologiques :

Ces modalités sont uniques et permanentes. Leur principe est basé sur l'identification de traits physiques particuliers de la personne, par d'exemple la forme de l'oreille, la thermographie faciale, la forme de la main, voir aussi la forme du visage, les empreintes digitales, l'iris, la rétine, etc.

1) L'empreinte digitale :

En matière de biométrie, la reconnaissance des empreintes digitales est encore l'approche la plus communément répandue. Une empreinte digitale est le dessin formé par un doigt sur un support suffisamment lisse pour qu'y restent marqués les dermatoglyphes.

Les empreintes digitales sont uniques à chaque individu et chaque doigt a son empreinte propre. La probabilité que deux personnes aient les mêmes empreintes digitales est infinitésimale : une chance sur 64 milliards.

Nous pouvons définir les empreintes comme suit : une empreinte digitale est une impression produite par la transpiration, la graisse, l'huile ou l'encre présente dans les lignes de crêtes non uniformes contenues dans la partie supérieure de chaque doigt de main d'un être humain. [3]

Il en existe trois grandes familles d'empreintes comme montre la figure suivante :

(a) (b) (c)

Figure I.2. Les familles d'empreintes :(a)Arche, (b) Boucle à droite, (c)Tourbillon.

2) L'iris :

Plusieurs entreprises développent et vendent des systèmes qui s'appuient sur l'iris humain pour reconnaître les personnes. L'iris est un mince diaphragme circulaire, qui se trouve entre la cornée et le cristallin de l'œil humain. L'iris est perforé près de son centre par une ouverture circulaire appelée pupille [3].

L'image de l'iris est capturée par un appareil qui contient une caméra infrarouge, lorsque la personne se place à une courte distance de l'appareil. La reconnaissance par iris est très utilisée dans les applications d'identification et de vérification, car il est hautement distinctif, unique, sa forme est stable et il est protégé et très robuste, toutefois les équipements d'acquisition coutent chères [4].

La reconnaissance par l'iris est utilisée aussi dans le secteur financier pour les employés et les clients, dans les hôpitaux et dans les grands aéroports [5].

Figure I.3.L'iris.

3) Le visage :

Le développement de systèmes biométriques basés sur la reconnaissance de la forme du visage est des plus récents [6].

La reconnaissance du visage est utilisée comme un système de surveillance ou d'identification par les autorités ou les corps policiers principalement dans les lieux publics. Elle est parmi les techniques les plus acceptables, mais elle nécessite un arrière-plan simple et fixe pour que le résultat soit précis [4].

Le problème de cette méthode vient des possibles perturbations pouvant transformer le visage (maquillage, faible luminosité, présence d'une barbe ou de lunettes, expression faciale inhabituelle, changement avec l'âge, chirurgie esthétique, environnement (condition d'éclairage), etc. [7]

Figure I.4. Système de reconnaissance du visage.

4) La voix :

C'est la seule technologie qui permet à l'heure actuelle de reconnaitre un individu à distance. Cependant, la reconnaissance vocale reste empêtrée dans ses limites : il est très difficile d'enregistrer et de reproduire une voix [7].

Les caractéristiques physiques de la voix d'un individu sont basées sur la forme et la taille des appendices (ex., les tractus vocaux, la bouche, les cavités nasales et les lèvres) qui sont utilisés dans la synthèse du son [2].

Elle nécessite une excellente qualité audio et un microphone afin de permettre la transcription sous forme d'un texte exploitable par la machine utilisée dans la synthèse du son.

La reconnaissance des locuteurs est plus utilisée par les téléphones, les corps policiers, les hôpitaux…etc. [4]

Figure I.5. Représentation temporelle de la parole

2.2.Les modalités comportementales :

La biométrie comportementale est liée à des caractéristiques comportementales dynamiques, par exemple votre façon de bouger, votre gestuelle très personnelle. L'exemple de biométrie physiologique le plus couramment utilisé est votre signature, mais les progrès technologiques permettent d'identifier d'autres caractéristiques comportementales personnelles et de les utiliser pour confirmer que nous sommes vraiment qui nous disons être! En conséquence, une modalité comportementale peut changer avec le temps. Voici quelques exemples de ce type de modalités biométrique : [5]

- La signature
- Dynamique de frappe au clavier
- La voix
- La démarche

I.3. Caractéristiques d'un système biométrique :

Un système biométrique typique peut être représenté par quatre modules principaux :

1) **Le module de capture :** est responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, etc.).
2) **Le module d'extraction de caractéristiques :** prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette

nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe.

3) **Le module de correspondance :** compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux.
4) **Le module de décision :** vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s). [1]

I.4. Modes de fonctionnement d'un système biométrique :

Les systèmes biométriques peuvent fournir trois modes de fonctionnement, à savoir, l'enrôlement, l'authentification (ou vérification) et l'identification.

I.4.1. Mode enrôlement :

C'est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données [3].

Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données.

I.4.2. Mode authentification :

L'utilisateur affirme son identité et le système vérifie si cette affirmation est valide ou non. Pour illustrer ce principe, prenons la situation où un utilisateur (M. X) souhaite retirer de l'argent à un distributeur de billets en entrant son code personnel d'identification (code PIN) et en présentant une modalité biométrique. Le système acquiert alors les données biométriques et va les comparer uniquement avec le modèle enregistré correspondant à M. X.

On parle alors de correspondance 1:1. Ainsi, si l'entrée biométrique de l'utilisateur et le modèle enregistré dans la base de données correspondant à l'identité affirmée possèdent un degré de similitude élevé, l'affirmation est validée et l'utilisateur est considéré comme étant un authentique. Dans le cas contraire, l'affirmation est rejetée et l'utilisateur est considéré comme étant un imposteur. En résumé, un système biométrique opérant en mode vérification répond à la question "Suis-je bien M. X ?".

I.4.3. Mode identification :

L'utilisateur ne dévoile pas explicitement son identité. Cependant, l'affirmation implicite faite par l'utilisateur est qu'elle est une des personnes déjà enrôlées par le système.

Ainsi, l'échantillon biométrique de l'individu est comparé avec les modèles de toutes les personnes de la base de données. On parle alors de correspondance 1:N. La sortie du système biométrique est constituée par l'identité de la personne dont le modèle possède le degré de similitude le plus élevé avec l'échantillon biométrique présenté en entrée. Typiquement, si la plus grande similarité entre l'échantillon et tous les modèles est inférieure à un seuil de sécurité minimum fixé, la personne est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système. Dans le cas contraire, la personne est acceptée [2].

I.5. Pourquoi la multi-modalité ?

Les systèmes biométriques uni-modaux ont des limitations dans la performance car ils sont basés sur le degré de correspondance entre les données biométriques comparées, qui ne permet pas une reconnaissance exacte d'un individu.

En effet, les systèmes biométriques sont souvent affectés par des problèmes comme le bruit du capteur, non universalité, manque d'individualité et la sensibilité aux attaques. Ainsi à causes de ces limitations, les taux d'erreurs associés aux systèmes biométriques uni-modaux sont élevés, ce qui les rend inacceptable dans un déploiement d'applications critiques de sécurité.

Pour pallier à ces problèmes, les chercheurs ont essayé toujours de voir d'autres façons pour améliorer la rentabilité des systèmes biométriques par l'utilisation de plusieurs modalités biométriques dans le même système, on parle alors de la biométrie ***multimodale.*** [8]

La biométrie multimodale désigne l'utilisation de plus d'une source d'information pour la reconnaissance d'un individu. Par exemple, un système biométrique multimodal peut utiliser la reconnaissance de l'iris et la reconnaissance de visage pour confirmer l'identité d'un utilisateur. L'utilisation de sources d'information multiples aide à résoudre certain des problèmes et limitations rencontrées précédemment par les systèmes uni-modaux (système monomodaux). On peut donc s'attendre à ce que les déploiements des systèmes biométriques multimodaux soient de plus courants dans le futur. [9]

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

I.6. Les types de fusion :

Il existe plusieurs types de scénarios de fusion de traits biométriques (Figure I.6) qui dépend essentiellement du type de sources et de caractéristiques utilisées :

I.6.1. Systèmes multiples biométriques :

Lorsque l'on considère plusieurs biométries différentes, par exemple visage et empreinte digitale. C'est le sens le plus classique du terme multimodal. Cette combinaison fournit une nette amélioration de la performance d'un système. Ces systèmes nécessitent différents capteurs ainsi que des algorithmes dédiés à chaque modalité biométrique.

Ce type de système a comme principale caractéristique, le fait que les caractères biométriques considérés peuvent être plus décorrelés par rapport aux systèmes multi-capteurs. [2]

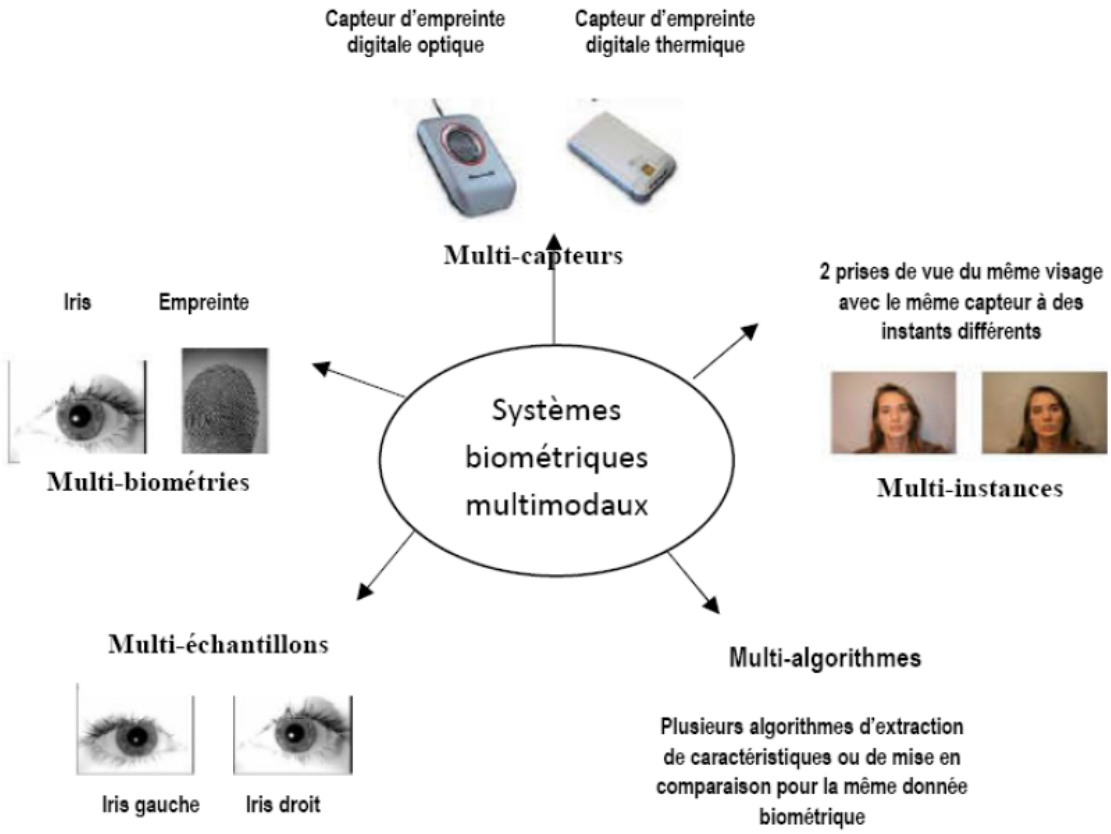


Figure I.6. Les différents types de fusion.

I.6.2. Systèmes multi-capteurs :

Dans ces systèmes, un même trait biométrique est analysé à l'aide de plusieurs capteurs afin d'extraire diverses informations provenant de l'enregistrement des images. Par exemple, un système peut enregistrer le contenu de la texture 2D du visage d'une personne avec une caméra CCD et la forme de la surface 3D du visage avec une autre gamme de capteurs dans le but de procéder 41 à la reconnaissance. Dans ce cas, c'est l'introduction des capteurs 3D servant à mesurer la variation de la surface du visage qui est responsable de l'augmentation du coût du système biométrique multimodal.

I.6.3. Systèmes multi-échantillons :

Un unique capteur peut être utilisé pour acquérir plusieurs échantillons du même trait biométrique dans le but de prendre en compte les variations qui peuvent se produire au sein de ce trait, ou pour obtenir une représentation plus complète du caractère sous-jacent. Par exemple, un système de reconnaissance faciale peut capturer (et enregistrer) le profil frontal du visage d'une personne ainsi que les profils gauches et droits afin de tenir compte des variations de la pose faciale.

I.6.4. Systèmes multi-instances :

Ces systèmes utilisent tout simplement plusieurs instances d'un même trait biométrique. Par exemple, les iris gauches et droits d'un individu peuvent être utilisés afin de vérifier son identité. Ces systèmes ne nécessitent généralement pas l'introduction de nouveaux capteurs, pas plus qu'ils n'entraînent le développement de nouveaux algorithmes d'extraction de caractéristiques ou de reconnaissance et sont, par conséquent, rentables. A titre d'information, les systèmes automatisés d'identification d'empreintes digitales ("*Automated Finger print Identification Systems*", AFIS) tirent profit de capteurs capables d'acquérir rapidement les empreintes des dix doigts d'un utilisateur.

1.6.5. Systèmes multi-algorithmes :

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

ne nécessite pas de capteurs supplémentaires et n'oblige pas l'utilisateur à interagir avec de multiples capteurs, d'où l'amélioration de la commodité d'utilisation. [1]

I.7. Conclusion :

Dans ce premier chapitre, nous avons décrit les technologies utilisées dans les systèmes biométriques pour l'identification des personnes, leurs fonctionnements et leurs différentes caractéristiques, ainsi nous avons donné un aperçu sur les techniques de mesure des performances des systèmes biométriques et montré les différentes modalités biométriques.

Nous avons aussi constaté que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre. On a conclu que l'une des solutions pour améliorer leur efficacité était la fusion de plusieurs modalités biométriques.

Ensuite on a présenté les architectures et les différents niveaux fusion qui peuvent être utilisés dans un système multimodal. La fusion se fait à plusieurs niveaux du système. Cependant, la combinaison de l'information est censée être plus efficace que la fusion a un niveau plus abstrait.

CHAPITRE II

Conception d'un système de reconnaissance biométrique multimodal

II.1. Introduction :

Les systèmes biométriques multimodaux établissent l'identité sur la base de plus d'un trait biométrique. En tant que tels, ils sont aujourd'hui considérés comme étant à la pointe de la technologie, principalement en raison de leur capacité à fournir des niveaux accrus de précision ainsi que de sécurité. Dans ce chapitre, nous proposons une solution utilisant les empreintes digitales combinées aux veines des doigts qui se trouve être robuste au déplacement des doigts ainsi qu'à la rotation.

II.2. Architecture du système multimodal proposé :

Dans cette section nous allons détailler les étapes de notre système de reconnaissance biométrique multimodale. L'architecture de ce dernier est illustrée dans la figure II.1.

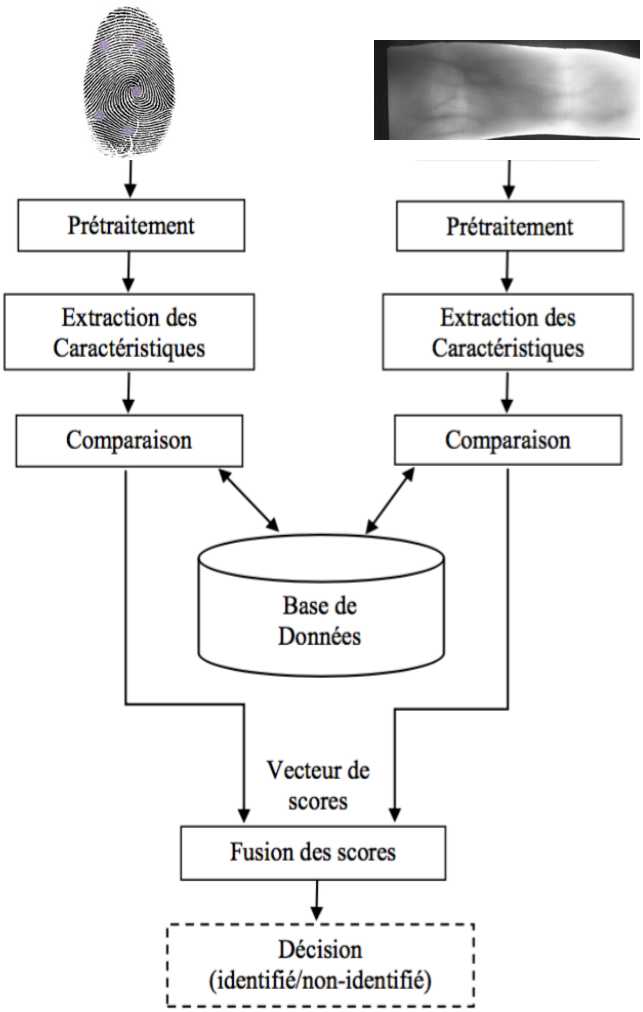


Figure II.1. Schéma du système de reconnaissance biométrique multimodal proposé

II.2.1. Système de reconnaissance basée sur l'empreinte digitale :

La reconnaissance de l'empreinte digitale est l'une des méthodes d'identification biométrique adoptée dans le monde entier. Tout d'abord, l'image est améliorée afin de garantir l'extraction fiable des éléments saillants, à savoir les points de détail.

Un système de reconnaissance des empreintes digitales est un système automatique de reconnaissance de formes qui se compose des trois étapes principales :

1) Module de prétraitement :

Les algorithmes de reconnaissance des empreintes digitales sont sensibles à la qualité des images de celles-ci. Le prétraitement est alors l'étape la plus essentielle dans le processus de reconnaissance entier. La qualité des images d'empreintes digitales dépend de plusieurs facteurs comme : le contact avec le sonde, la qualité de la sonde, la profondeur des crêtes /bifurcations, etc.

Généralement, le prétraitement se compose du lissage, l'amélioration de contraste, le filtrage de domaine fréquentiel. Sa première partie consiste en une segmentation des empreintes digitales pour empêcher le traitement ultérieur de l'arrière-plan. Dans les cas extrêmes, une empreinte digitale avec une qualité très pauvre peut être automatiquement renforcée en utilisant le filtrage de Gabor.

Ce module permet d'effectuer des tâches telles que l'alignement des images, le rehaussement ou l'identification des régions d'intérêt. [3]

L'une des étapes les plus importantes de la phase de prétraitement est le calcul de l'orientation de la crête locale. En outre, il est nécessaire pour déterminer l'orientation des points caractéristiques dans la phase d'extraction.

L'application du filtre de Gabor est, par calcul, l'étape la plus exigeante du prétraitement, le filtre lui-même fonctionne comme un filtre passe-bas qui élimine les hautes fréquences (par exemple, le bruit) et met en évidence les fréquences correspondant à la densité de la crête dans l'image de l'empreinte digitale.

$$G(x,y,\theta,f) = \exp\left\{-\frac{1}{2}\left[\frac{x_\theta^2}{\sigma_x^2}+\frac{y_\theta^2}{\sigma_y^2}\right]\right\}\cos(2\pi f x_\theta) \quad (1)$$

$$x_\theta = x\cos\theta + y\sin\theta \quad (2)$$

$$y_\theta = -x\cos\theta + y\sin\theta \quad (3)$$

Où θ est l'orientation du filtre. f Est l'onde co-sinusoïdale fréquence (f= 1/λ) et σ_x, σ_y étant les écarts types de la courbe gaussienne le long des axes x et y.L'application du filtre procède

par convolution spatiale de l'image de l'empreinte digitale avec le filtre de Gabor. L'image d'orientation O ainsi que l'image de fréquence F est nécessaire pendant la convolution de l'image. Par conséquent, l'image E avec le filtre de Gabor G appliqué est obtenue comme suit :

$$E(i,j) = \sum_{u=-\frac{w_x}{2}}^{\frac{w_x}{2}} \sum_{v=-\frac{w_y}{2}}^{\frac{w_y}{2}} G\big(u,v;O(i,j),F(i,j)\big)N(i-u,j-v) \qquad (4)$$

OùN est l'image normalisée de l'empreinte digitale etw_x, $w_y$indiquent la largeur et la hauteur du masque filtrant de Gabor.

La création du squelette est la dernière étape du prétraitement phase. La largeur des lignes de crête est réduite à 1px, ce qui se traduit par l'empreinte digitale étant présentée comme cette courbe noire.

2) Module d'extraction des caractéristiques :

Le module d'extraction de caractéristiques permet d'extraire la région d'intérêt et de la convertir sur un modèle approprié [5]. Après un prétraitement réussi, les caractéristiques saillantes sont extraites.

Dans notre travail en extraction des caractéristiques de l'empreinte digitale nous avons choisi d'utiliser la méthode SURF pour « Speeded Up Robust Features ».

L'algorithme SURF, que l'on peut traduire par caractéristiques robustes accélérées, développé par [22], est un détecteur et descripteur de caractéristique. 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 [16], qu'il surpasse en rapidité, Le détail de la méthode est présenté par la suite.

La méthode des SURF utilise le Fast-Hessien pour la détection de points d'intérêts et une approximation des ondelettes de Haar pour calculer les descripteurs.

Le fast-Hessien se fonde sur l'étude de la matrice hessienne :

$$\mathrm{H}(x,y,\sigma) = \begin{bmatrix} \mathbb{L}_{xx}(x,y,\sigma)\mathbb{L}_{xy}(x,y,\sigma) \\ \mathbb{L}_{xy}(x,y,\sigma)\mathbb{L}_{yy}(x,y,\sigma) \end{bmatrix} \quad (5)$$

Où $\mathbb{L}_{ij}(x,y,\sigma)$est la dérivée seconde suivant les directions en i et en j de $\mathbb{L}$ avec :

$$\mathbb{L}_{ij}(x,y,\sigma) = G(x,y,\sigma) * I(x,y) \quad (6)$$

Où,

$$G(x,y,\sigma) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{(x^2+y^2)}{2\sigma^2}} \quad (7)$$

Et I est l'image de départ. La maximisation du déterminant de cette matrice permet d'obtenir les coordonnées des points d'intérêts à une échelle donnée. Cette étape apporte une invariance des points d'intérêts par rapport à la mise à l'échelle.

Le déterminant est défini ainsi :

$$\det\big(\mathrm{H}(x,y,\sigma)\big) = \sigma^2(\mathbb{L}_{xx}(x,y,\sigma)\mathbb{L}_{yy}(x,y,\sigma) - \mathbb{L}_{xy}^2(x,y,\sigma) \quad (8)$$

Cette étape permet donc détecter les points d'intérêts candidats. L'algorithme comporte ensuite des étapes intermédiaires destinées à apporter plus de précision dans leur localisation.

Le calcul des descripteurs se fait grâce aux ondelettes de Haar. Elles permettent d'estimer l'orientation locale du gradient et donc d'apporter l'invariance par rapport à la rotation. Les réponses des ondelettes de Haar sont calculées en x et y dans une fenêtre circulaire dont le rayon dépend du facteur d'échelle du point d'intérêt détecté. Ces réponses spécifiques contribuent à la formation du vecteur de caractéristique correspondant au point clé.

3) Module de comparaison (Matching) :

Dans ce module, le système vérifie dans la base de données s'il existe des modèles similaires. La correspondance est traitée en calculant un score de similarité entre le nouveau modèle et le modèle stocké. La concordance n'est applicable que lors de l'identification ou de la vérification après que l'empreinte digitale fournie a été traitée. Cette étape conclut le processus de reconnaissance des empreintes digitales. [10]

L'empreinte digitale présente un intérêt certain dans la reconnaissance des individus compte tenu de son avantage (peu coûteuse, facilité d'utilisation, petite taille, La plus éprouvée et son traitement rapide).

Pour qu'un système d'identification soit robuste, on associe plusieurs méthodes d'identification biométrique en les combinant, dans notre cas nous avons concaténé l'empreinte digitale avec les veines des doigts.

II.2.2. Système de reconnaissance basée sur les veines des doigts :

Malgré les nombreux avantages de la reconnaissance basée sur les veines des doigts, il existe un certain nombre de défis à relever. Lors de l'acquisition, un mauvais éclairage ou un mauvais alignement de la position du doigt sont quelques-unes des circonstances qui peuvent réduire considérablement le taux de reconnaissance [11]. Il est donc nécessaire de mettre en place un processus de reconnaissance fiable.

1) Module de prétraitement et segmentation :

Habituellement, dans les systèmes biométriques basés sur l'image (par exemple, la biométrie des veines fines), un certain nombre de tâches de prétraitement sont nécessaires avant d'améliorer la qualité de l'image, telles que :la luminosité, l'information sur les bords, la suppression du bruit, la netteté de l'image, etc. En outre, la meilleure qualité d'image permettra d'obtenir un meilleur taux de reconnaissance de la part du système biométrique lui-même. [12]

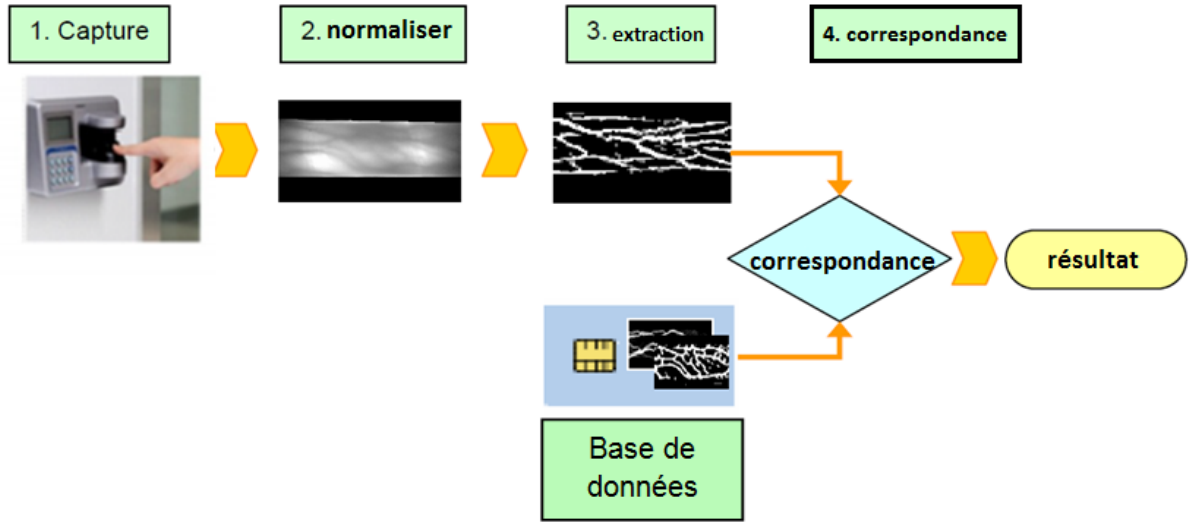


Figure II.2. Authentification fonctionnel des viens des doigts

Il existe quatre étapes dans le prétraitement comme suite :

A. Lissage des bords à l'aide d'un filtre bilatéral :

Afin de détecter de manière fiable les bords des doigts, nous les laissons en utilisant un filtre bilatéral. Car il nous aide à éliminer les bruits indésirables et sans en brouiller les contours.
Le filtrage bilatéral est une technique de dé bruitage effective de l'image. Il se base sur des gaussiennes spatiales et une intensité. Il permet de faire un lissage et d'éliminer des détails inutiles, avec l'avantage de préserver les contours entre les régions de l'image ; quand on fait le lissage on ne se déplace que dans les zones semblables [13]

B. Détection des bords par l'algorithme de Canny :

Après avoir aplani les bords, nous utilisons l'algorithme du détecteur de bord Canny (CED) sur notre image filtrée. Le résultat du CED est une matrice de la même taille que notre image recadrée, cependant, cette matrice ne contient que les valeurs 0 et 255. Si la valeur à (x, y) est 0, cela signifie que le CED n'a pas détecté de bord - comme le pixel à (x, y), donc ce pixel est noir dans la matrice du CED. Si la valeur à (x, y) est 255, alors ce pixel représente un bord - comme le pixel et ce pixel est blanc, respectivement. [14]

C. Calcul de contours :

OpenCV[1]fournit une implémentation pour trouver des contours, à savoir qu'il est appliqué sur la matrice Canny et donne un vecteur de vecteurs de points, où chaque vecteur représente un contour particulier, tandis que chaque point représente un bord - comme un pixel dans la matrice Canny. Cette approche est utilisée pour simplifier la recherche de points finaux dans l'étape d'extraction du retour sur investissement. [10]

D. Extraction du ROI (Region Of Interest) :

L'étape la plus cruciale dans la phase de prétraitement des veines du doigt est l'extraction du retour sur investissement. Tout d'abord, nous trouvons le contour le plus long ainsi que le deuxième plus long dans le vecteur de contour. Ils représentent vraisemblablement les bords des doigts. Ensuite, dans chacun de ces contours, nous recherchons les points d'extrémité. Le candidat pour le point final est un point situé près de la limite de l'image. Ces points d'extrémité

[1]Open Computer Vision :est une bibliothèque graphique libre, initialement développée par Intel, spécialisée dans le traitement d'images en temps réel.

potentiels sont ensuite filtrés en balayant leur voisinage. Cela doit être fait afin d'éviter d'avoir un pixel de bruit aléatoire comme point final de retour sur investissement. Pour s'assurer que le candidat est un point d'extrémité valide, c'est-à-dire qu'il fait partie du bord du doigt, nous utilisons un algorithme qui balaye 50 bords voisins - comme des pixels. Avec l'aide de la matrice Canny, cette approche garantit une sélection fiable du point final.
Une fois le retour sur investissement extrait, nous le soumettons à un processus d'amélioration, à savoir l'égalisation de l'histogramme.

2) Module d'extraction des caractéristiques :

De nombreuses méthodes ont été proposées pour l'extraction de caractéristiques dans les veines des doigts. Cependant, même si elles offrent une grande précision, l'absence de rotation ainsi que l'invariance de l'échelle peuvent être considérées comme des inconvénients. À cette fin, nous avons décidé d'utiliser l'algorithme SIFT, introduit par D. Lowe [21].
SIFT fonctionne en cinq phases différentes. Premièrement, en balayant l'image entière, SIFT détecte les points d'intérêt potentiels qui sont invariants à l'échelle et à la rotation. Ensuite, les points clés sont sélectionnés en fonction de leur stabilité, c'est-à-dire que chaque point candidat passe par un test de détermination de l'échelle et de l'emplacement. À chaque emplacement de point clé, une ou plusieurs orientations sont attribuées en fonction des directions de gradient local. Autour de chaque point clé, les gradients locaux sont mesurés à l'échelle sélectionnée et sont désormais transformés en représentations, qui permettent un degré significatif de distorsion de la forme locale ainsi qu'un changement de luminosité.[16]

3) Module de comparaison (Matching) :

Lorsque les caractéristiques sont extraites, nous employons l'appariement *BruteForce*[2]d'OpenCV pour effectuer la comparaison des points clés.
Pour chaque descripteur du premier ensemble, l'appariement *BruteForce* trouve le descripteur le plus proche du second ensemble en essayant chacun des descripteurs. Le résultat est le vecteur des points clés appariés, alors que chacun d'entre eux contient la distance euclidienne comme attribut. Cela signifie que plus la distance est élevée, moins la correspondance est fiable.
Il en résulte un inconvénient de SIFT. En effet, nous avons découvert que SIFT est très sensible aux variations intra-classe. Cela signifie que si une empreinte d'un doigt particulier devait être

[2]BruteForce : présente le processus de base pour résoudre le problème.

scannée avec un contraste légèrement différent, cela pourrait entraîner la correspondance correcte de quelques points clés. [10]

4) Module de normalisation :

Avant de procéder à la fusion, les scores de concordance du module des veines du doigt doivent être normalisés (entre 0 et 1), puisque ces scores vont de 0 à ~500 (notons que ceux-ci représentent des distances).

Nous utilisons la fonction double sigmoïde pour la normalisation des scores qui fait correspondre les scores obtenus à l'intervalle [0,1]. Le score normalisé à l'aide de la fonction double sigmoïde est alors donné comme suit :

$$s'_k = \begin{cases} \dfrac{1}{1+\exp\left(-2((s_k - t)/r_1)\right)}, \text{if } s_k < t \\ \dfrac{1}{1+\exp\left(-2((s_k - t)/r_2)\right)}, \text{otherwise} \end{cases} \quad (9)$$

Où t est le point de fonctionnement de référence,$r1$ et $r2$ désignent les bords gauche et droit de la région dans laquelle la fonction est linéaire, c'est-à-dire que la fonction sigmoïde double présente des caractéristiques linéaires dans l'intervalle $(t - r1, t + r2)$. La valeur t est généralement choisie pour être une valeur de la région de chevauchement entre la distribution des scores réels et celle des scores imposteurs, alors que $r1$ et $r2$sont rendus égaux à l'étendue du chevauchement entre les deux distributions vers la gauche et la droite de t, respectivement.

II.2.3. Score - Fusion des Niveaux :

Plusieurs méthodes ont été proposées sur l'approche de la fusion au niveau du score. Cependant, nous avons mené nos expériences en utilisant les méthodes de fusion min, max, tanh, la somme et la moyenne.

La fusion des scores à l'aide des méthodes sélectionnées est réalisée comme suit [18].

- **La règle minimum (Min rule) :** c'est le score minimum des différentes modalités.

$$MS_{final} = min(MS_{fp}; MS_{fv}) \quad (10)$$

- **La règle maximum (Max rule) :** c'est le score maximum des différentes modalités.

$$MS_{final} = max(MS_{fp}; MS_{fv}) \quad (11)$$

- **La règle tanh (tanh rule) :**

$$MS_{final} = \tanh(MS_{fp}) + \tanh(MS_{fv}) \quad (12)$$

- **La règle somme (Sumrule) :** La règle de somme combine les scores en tant que transformation linéaire. Le produit, la somme, le minimum, le maximum ou la médiane.

$$MS_{final} = MS_{fp} + MS_{fv} \quad (13)$$

Où MS_{final}représente le score final de la concordance tandis que MS_{fp} et MS_{fv}indiquent le score de la concordance à partir de l'empreinte digitale et de la veine du doigt, respectivement.

- **La règle moyenne (mediumrule) :**

$$MS_{final} = (axMS_{fp} + bxMS_{fv})/2 \quad (14)$$

Où a et $b$représentent les poids attribués à chaque trait. Nous avons utilisé 0,5 pour a et b, respectivement.

II.2.4. Module de décision :

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

II.3. 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 :

- **En 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.
- **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.
- **FalseRejectRate (FRR)**, ou taux de faux rejets : exprime le pourcentage d'utilisateurs rejetés alors qu'ils devraient être acceptés par le système.
- **EqualError Rate (EER),** calculé à partir des deux premiers critères, il correspond à l'endroit où FAR = FRR. C'est le meilleur compromis entre les faux rejets et les fausses acceptations.

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

Et

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

Avec

FR : nb faux rejets.

FA : nb fausses acceptations.

NL : nb total légitimes.

NI : nb total imposteurs.

- **Vérification 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. [23]

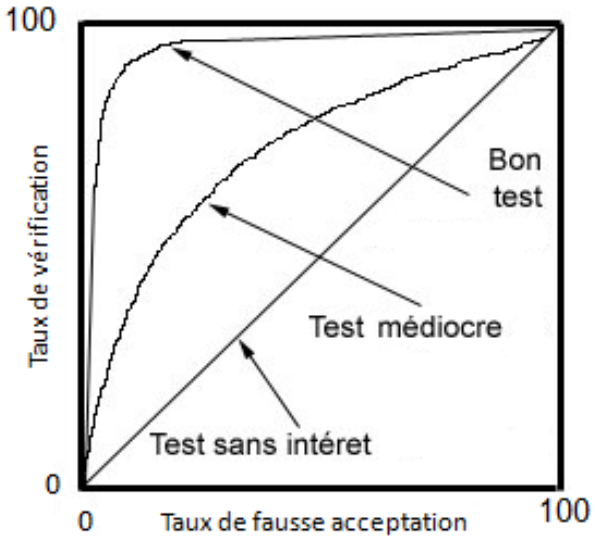


Figure II.3. Principes d'une courbe ROC.

II.4. Conclusion :

Dans ce chapitre, nous présentons un résumé de la recherche sur le système biométrique multimodal qui utilise les empreintes digitales et les veines des doigts, y compris le prétraitement, l'extraction et la correspondance des caractéristiques, ainsi que les niveaux fusion et la décision. Et enfin nous terminons par un état de l'art sur la fiabilité des systèmes biométriques.

CHAPITRE III

Simulations et résultats

III.1.Introduction :

Le présent chapitre est consacré à la présentation des tests effectués et les résultats obtenus. Nous étudions les performances des deux systèmes (veines et empreintes digitales) de façon séparée avant de présenter les résultats de nos combinaisons.

III.2. Paramètres et métriques de simulation :

III.2.1. Langage de programmation utilisé :

MATLAB est une abréviation de « MATrix LABoratory ». 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'éviter 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.

III.2.2. Base de données multimodale (SDUMLA-HMT) :

Pour évaluer notre système multimodal proposé, nous avons utilisé la base de données multimodale réelle SDUMLA-HMT [22]. La base de données des utilisateurs réels a été recueillie à l'université de Shangdong en 2010 auprès de 106 personnes (61 hommes et 45 femmes âgés de 17 à 31 ans) et comprenait cinq sous bases de données (visage, iris, veine digitale, empreintes digitales, démarche). Dans notre travail, nous utilisons deux sous bases de données : veines et empreintes digitales.

Année	**Sujet**				**Capteurs**	**Instances**	**Echantillon**
	Nombre	Homme	Femme	Age			
2010	106	61	45	17-31	5	6	8

TABLE III.1 – Description de la sous base de données d'empreinte digitale.

A. Base de données des empreintes digitales :

Les données d'empreintes digitales ont été obtenues à partir de cinq capteurs différents, cependant, notez que nous n'avons utilisé que les données de 4 capteurs (figure III.1). Les images provenant du cinquième capteur sont des empreintes digitales enregistrées par balayage.

Les images ont été prises à partir de six doigts, alors que huit empreintes ont été prises à partir de chaque doigt.

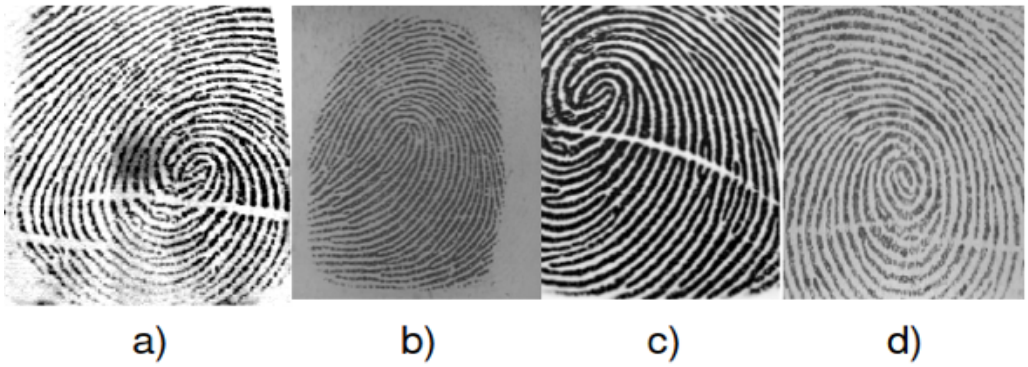


Figure III.1. Images d'empreintes digitales SDUMLA-HMT provenant de différents capteurs : a) URU4000B b) ZY202-B c) FT2BU d) FPR620

B. Base de données des veines digitales :

Les données relatives aux veines des doigts ont été obtenues à partir de six doigts de chaque sujet, tandis que six scanners supplémentaires de chaque doigt ont été effectués. [10]

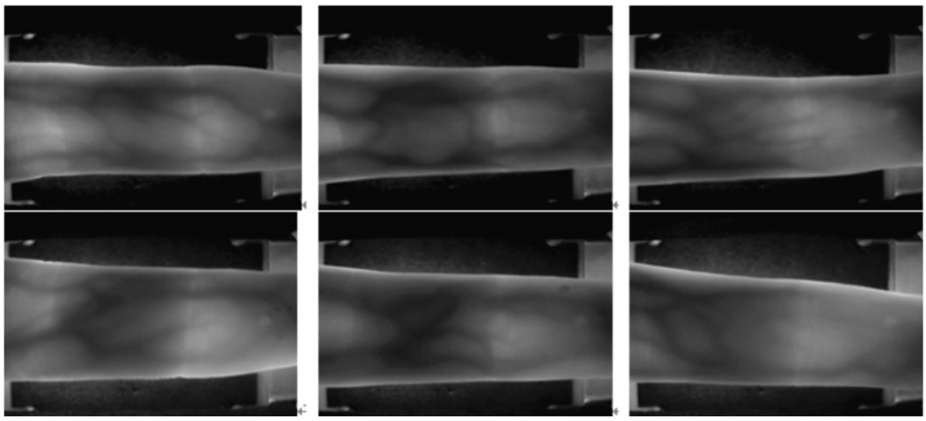


Figure III.2. Images de veines de doigts digitales de la base SDUMLA-HMT.

C. 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 :

- **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.

III.3.Résultats expérimentaux et évaluation de performance :

III.3.1. Système de reconnaissance basé sur les empreintes digitales :

A. Phase de prétraitement :

La figure III.3 représente le résultat de la phase de prétraitement décrite dans le chapitre II.

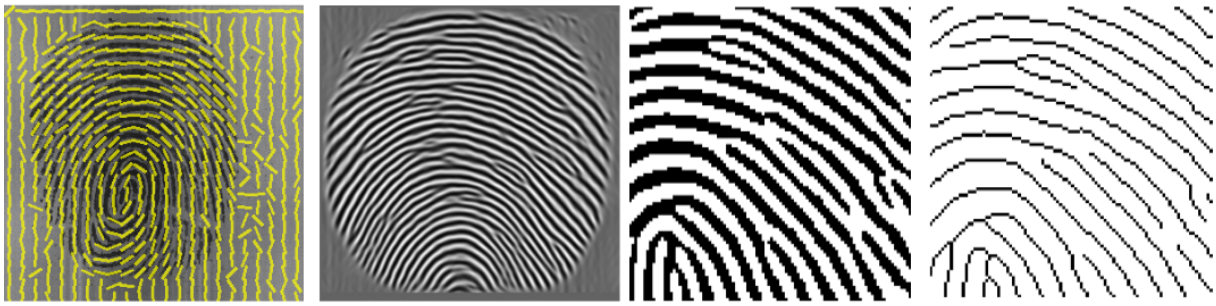


Figure III.3. a) Carte d'orientation ; b) Application du filtre de Gabor ; c) Image binaire ; d) Squelette de l'empreinte digitale

B. Phase d'extraction des caractéristiques :

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 per- formances 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 III.4

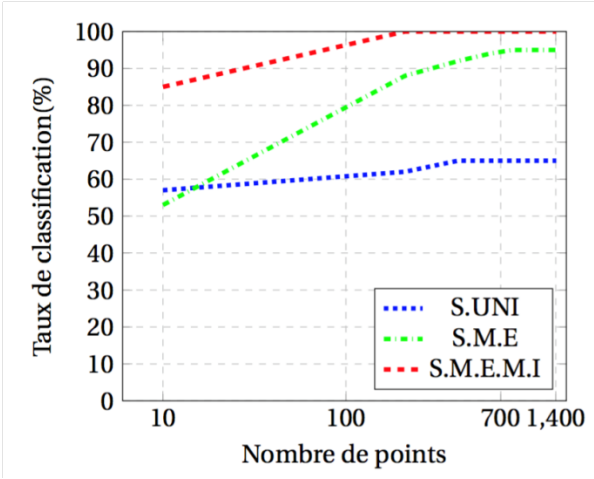


Figure III.4 – Evaluation du taux de classification en fonction du nombre de points utilisés dans les trois systèmes : uni-modal, multi-échantillon et multi-instance multi-échantillon.

III.3.2. Système de reconnaissance basé sur les veines :

A. Phase de prétraitement :

Puisque les images des veines du doigt provenant de la base de données SDUMLA-HMT contiennent du bruit latéral, nous recadrons légèrement chaque image. L'image originale est de taille 240 x 320 pixels, alors que notre image recadrée est d'une taille de 200 x 220 pixels. Cette résolution a été obtenue à partir de l'observation empirique. En outre, cela améliore sensiblement notre recherche de points finaux pendant l'extraction du retour sur investissement.

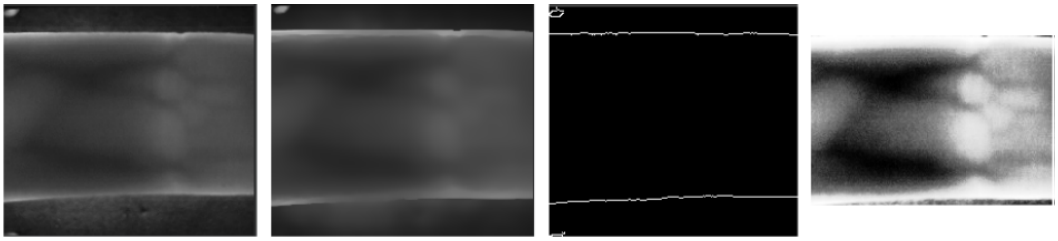


Figure III.5. Résultats du prétraitement de la veine du doigt. a) Original coupé ; b) Application bilatérale du filtre ; c) Détection du bord de Canny ; d) Région d'intérêt améliorée.

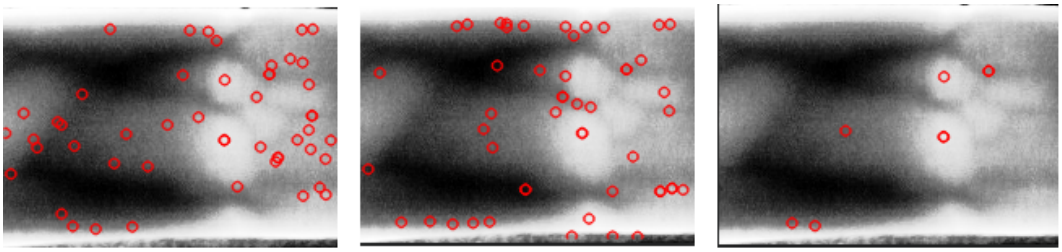
B. Phase d'extraction des caractéristiques :

La mise en œuvre de SIFT nécessite cinq arguments en entrée. Nous les avons définis comme suit :

- Le nombre de fonctionnalités à retenir est fixé à 50.

- Le nombre de couches d'octave est fixé à 3, puisqu'il s'agit de la valeur utilisée par Lowe dans son article [16].
- Comme le montre la figure III.6.c, le seuil de contraste plus élevé entraîne une diminution du nombre de points clés détectés. Pour cette raison, nous avons fixé le seuil de contraste à la valeur de 0,009.

Afin de filtrer les caractéristiques de type "edge", le seuil "edge" doit être à des valeurs inférieures. Par défaut, il est fixé à 10, mais un seuil plus élevé entraîne la détection d'un plus grand nombre de points clés sur les bords des doigts. Ces points clés ne peuvent pas être considérés comme une source d'information fiable. Nous avons donc fixé la valeur à 4, le sigma du gaussien appliqué à l'image d'entrée à l'octave no. 0 est laissé à 1,6, qui est sa valeur par défaut.



(a) **(b)** **(c)**

Figure III.6. Détection du point clé SIFT. a) Seuil du bord inférieur ; b) Seuil de bord plus élevé ; c) Seuil de contraste plus élevé.

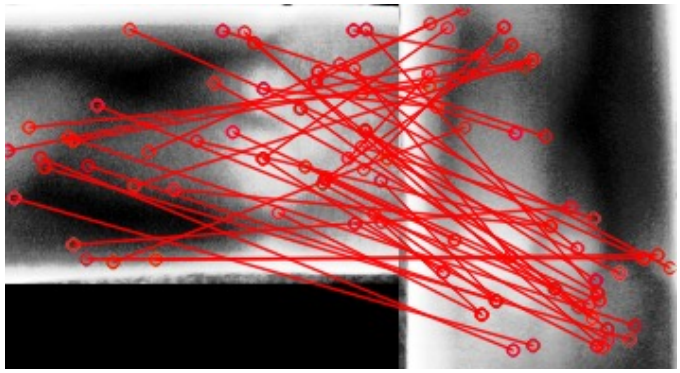


Figure III.7. Comparaison des points clés à l'aide de l'outil de comparaison *BruteForce*

La figure III.7 montre la distribution des authentiques et des imposteurs à partir de notre module de veines du doigt. Dans l'équation (II.9). Nous avons choisi la valeur 230 pour t, tandis que r1 et r2 sont tous deux fixés à 20.

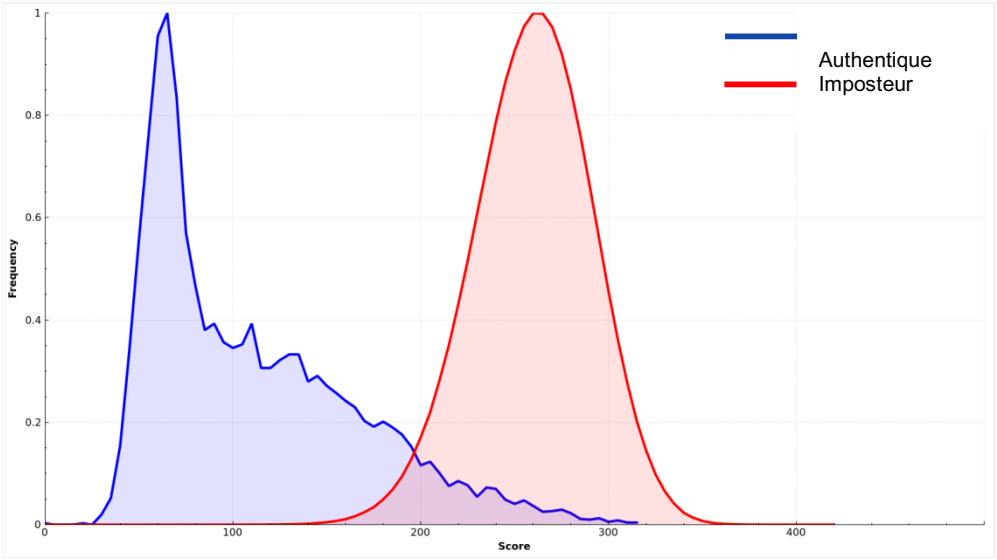


Figure III.8. Répartition des véritables et des imposteurs.

Les valeurs normalisées sont indiquées dans la figure III.8. Il convient de noter que la fréquence élevée des scores d'authenticité se situe autour de 1, tandis que la fréquence des scores d'imposture est plus élevée autour de 0. Cela montre que notre module de veines de doigt a permis de faire correspondre correctement différentes empreintes du même doigt comme étant authentiques, tandis que différentes empreintes de différents doigts ont été comparées comme étant des impostures, respectivement.

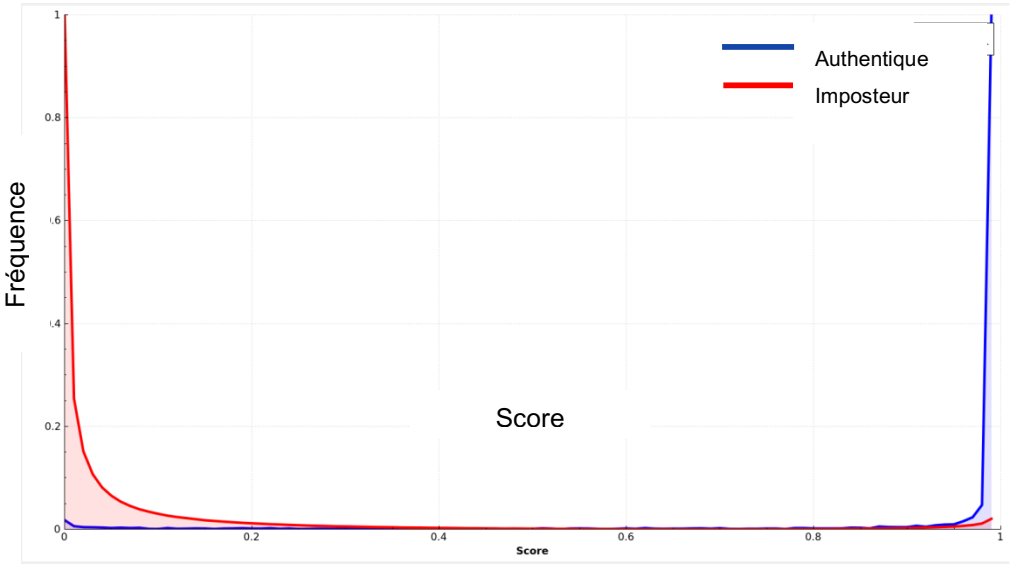


Figure III.9. Valeurs normalisées à l'aide de la fonction double sigmoïde.

III.3.3. Evaluation de performance :

Les indicateurs de performance généralement utilisés d'un système biométrique sont le taux de fausses acceptations (FAR), le taux de faux rejets (FRR), la courbe opérationnelle du récepteur (ROC) et le taux d'erreurs égales (EER). Une fausse acceptation se produit lorsqu'un score authentique tombe en dessous du seuil η, alors qu'un faux rejet est le résultat d'un score imposteur dépassant le seuil donnéη. Ainsi, la FAR représente une fraction des scores de l'imposteur qui dépassent le seuil η, tandis que la FRR marque une partie des scores réels qui ont dépassé le seuil η. Les courbes ROC sont principalement utilisés pour comparer les performances des systèmes biométriques différents où le FRR est tracé par rapport au FAR sur une échelle logarithmique. Le TRE indique le point où le FAR est égal au FRR. Un TRE plus élevé suggère donc une moins bonne performance du système.

Pour évaluer notre système, nous avons effectué plusieurs tests. Nous avons notamment testé la performance de chaque module, où un module particulier représente un système biométrique uni modal. Par la suite, nous avons effectué des tests sur les deux modules dans le cadre de notre système multimodal. Les tests du système multimodal ont été effectués en utilisant chacune des cinq méthodes de fusion susmentionnées. Comme le montre le tableau III.2, le taux moyen de reconnaissance de notre système multimodal est de 94%. Le meilleur score a été obtenu en utilisant le $tanh$ comme méthode de fusion.

Méthode de fusion	**Taux d'erreur**	**Taux de reconnaissance**
Min	6.2%	93.8%
Max	6%	94%
Tanh	5%	95%
Sum	5.47%	94.53%
Mean	5.4%	94.6%

TABLEIII.2. Résultats obtenus à l'aide de méthodes de fusion différentielle.

Un score notable a également été obtenu par chaque module, à savoir chaque système uni modal. Le taux d'erreur du système uni modal basé sur les empreintes digitales a atteint 5,7 %, tandis que son taux de reconnaissance était de 94,3 %. Le système uni modal basé sur les veines des doigts a également atteint une précision de reconnaissance notable de 93,9 % alors que son taux d'erreur était de 6,1 %, respectivement. Les résultats de performance présentés sur les

figures III.10 et III.11 illustrent les résultats obtenus par le système multimodal utilisant le $tanh$ comme méthode de fusion. Il est également important de noter concernant le graphique de la courbe ROC. Plus l'aire sous la courbe est grande, plus les performances d'un système particulier sont élevées.

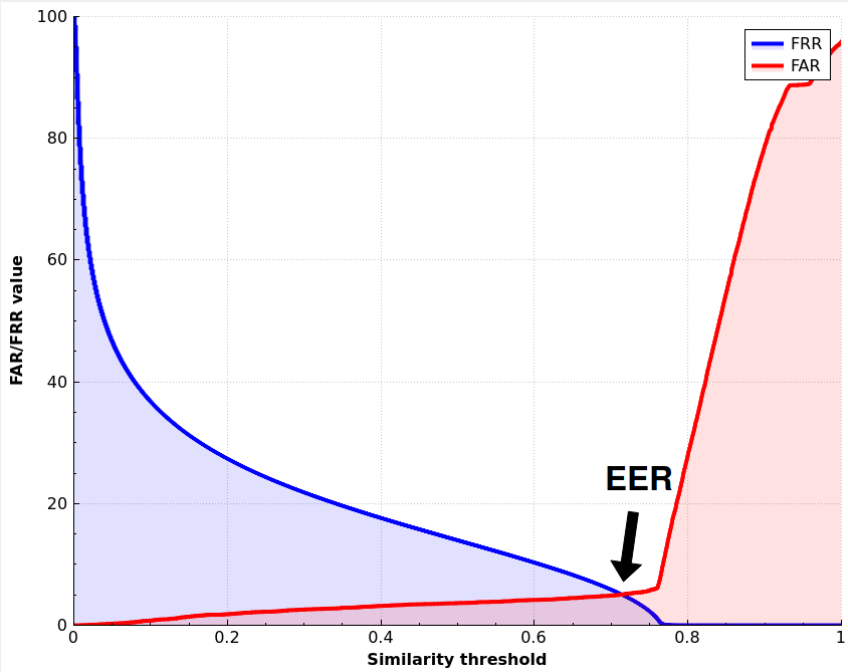


Figure III.10. Résultat FAR/FRR obtenu en utilisant le tanh comme méthode de fusion.

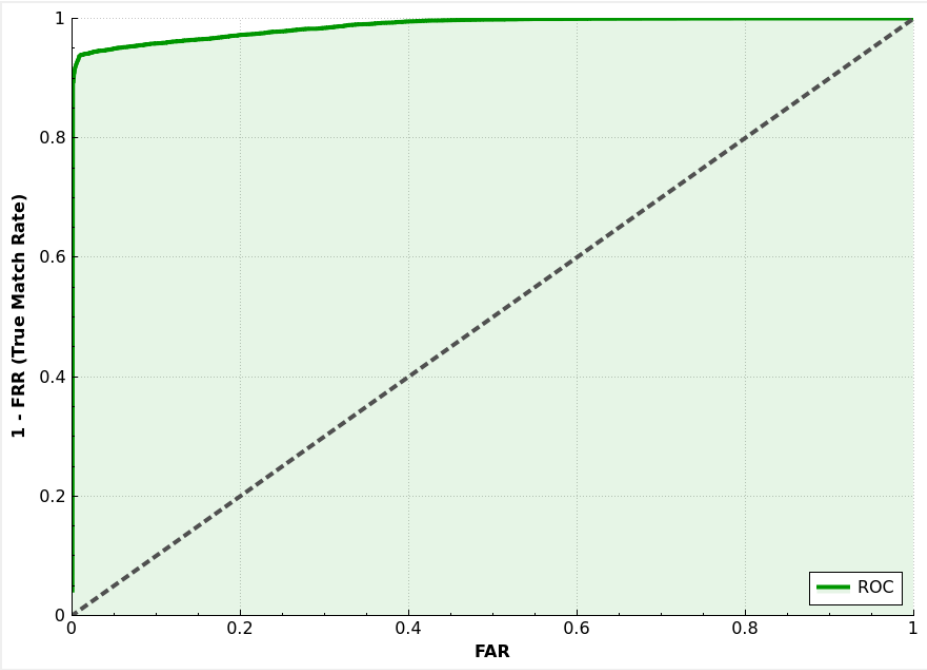


Figure III.11. Courbe ROC obtenue en utilisant le tanh comme méthode de fusion.

III.4.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 pour chaque individu avec la modalité « empreinte digitale » et la modalité « veine des doigts ». Par la suite on a exposé les résultats obtenus lors de la phase de test d'évaluation de notre système en utilisant les courbes FRR/FAR et ROC.

Enfin, nous remarquons à travers les expériences effectuées, que la fusion au niveau de score des empreintes digitales/veines des doigts 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 95%utilisant le $tanh$ comme méthode de fusion.

Conclusion générale :

Dans ce mémoire, nous avons proposé un système biométrique multimodal qui utilise les empreintes digitales et les veines des doigts. Le noyau est représenté par deux modules indépendants qui sont mis en œuvre sous forme de bibliothèques dynamiques. L'un utilise un réseau de neurones convolutifs afin d'extraire de manière efficace les caractéristiques saillantes, tandis que l'autre s'appuie sur des caractéristiques basées sur des points clés. Cependant, la solution que nous proposons, à savoir, a obtenu des résultats légèrement meilleurs que les systèmes basés sur un seul module. Néanmoins, un système biométrique multimodal entièrement automatisé, interopérable au niveau des capteurs et invariant les rotations et les échelles, utilisant les empreintes digitales et les veines des doigts avec un taux de reconnaissance global de 95%, ainsi que son évaluation, peut être considéré comme une contribution au domaine de la biométrie.

Bibliographie

[1]. Morizet, N. (2009). Reconnaissance biométrique par fusion multimodale du visage et de l'iris (Doctoral dissertation).

[2]. Hezil, N., &Boukrouche, A. (2017).Multimodal biometric recognition using human ear and palmprint. IET Biometrics, 6(5), 351-359.

[3]. Neves, J. R. G., &Correia, P. L. (2014, January). Hand veins recognition system. In 2014 International Conference on Computer Vision Theory and Applications (VISAPP) (Vol. 1, pp. 122-129). IEEE.

[4]. Boussafeur, Y., &Yeddiou, I. (2017). La biométrie multimodale basée sur la fusion de la reconnaissance de visage et l'empreinte palmaire.

[5]. Toufik, H. (2016). Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques: l'empreinte digitale et la signature manuscrite cursive en ligne (Doctoral dissertation, PhD thesis, UNIVERSITE BADJI MOKHTARANNABA).

[6]. BENCHENNANE, I. (2015). Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus (Doctoral dissertation, University of sciences and technology in Oran).

[7]. Dib, F. (2018). Identification des personnes par le réseau veineux de la main (Doctoral dissertation).

[8]. IDRIGUEN, S., & BAHLOUL, W. (2018). Réalisation d'un Système de Reconnaissance Biométrique Multimodal (Doctoral dissertation, Université AkliMouhandOulhadj-Bouira).

[9]. NOUAR, L. (2018). Identification Biométrique par Fusion Multimodale (Doctoral dissertation).

[10]. Kovac, Ivan, and Pavol Marák. "Multimodal biometric system based on fingerprint and finger vein pattern."

[11]. Radzi, S. A., HANI, M. K., &Bakhteri, R. (2016). Finger-veinbiometric identification usingconvolutional neural network. Turkish Journal of Electrical Engineering & Computer Sciences, 24(3), 1863-1878.

[12]. Mulyono, David, and HorngShiJinn. "A study of fingerveinbiometric for personal identification." 2008 International Symposium on Biometrics and Security Technologies. IEEE, 2008.

[13]. Guemmini, Mourad. "Filtrage bilatérale appliqué sur des images bruitées." (2013).

[14]. YAZID, Zineb, and Ouafaa YAHI. Contours actifs Paramétriques pour la Segmentation d'images. Diss. Université AkliMouhandOulhadj-Bouira, 2017.

[15]. Zhang, David D. Automatedbiometrics: Technologies and systems. Vol. 7. Springer Science & Business Media, 2013.

[16]. Lowe, David G. "Distinctive image featuresfromscale-invariant keypoints." International journal of computer vision 60.2 (2004): 91-110.

[17]. Berredjem, Achref. "Lare connaissance des individus par leur empreinte des articulations des doigts." (2019).

[18]. LATHA, L.; THANGASAMY, S. Efficient approach to normalization of multimodal biometric scores. International Journal of Computer Applications, 2011, 32.10: 57-64.

[19]. Duque Vehils, J. M. (2011). Design and implementation of a finger vein identification system.

[20]. Shaheed, K., Liu, H., Yang, G., Qureshi, I., Gou, J., & Yin, Y. (2018). A systematic review of finger vein recognition techniques. Information, 9(9), 213.

[21]. Herbert Bay, Andreas Ess, TinneTuytelaars, and Luc Van Gopppol. Speeded-up robustfeatures (surf). Computer vision and image understanding, 110(3) :346–359, 2008.

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

[23]. AMARA fatima zohra, Identification biométrique par fusion multimodale de l'empreinte digitale (2018), université BELHADJ BOUCHAIB D'AÏN-TÉMOUCHENT