REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Kasdi Merbah Ouargla

Faculté des nouvelles technologies de l'information et de la communication

Département d'électronique et de télécommunications

Mémoire de fin d'étude en vue de l'obtention du diplôme de

Master, Filière: Télécommunications

Spécialité: Systèmes de Télécommunications

Thème

Reconnaissance des personnes par finger Vein

Présenté par:

- KHERROUBI MIMOUNA
- TIDJANI HALA

Soumis au jury composé de :

CHEBARA Fouad	**Professeur**	**UKM Ouargla**	**Président**
NASRI Nadjib	**MAA**	**UKM Ouargla**	**Examinateur**
CHAA Mourad	**MCA**	**UKM Ouargla**	**Encadreur**

Année Universitaire: 2020 / 2021

Remerciement

Tous d'abord, nous remercions le Dieu le tout puissant qui nous a donné la force, la patience, la volonté, et le privilège d'étudier et de réaliser ce travail.

Nous tenons à remercier notre encadreur monsieur Dr. **CHAA Mourad** qui a toujours montré l'écoute et li était très disponible tout au long de la réalisation de ce modeste travail et nos professeurs du département d'électronique et d'ingénierie.

Sans oublier nos parents qui nous ont apporté leur soutien et leur expertise et qui nous a donné le bon climat de travail.

Nous Remercions les membres du jury pour leurs éminentes contributions à l'évaluation de ce projet. Nous remercions tous les professeurs et le personnel administratif du Département d'informatique de l'Université kasdi Marbah.

Enfin, nous adressons nos plus sincères remerciements à tous les membres de la famille TIDJANI et KHERROUBI et tous nos proches et amis, qui nous ont toujours soutenu et encouragé au cours de la réalisation de ce travail.

DÉDICACE

Je dédie ce mémoire à mes chers parents ; ma mère Fatima Zouhra et mon père Mebrouk et mon mari Sami pour leur patience, amour, soutien et encouragements.

A mes sœurs et mes frères : Dalila, Chafik, Hanifa, Romaissa, Djaber, Abd El Ouadoud, Abd El Bari, Abd Ennour, Salsabil, Anfal.

A toute ma grande famille et à ceux et celles qui ayant une relation de près ou de loin avec ce modeste travail.

A mes amis et les collègues de la classe.

Sans oublier tous les enseignants qui ont contribué à ma réussite.

KHERROUBI Mimouna

DÉDICACE

Je dédie ce modeste travail à Mes chers parents,

Mon Père Mohammed Lamine et Ma Mère Latifa.

A mes frères Mohammed, Rabie, Imad et Bilal

A ma sœur Amani

Les femmes de mes frères Manel et Saida

A mon binôme Mimouna.

A celui qui m'a soutenu tout au long de ce projet

Mon mari Abd Elouahed.

A toute ma famille Tidjani,

Mes amies et mes collègues d'études.

A tous ceux qui ont contribué de prés ou de loin
pour que ce projet soit possible.

Je vous dis merci.

TIDJANI Hala

Résumé :

Les propriétés biologiques des individus ont été utilisées comme système de sécurité efficace dans ce que nous appelons un système biométrique.

L'objectif de ce travail est de développer un système d'identification des individus à partir de leurs veines de doigts qui sont uniques à l'individu.

Notre système est basé sur le principe d'apprentissage automatique, dont nous avons extrait des paramètres caractéristiques tels que Tan and Triggs Gamma correction et Dog. Ces paramètres seront l'entré du classificateur K-NN, SVM, Random Forest.

Après cette étape notre système sera capable de décider est-ce que une nouvelle personne appartient à la base ou non. Nous avons trouvé que la méthode KNN présente l meilleure valeur de l'accuracy acceptable qui atteint les 92%.

Mots-clés: système d'identification, veines de doigts, apprentissage, ROI , classificateur KNN, SVM, Random Forest, taux de reconnaissance(accuracy).

Abstract:

The biological properties of individuals have been used as an effective security system in what we call a biometric system.

The objective of this work is to develop a system for identifying individuals from their finger veins which are unique to the individual.

Our system is based on the principle of machine learning, from which we have extracted characteristic parameters such as Tan and Triggs Gamma correction and Dog. These parameters will be the input of the K-NN, SVM, Random Forest classifier.

After this step our system will be able to decide whether a new person belongs to the base or not. We have found that the KNN method presents the best value of acceptable accuracy which reached 92%.

Keywords: identification system, finger veins, learning, ROI, classifier K-NN, SVM, Random Forest, recognition rate (accuracy).

الملخص:

تم استخدام الخصائص البيولوجية للأفراد كنظام أمان فعال فيما نسميه نظام القياسات الحيوية.

الهدف من هذا العمل هو تطوير نظام للتعرف على الأفراد من أوردة الأصابع التي تكون فريدة بالنسبة للفرد.

يعتمد نظامنا على مبدأ التعلم الآلي ، والذي استخرجنا منه المعلمات المميزة مثل Random Forest, SVM, KNN ستكون هذه المعلمات هي مدخلات مصنف.

بعد هذه الخطوة، سيتمكن نظامنا من تحديد ما إذا كان شخص جديد ينتمي إلى القاعدة أم لا. لقد وجدنا أن طريقة تقدم أفضل قيمة للدقة المقبولة وصلت إلى 92 %.

الكلمات الدالة : نظام تحديد الهوية، أوردة الأصابع، التعلم، ROI، مصنف KNN، SVM، Random Forest، معدل التعرف (الدقة).

Liste de figure

Figure I.1: Exemples de modalités biométriques..... ……15
Figure I.2: principaux modalités biométriques..... ……16
Figure I.3: Reconnaissance par visage..... …...17
Figure I.4: Images de L'empreinte digitale ..... ……18
Figure I.5: Géométrie de la main ..... …19
Figure I.6: Quelques images des empreintes des articulations des doigts..... …19
Figure I.7: Image de L'iris..... ….21
Figure I.8: Image de la rétine..... ….21
Figure I.9: Image de signature..... ….22
Figure I.10: Image de la voix..... ……23
Figure I.11: Image d'un clavier……..23
Figure I.12: La Démarche ..... ……24
Figure I.13: Mode enrôlement d'un système biométrique ..... ……24
Figure I.14: Mode vérification d'un système biométrique..... ……25
Figure I.15: Illustration du FRR et du FAR ..... …...28
Figure I.16: Courbe du point d'équivalence des erreurs dans un système biométrique……...29
Figure I.17: Courbe DET..... ……29
Figure I.18: Les différents systèmes multimodaux..... ……31

Figure II.1: Schéma synoptique de système d'identification biométrique……..35
Figure II.2: Positionnement de la source lumineuse et du capteur d'image, à gauche: transmission de la lumière, à droite : lumière réfléchie……37
Figure II.3: ROI d'extraction……38
Figure II.4: Opérateur LBP de base……41
Figure II.5: Extraction de caractéristiques par LPQ et BSIF……...44
Figure II.6: Inception V3……..45
Figure II.7: Méthode des K plus proches voisins (KNN)……...46
Figure II.8: Algorithme de Random Forest……..47

Figure III.1: Organigramme d'identification biométrique (finger vein)……50
Figure III.2: Technique de normalisation Tan et Triggs……..50
Figure III.3: Montré un exemple d'image de profondeur corrigée avec différentes valeurs gamma……51
Figure III.4: Quelque exemple de Base de donnes……..52
Figure III.5: Exemple image de doigt annulaire droit avec la méthode tan et triggs……...53
Figure III.6: Exemple image de doigt majeur droit avec la méthode tan et triggs……...53
Figure III.7: Exemple image de doigt index droit avec la méthode tan et triggs……53
Figure III.8: Exemple image de doigt annulaire gauche avec la méthode tan et triggs……...53
Figure III.9: Exemple image de doigt majeur gauche avec la méthode tan et triggs……...53
Figure III.10: Exemple image de doigt doigt index gauche avec la méthode tan et triggs……..53

Liste des tableaux

Tableau III.1 : Le taux de reconnaissance de doigt annulaire droit avec les différentes valeurs de Gamma correction……...54
Tableau III.2 : Le taux de reconnaissance de doigt majeur droit avec les différentes valeurs de Gamma correction……54
Tableau III.3 : Le taux de reconnaissance de doigt index droit avec les différentes valeurs de Gamma correction……54
Tableau III.4 : Le taux de reconnaissance de doigt annulaire gauche avec les différentes valeurs de Gamma correction……...55
Tableau III.5 : Le taux de reconnaissance de doigt majeur gauche avec les différentes valeurs de Gamma correction……55
Tableau III.6 : Le taux de reconnaissance de doigt index gauche avec les différentes valeurs de Gamma correction……56
Tableau III.7: Le taux de reconnaissance de doigt annulaire droit avec les différentes valeurs de Dog (2 fixé)……..56
Tableau III.8: Le taux de reconnaissance de doigt majeur droit avec les différentes valeurs de Dog (2 fixé)……..57
Tableau III.9 : Le taux de reconnaissance de doigt index droit avec les différentes valeurs de Dog (2 fixé)……...57
Tableau III.10 : Le taux de reconnaissance de doigt annulaire gauche avec les différentes valeurs de Dog (2 fixé)……58
Tableau III.11 : Le taux de reconnaissance de doigt majeur gauche avec les différentes valeurs de Dog (2 fixé)……58
Tableau III.12 : Le taux de reconnaissance de doigt index gauche avec les différentes valeurs de Dog (2 fixé)……59
Tableau III.13 : Le taux de reconnaissance de doigt annulaire droit avec les différentes valeurs de Dog (1.6 fixé)……...59
Tableau III.14 : Le taux de reconnaissance de doigt majeur droit avec les différentes valeurs de Dog (1.6 fixé)……60
Tableau III.15 : Le taux de reconnaissance de doigt index droit avec les différentes valeurs de Dog (1.6 fixé)……60
Tableau III.16 : Le taux de reconnaissance de doigt annulaire gauche avec les différentes valeurs de Dog (1.6 fixé)……...60
Tableau III.17 : Le taux de reconnaissance de doigt majeur gauche avec les différentes valeurs de Dog (1.6 fixé)……...61
Tableau III.18 : Le taux de reconnaissance de doigt index gauche avec les différentes valeurs de Dog (1.6 fixé)……...61

Liste des Abréviations

FV: Finger veine.
ADN: Acide Désoxyribonucléique.
RAM: Random Access Memory.
DSP: Digital signal processor.
PIN: Personal Identification Number.
FRR: False Rejection Rate.
FAR: False Acceptante Rate
ERR: Equal Error Rate.
ROC: Receiver Operating Characteristic.
LPQ: Local phase Quantization
SVM: Support Vector Machine
KNN: K-Nearest Neighbors (K plus Proches Voisines).
LED: Light-Emitting Diode
CCD: Charged Coupled Device
ROI: Région of Interrest
LIF: Left Index Fingers
LMF: Left Middle Fingers
RIF: Right Index Fingers
RMF: Right Middle Fingers

SOMMAIRE

REMERCIEMENT
DEDICACES
RESUME
LISTE DE FIGURE
LISTE DES TABLEAUX
LISTE DES ABREVIATIONS
INTRODUCTION GENERALE

CHAPITRE I : INTRODUCTION A LA BIOMETRIE ET MULTI MODALITE

Introduction ……14
I.1.Définition de la biométrie ……..15
I.2. Principaux modalités biométriques …….....16
I.2.1.Les modalités physiologiques …….....17
I.2.2.Les modalités comportementales ……..22
I.3.Modes de fonctionnement d'un système biométrique …….....24
I.3.1.Le mode enrôlement …….....24
I.3.2.Mode vérification (authentification) ……..…….....25
I.3.3.Mode identification ……..……25
I.4.Principaux modules du système biométrique ……..…….....26
I.4.1.Module de capture (d'acquisition biométrique) ……...26
I.4.2.Module d'extraction des caractéristiques ……26
I.4.3.Module de correspondance ……..……..26
I.4.4.Module de décision ……..……26
I.5.Évaluation des performances des Systèmes biométriques …….....27
I.5.1.Le FAR (False Accepte en ce Rate) …….....27
I.5.2.Le FRR (False Reject Rate) ……...27
I.5.3.EER (Error Equal Rate) ……28
I.6.Les applications de la biométrie …….....30
I.7.La multi modalité …….....30
I.7.1.Système Biométrique multimodale ……...30
I.7.2.Les différentes multi modalité possible ……31
I.7.2.1. Systèmes multi algorithmes ……...31
I.7.2.2. Systèmes multi capteurs …….....31
I.7.2.3. Systèmes multi instances ……...32
I.7.2.4. Systèmes multi échantillons ……..32
I.7.2.5. Systèmes multi biométries ……32
Conclusion …….....33

CHAPITRE II : L'ETAT DE L'ART FINGER VEIN

Introduction ……35
II.1. Système d'identification ……35
II.2. Les caractéristiques de la reconnaissance des veines des doigts ……..35
II.3. La reconnaissance des veines des doigts (finger Vein) …….....36
II.4.Les méthodes de prétraitement ……..38
II.4.1.Filtre Dog (Difference of Gaussians) ……...38
II.4.2.Filtre laplacien ……..40

II.4.3.Technique de normalisation Tan et Triggs ……..40
II.4.4. Extraction de caractéristiques ……40
II.4.4.1. Méthode binaire locale (LBP) ……..41
II.4.4.2. Quantification de la phase locale (LPQ) ……..42
II.4.4.3. Inception v3 …….....44
II.4.5. La classification ……..45
II.4.5.1. Machine à Vecteurs de support (SVM) …….....45
II.4.5.2. Définition de K voisin plus proche (K-NN) …….....45
II.4.5.3. Random Forest …….....47
Conclusion …….....47

CHAPITRE III : APPLICATION ET RESULTATS

Introduction ……..49
III.1. Que signifie MATLAB (Matrix Laboratory) ……..49
III.2. Organigramme d'identification biométrique ……..49
III.2.1. Technique de normalisation Tan et Triggs …….....51
III.2.2. Gamma correction ……51
III.2.3.Différence of Gaussians (DOG) ……51
III.3. Expérience sur les images finger Vein …….....52
III.3.1 base de donnes …….....52
III.3.2. Séparation de la base de données ……...53
III.4. Résultats Expérimentales …….....53
Conclusion …….....62

CONCLUSION GENERALE ……64
BIBLIOGRAPHIE ……..66

INTRODUCTION GENERALE

INTRODUCTION GENERALE

Compte tenu de l'insécurité actuelle dans notre société, l'être humain a développé des moyens pour renforcer la protection afin de préserver sa sécurité, et a créé des moyens pour vérifier l'identité liée à ce qu'une personne possède, comme un passeport ou une carte d'identité, pour sécuriser la propriété. Cependant, ces éléments peuvent être manipulés ou oubliés. Afin de surmonter ces contraintes, nous avons lancé une nouvelle méthode pour mettre fin et réduire ce problème appelé biométrie, où il permet de vérifier que l'utilisateur est bien la personne qui prétend être celle. La reconnaissance biométrique est utilisée dans de nombreuses applications telles que la protection de l'accès à un ordinateur, un téléphone portable, une entreprise, des cartes bancaires, etc. De nombreuses techniques biométriques ont été développées, toutes basées sur des déterminants biométriques, physiologiques et comportementaux tels que dégoûtant, son, empreintes digitales, visage, Finger Vein, FKP... Etc.

C'est plus fiable que les systèmes conventionnels (clés, mot de passe...) parce que c'est difficile à falsifier.

Le système qui vient d'être étudié est le système d'identification des personnes à travers leurs images de veine des doigts.

L'objectif de cette étude est de développer le système biométrique idéal pour la reconnaissance des doigts, et dans cette étude, nous essaierons d'atteindre cet objectif à travers trois chapitres, et de nombreux concepts et concepts de la biométrie et de la reconnaissance du système de reconnaissance seront abordés.

CHAPITRE I

INTRODUCTION A LA BIOMETRIE ET MULTIMODALITE

Introduction :

La sécurité des technologies de l'information est un ensemble de moyens techniques, organisationnels, juridiques et humains pour mettre au point des moyens de prévenir l'utilisation non autorisée, l'utilisation abusive, la modification ou le détournement d'un système d'information. Une tâche prioritaire consiste à concevoir un système d'identification fiable, efficace et robuste. L'identification d'une personne est également nécessaire pour assurer la sécurité des systèmes et des institutions et contrôler l'accès à une zone hautement sécurisée accessible uniquement à un nombre limité de personnes. Ceci est cohérent avec la recherche de l'identité de la personne dans la base de données et de la personne avec la fonctionnalité compatible. Il existe de nombreuses technologies d'identification, dont certaines sont largement utilisées depuis des années. La méthode la plus courante d'authentification ou de vérification de l'identité d'une personne est la biométrie. Dans le premier chapitre, nous présenterons le système biométrique et ses différentes méthodes, et nous parlerons du système biométrique multimédia en abordant certains des problèmes du système biométrique unifié.

Dans ce chapitre, on donne quelques notions et définitions de base liées à la biométrie. Nous introduirons aussi le principe de fonctionnent d'un système biométrique et ses performances ainsi que les différentes modalités utilisées et systèmes multimodales.

I.1.Définition de la biométrie :

L'expression « biométrie » est originaire d'une contraction des deux anciens termes grecs : « bios » qui signifie : la vie et « metron» qui se traduit par: mesure. **[1]**

La biométrie est La reconnaissance automatique d'une personne selon ses caractéristiques physiologiques, biologiques ou comportementales.

La biométrie comprend l'ensemble des processus penchant à déterminer une personne à partir de la mesure de l'une ou de plusieurs de ses caractéristiques physiologiques, comportementales ou biologique. La biométrie est la science d'établir l'identité d'une personne basée sur :

Physiologiques Les attributs: comme empreintes digitales, visage, géométrie de la main, iris, rétine…etc. Comportementaux comme démarche, signature, dynamique de clavier…etc.

Les attributs biologiques : comme ADN, Odeur et cheveux…. etc. liés à un individu [2]. (Figure I.1)

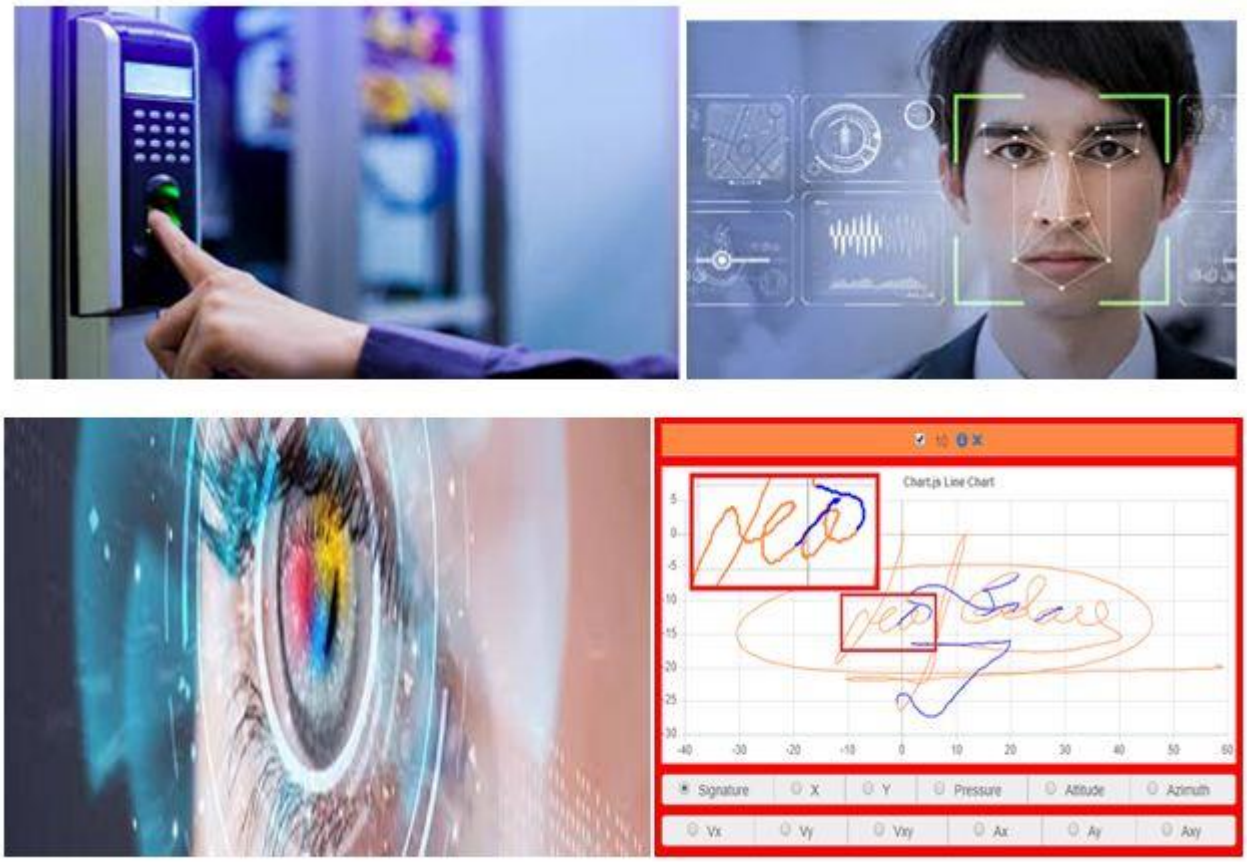


Figure I.1: Exemples de modalités biométriques.

I.2. Principaux modalités biométriques :

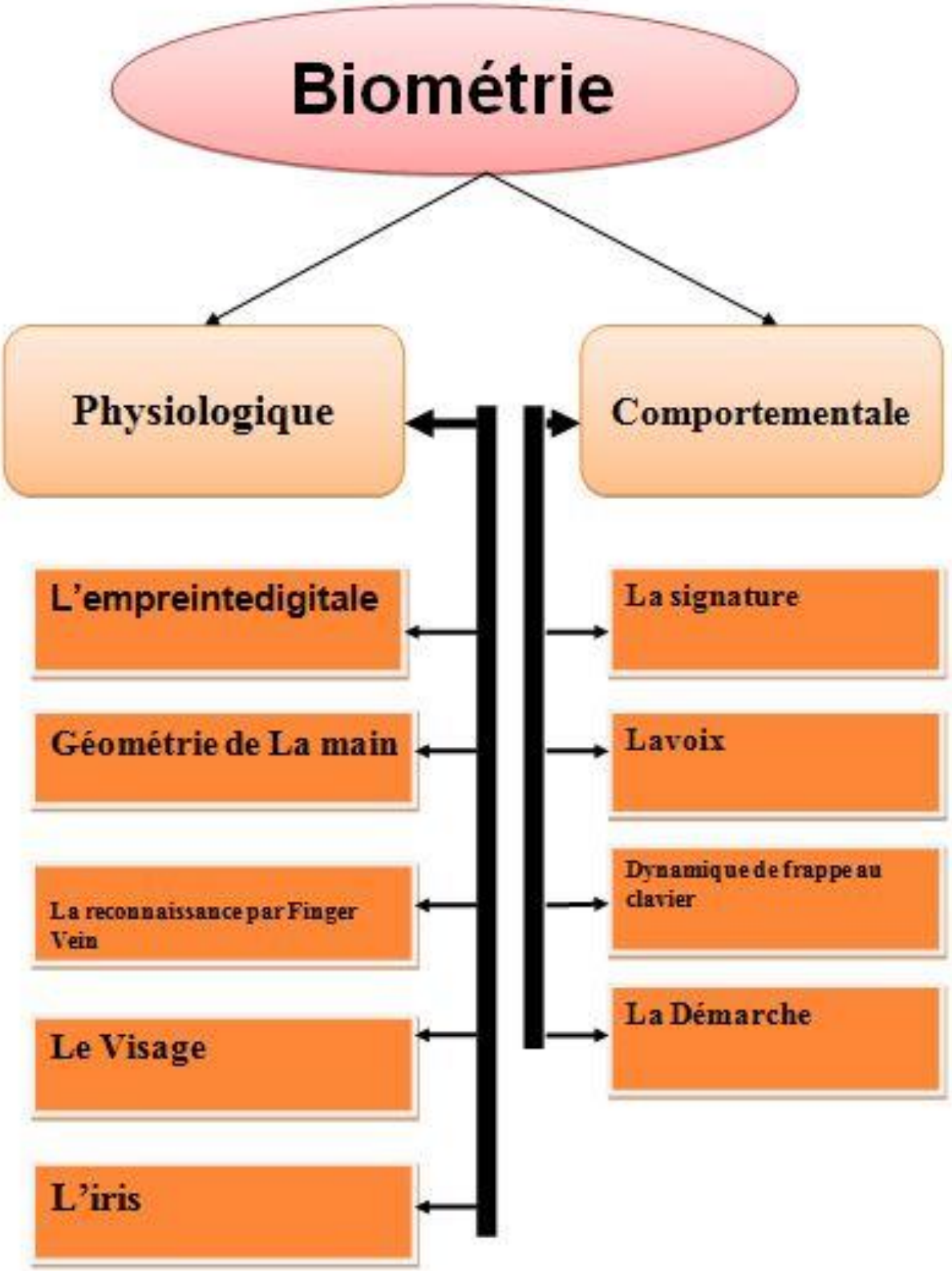


Figure I.2 : Principaux modalités biométrique

I.2.1.Les modalités physiologiques

Analyse physiologique (morphologique) :

Elle est basée sur l'identification de traits physiologique particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe l'iris de l'œil, la forme de la main, les empreintes digitales, les traits du visage, etc. **[3]**

1. Le Visage:

Les systèmes actuels de reconnaissance du visage sont composés d'un module d'acquisition d'images avec une caméra. Il procède d'abord à une détection du visage dans l'image acquise. Ensuite, qui va la traiter en utilisant des algorithmes afin d'extraire une signature du visage. Finalement, cette signature est comparée, à l'aide d'un classificateur, avec les signatures déjà existantes dans une base de données locale, afin d'identifier l'individu. Les caractéristiques jugées significatives pour la reconnaissance du visage sont : les yeux, la bouche et le tour du visage. [4]

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. Elle nécessite un arrière-plan simple et fixe pour que le résultat soit précis [11]. (Figure I.3)

Figure I.3: Reconnaissance par visage.

2. L'empreinte digitale:

Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers (minutes) et constituent un motif unique, universel et permanent. Pour obtenir une image de l'empreinte d'un doigt, on utilise des capteurs. Les avancées technologiques ont permis d'automatiser la tâche au moyen de capteurs intégrés, remplaçant ainsi l'utilisation classique de l'encre et du papier. Les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Ces éléments sont appelés minuties **[5]**. (**Figure I.4)** Ce type de système est utilisé par les institutions financières pour leurs employés et leurs clients. Il se retrouve également dans les hôpitaux, les écoles, les aéroports, les cartes d'identité, les passeports, les permis de conduire et de nombreuses autres applications **[6]**.

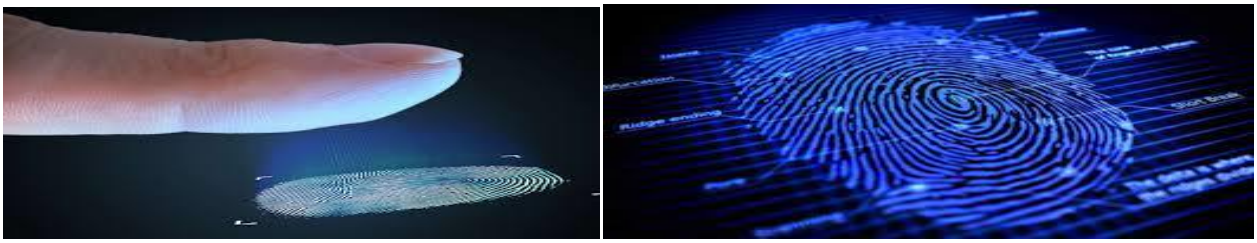


Figure I.4: Images de L'empreinte digitale.

3. Géométrie de La main :

Cette modalité consiste à analyser, la forme de la main sa longueur, sa largeur, son hauteur, la courbure des doigts…etc. Cette technique est récente, simple, et bien acceptée par les utilisateurs qui suivent des guides des capteurs (LEDs infrarouge, des appareils photos numériques) pour qu'ils bien positionner leurs doigts, ce qui rende ainsi la détection / la segmentation plus aisée, cependant ce genre de système peut être trompé par de vrais jumeau ou même par des personnes ayant des formes de la main proches. Cette technologie offre un niveau raisonnable de précision est relativement facile à utiliser. Cependant elle peut être facilement trompée par des jumeaux ou par des personnes ayant des formes de la main proches. **[7]**

(**Figure I.5)**.

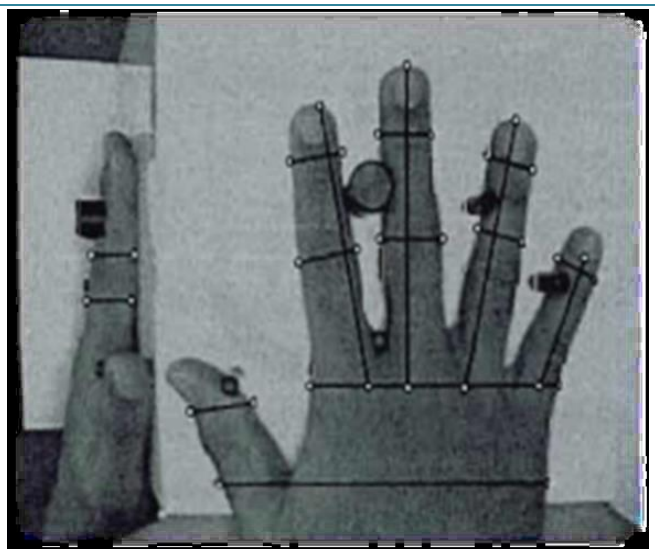


Figure I.5 : Géométrie de la main.

4. La reconnaissance par Finger Vein:

La reconnaissance des veines des doigts est une méthode qui spécifie un individu en utilisant le motif veineux à l'intérieur de ses doigts.

Les caractéristiques de la reconnaissance des veines des doigts sont les suivantes:

Les modèles de veine des doigts sont uniques à chaque individu, même parmi les jumeaux identiques. Le taux de fausse acceptation est très faible (proche de zéro).

Placer une main ou un doigt est moins intrusif que les autres technologies biométriques. (Figure I.6.)

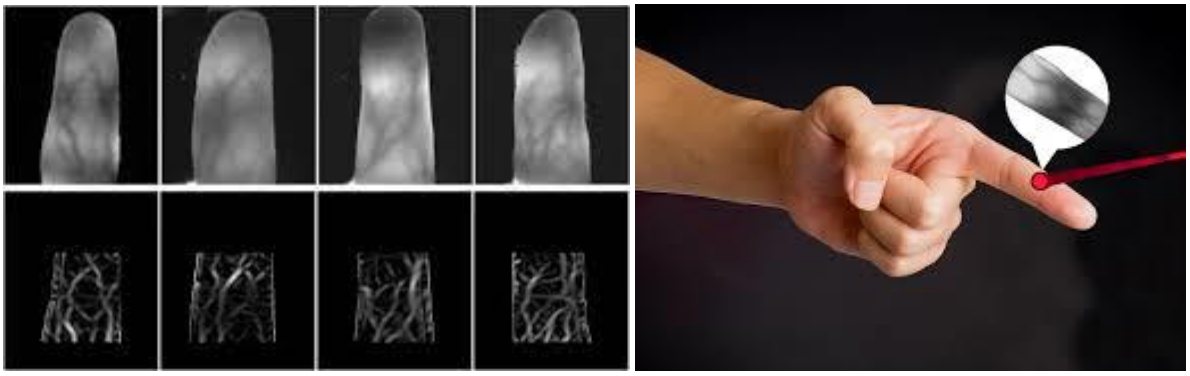


Figure I.6: Quelques images des empreintes des finger Vein

Les avantages :

✓ IL n'existe aucun moyen de frauder, car on ne peut pas "photographier" les veines de la main. Parce que Le réseau vasculaire est propre à chaque individu (même les vrais jumeaux en ont un différend).

✓ Il n'y a aucun contact lors de l'authentification comme avec les empreintes digitales, donc pas de problème d'hygiène.

✓ Le TFA - taux de fausses acceptations est de moins de 0,00008% Selon Fujitsu, qui a comparé 140 000 paumes de main.

Les inconvénients :

✓ Le scanner est relativement encombrant comparer aux capteurs d'empreintes digitales.

✓ Très coûteuse.

La méthode de la veine numérique peut être utilisée par les systèmes biométriques en raison de certains avantages. Tout d'abord, l'acquisition de données est facile et relativement économique avec les caméras commerciales basse résolution. Deuxièmement, les systèmes d'accès basés sur les veines des doigts sont très appropriés pour une utilisation intérieure et extérieure, et peuvent bien fonctionner dans des conditions météorologiques extrêmes et de mauvaises conditions d'éclairage. Troisièmement, les caractéristiques de la veine du doigt chez l'adulte sont plus stables dans le temps et ne subissent pas de changements majeurs. Enfin, la bio-informatique digitale basée sur les veines digitales est utilisée avec succès pour identifier des personnes parmi plusieurs personnes **[29]**.

5. L'iris:

Elle est considérée comme la modalité la plus précise pour l'identification et l'authentification. Son seul inconvénient est son coût assez élevé, ce qui la rend pas autant répondu pour des applications quotidiennes. Alors, son utilisation s'est limitée dans des endroits où la sécurité est primordiale et même critique. 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. Une personne voulant s'identifier place son œil à quelques centimètres du capteur et l'image de l'iris

est prise par une caméra. En suite, les caractéristiques sont extraites de l'image de l'iris et comparées à celles enregistrées dans la base de données.est unique. L'iris a une structure extra ordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. **[7]**

L'acquisition de l'iris est effectuée au moyen d'une caméra pour pallier aux mouvements inévitables de la pupille. Elle est très sensible (précision, reflet…) et relativement dés agréable pour l'utilisateur car l'œil doit rester grand ouvert et il est éclairé par une source lumineuse pour assurer un contraste correct. **[9][10] (Figure I.7)**

Figure I.7: Image de L'iris.

6. La rétine:

Elle se base sur le schéma et le dessin formés par les vaisseaux sanguins de la

Rétine qui sont uniques pour chaque personne et assez stables tout au long de la vie. Elle est très peu utilisée et mal acceptée par le public et les utilisateurs car il doit placer son œil près de la caméra (quelques centimètres). Elle est utilisée essentiellement dans des environnements de haute sécurité comme l'accès aux sites nucléaires militaires.

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. Aussi, cette technologie, très précise **[12]. (Figure I.8)**

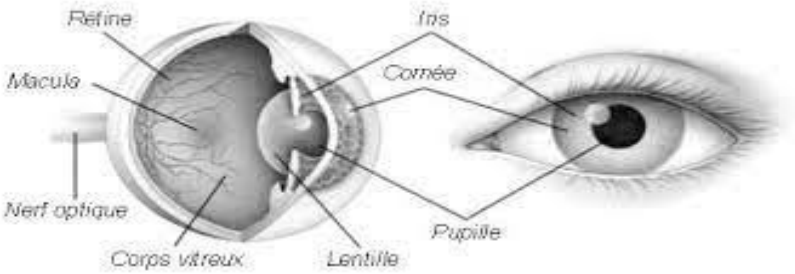


Figure I.8 : Image de la rétine.

I.2.2.Les modalités comportementales :

1. La signature:

La vérification de la signature analyse la façon dont un utilisateur signe son

Nom. Les caractéristiques dynamiques de la signature comme la vitesse et la pression sont aussi importantes que la forme géométrique de la signature.

Cette technique est considérée parmi les premières utilisées dans le domaine de la biométrie. Elle se base généralement sur le fait que l'utilisateur signe avec un stylo électronique sur une palette graphique et au même temps elle examine l'ensemble de dynamique comme la vitesse, la direction, et la pression de l'écriture, le temps pendant lequel le stylo est en contact avec le papier, le temps pris pour faire la signature et les positions où le stylo est relevé et abaissé sur le papier [13].

Ces données sont enregistrées pour comparaison ultérieure. Certains systèmes ne font qu'enregistrer limage statique de la signature pour comparaison [14]. (Figure I.9)

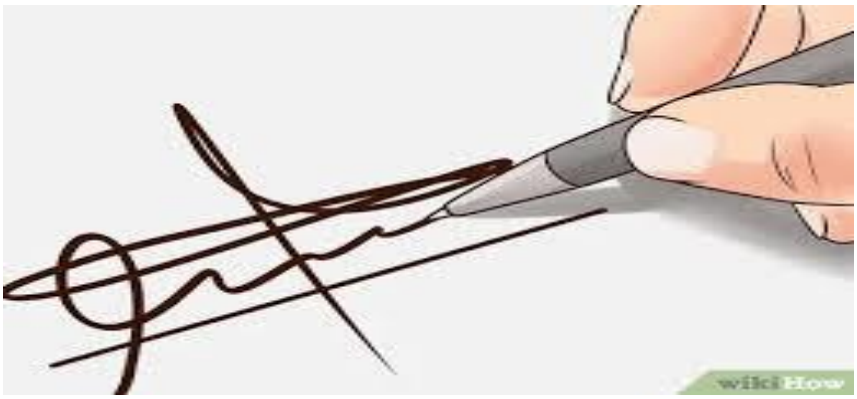


Figure I.9: Image de signature

2. La voix:

La biométrie de la voix traite des données qui proviennent à la fois de facteurs physiologiques dépendants de l'âge, du sexe, de la tonalité, de l'accent et de facteurs comportementaux comme la vitesse et le rythme. Ils ne sont en général pas imitables. C'est la seule technique qui permette à l'heure actuelle de reconnaître une personne à distance et qui est en général bien accepté par les usagers. Cependant cette technique est très facilement falsifiable et nécessite en plus une excellente qualité d'enregistrement. En outre peu de différences existent entre deux voix ce qui rend cette technique peu fiable. Cette technique est très facilement falsifiable et nécessite en plus une excellente qualité d'enregistrement**. [4]**

Figure I.10: Image de la voix.

3. Dynamique de frappe au clavier:

Le système est basé sur la dynamique de frappe au clavier, il ne nécessite aucun équipement particulier, chaque ordinateur disposant d'un clavier. Il s'agit d'un dispositif logiciel qui calcule le temps ou un doigt effectue une pression sur une touche et le temps où un doigt est dans les airs (entre les frappes).Cette mesure est capturée environ 1000 fois par seconde. La séquence de frappe est prédéterminée sous la forme d'un mot de passe. Initialement l'utilisateur doit composer son mot de passe à quelques reprises afin que soit constitué un gabarit de référence.

Ce dispositif biométrique est utilisé comme méthode de vérification pour le commerce électronique et comme mécanisme de contrôle d'accès à des bases de données [15].**(Figure I.11)**

Figure I.11: Image d'un clavier.

4. La Démarche:

Il s'agit de reconnaître un individu par sa façon de marcher et de bouger. En analysant les déformations des jambes et bras au niveau des articulations. La démarche serait en effet étroitement associée à la musculature naturelle donc elle est très personnelle [16], l'intérêt de cette technologie réside que l'identification de démarche se situe dans la capacité d'identifier un individu à distance [5]**. (Figure I.12)**

Figure I.12: La Démarche.

I.3.Modes de fonctionnement d'un système biométrique:

Les systèmes biométriques peuvent fournir trois modes de fonctionnement à savoir mode d'enrôlement**,** mode vérification ou bien en mode d'identification.

I.3.1.Le mode enrôlement:

Il est considéré comme la première étape du système biométrique (voir Figure I.13), car il représente la première étape téléchargée, au cours de laquelle un ou plusieurs utilisateurs sont enregistrés pour collecter des informations biométriques sur les personnes à identifier. Les propriétés biométriques sont collectées par le capteur biométrique, puis représentées sous forme numérique, stockées et enfin enregistrées dans la base de données **[17]**.

Comme illustré dans la **Figure I.13**.

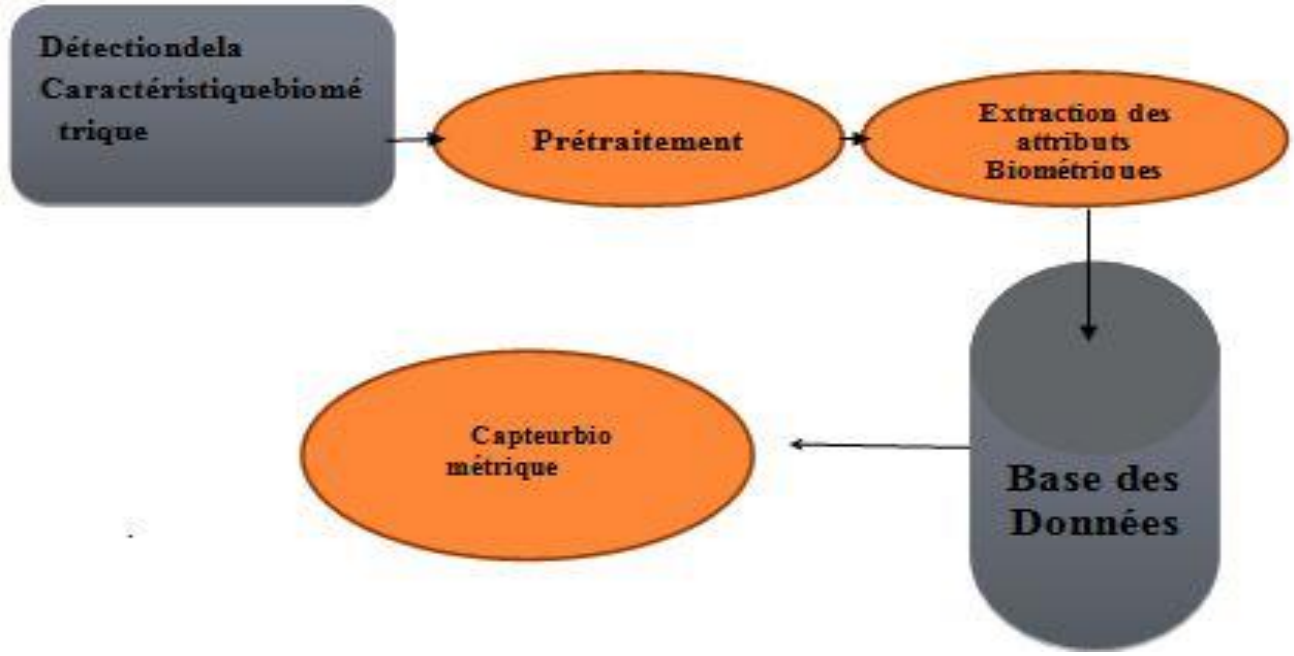


Figure I.13: Mode enrôlement d'un système biométrique.

I.3.2.Mode vérification (authentification) :

A ce stade, l'utilisateur confirme son identité (voir Figure I.14) Le système vérifie l'identité de l'utilisateur en comparant les données dynamiques acquises avec celles stockées dans la base de données. Dans un tel système, la personne revendique une identité, généralement via PIN, nom d'utilisateur, carte à puce,

Etc..., puis le système effectue une comparaison sur le couplage (1: 1) afin de déterminer Si les données sont valides ou non. **[6]. (Figure I.14)**.

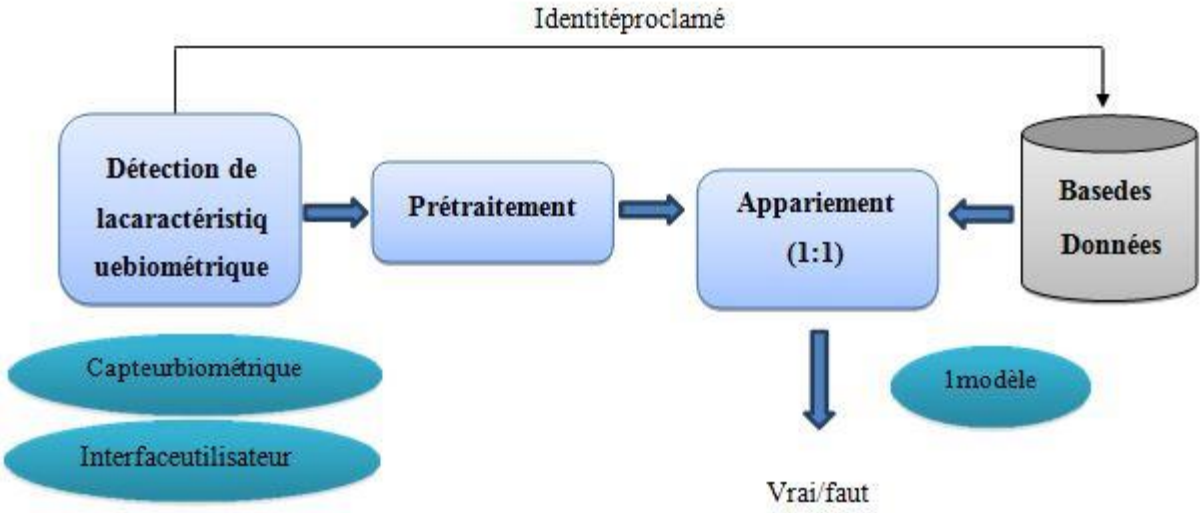


Figure I.14: Mode vérification d'un système biométrique.

I.3.3.Mode identification :

À ce stade, l'utilisateur ne révèle pas son identité. Cependant, la seule affirmation implicite faite par l'utilisateur est qu'il s'agit d'une personne déjà inscrite sur le système. Ainsi, l'échantillon biométrique de l'individu est comparé aux échantillons de toutes les personnes enregistrées dans la base de données. C'est ce qu'on appelle la publication Correspondance 1: **1 : N**, où Le système biométrique consiste en l'identité d'une personne portant un modèle de Diplôme Similitude significative avec l'échantillon biométrique fourni en entrée.

Habituellement, si c'est La plus grande similitude entre l'échantillon et tous les modèles est en dessous du seuil de sécurité c'est-à-dire le groupe minimum, la personne est **rejetée**, ce qui signifie que l'utilisateur n'était pas à l'intérieur Personnes précédemment enregistrées dans le système.

Dans le cas contraire. La personne est **acceptée** Un exemple de système opérant en mode identification serait l'accès à un bâtiment sécurisé : tous les utilisateurs qui sont autorisés à entrer

dans le bâtiment sont enrôlés par le système; lorsqu'un individu essaye de pénétrer dans le bâtiment, il doit d'abord présenter ses données biométriques au système et, selon la détermination de l'identité de l'utilisateur, le système lui accorde le droit d'entrée ou non. En résumé, un système biométrique opérant en mode identification répond à la question "Suis-je bien connu du système ?".**[18]**

I.4.Principaux modules du système biométrique :

Un système biométrique est essentiellement un système de reconnaissance de personnes.

Il peut être représenté par quatre modules principaux chacun de ces modules sont définis dans ce qui suit :

I.4.1.Module de capture (d'acquisition biométrique):

Il est responsable de l'obtention des données biométriques: certaines caractéristiques physiologiques, comportementales ou biologiques d'un individu à l'aide d'un scanner, au moyen d'un capteur biométrique approprié (appareil photo, appareils photo numériques pour lecteur d'empreintes digitales, caméra de sécurité, etc.). **[19]**

I.4.2.Module d'extraction des caractéristiques:

Les données biométriques acquises sont traitées d'une façon qui permet d'obtenir un modèle numérique de la personne ''signature biométrique'', qui sera conservé sur un support portable (puce ou autre) ou généralement dans une base de données **[20]**.

I.4.3.Module de correspondance:

Il 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 **[20]**.

I.4.4.Module de décision:

Il 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 les modèles stockés **[20]**.

I.5.Évaluation des performances des Systèmes biométriques :

Chaque modalité biométrique a des points de force et de faiblesse, aucun système biométrique n'est « parfait ». Faire correspondre un système biométrique spécifique à une application dépend du mode opérationnel de l'application et des caractéristiques biométriques choisies **[17]**.

Mesure des performances :

Un utilisateur final doit faire une demande identifier/vérifier de son identité, alors le système biométrique doit déterminer si l'identité par l'utilisateur est acceptée ou rejetée. Deux taux sont alors calculés :

I.5.1.Le FAR (False Accepte en ce Rate):

Ce taux est le pourcentage de personnes qui ne devraient pas être reconnues. Mais ils sont accepté par le système Autrement dit, les fraudeurs acceptés par le système, qui sont caractérisés par deux caractéristiques de deux personnes différentes et sont classés comme appartenant à la même personne **19]**.

$$\boldsymbol{FAR} = \frac{\boldsymbol{nombre\ des\ imposteurs\ acceptées}}{\boldsymbol{nombre\ totale\ d'accés\ imposteurs}}$$

I.5.2.Le FRR (False Reject Rate) :

Le deuxième critère est appelé le taux de faux rejet (FRR). Ce taux Représente le pourcentage de personnes que le système devrait reconnaître mais ont rejeté

$$\boldsymbol{FRR} = \frac{\boldsymbol{nombre\ des\ imposturs\ rejetés}}{\boldsymbol{nombre\ totale\ d'accés\ imposteurs}}$$

Une diminution du FAR entraîne systématiquement une augmentation du FRR (et inversement) **[19]**. La performance du système ne peut pas être mesurée en utilisant séparément les taux d'erreur (FAR/FRR) mais on utilise le taux d'erreur égale (EER).

I.5.3.EER (Error Equal Rate):

Le troisième critère est connu sous le nom de taux d'égale erreur ("Equal Error Rate" Ou EER). Ce taux est calculé à partir des deux premiers critères et constitue un point de Mesure de performance courant. Ce point correspond à l'endroit où FRR = FAR, c'est-adire le meilleur compromis entre les faux rejets et les fausses acceptations **[21]**.

La figure 1.15 illustre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs tandis quel' EER est représenté sur la (**Figure I.15**)

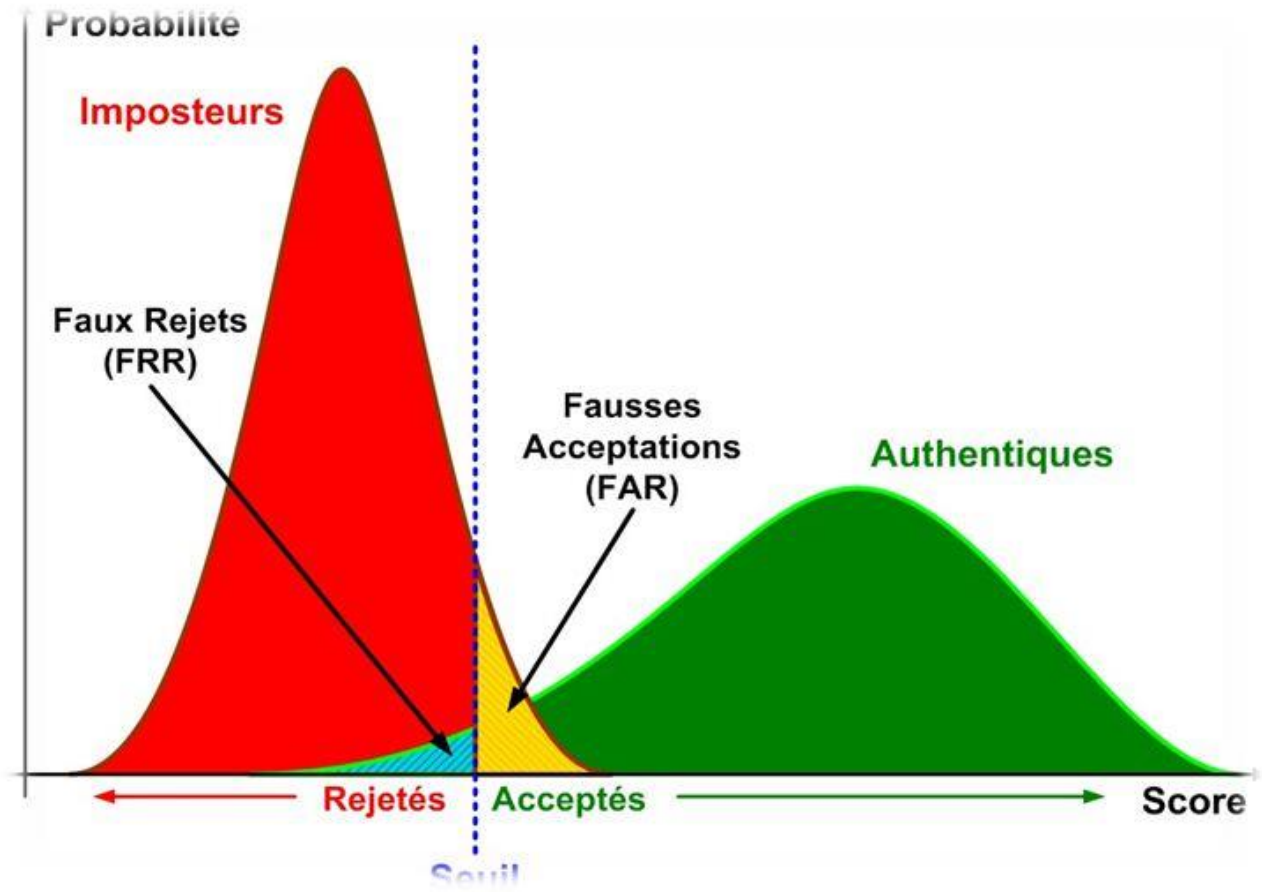


Figure I.15: Illustration du FRR et du FAR.

Le choix du seuil de similarité est important cari influe directement sur les performances du système. Un seuil trop petit entraîne l'apparition d'un grand nombre de faux rejets, tandis qu'un seuil trop grand engendre un taux important de fausses acceptations.

La statistique la plus simple pour mesurer la performance d'un algorithme dans le contexte de la Vérification est de calculer le point d'équivalence des erreurs (Equal Error Rate - EER). Le point

d'équivalence des erreurs, ou taux d'exactitude croisée, est déterminé par le point d'inter section entre la courbe du taux de fausses acceptations et la courbe du taux de faux rejets. Un exemple de courbes d'erreurs croisées est donné à la figure (**I** .16). **[17]**

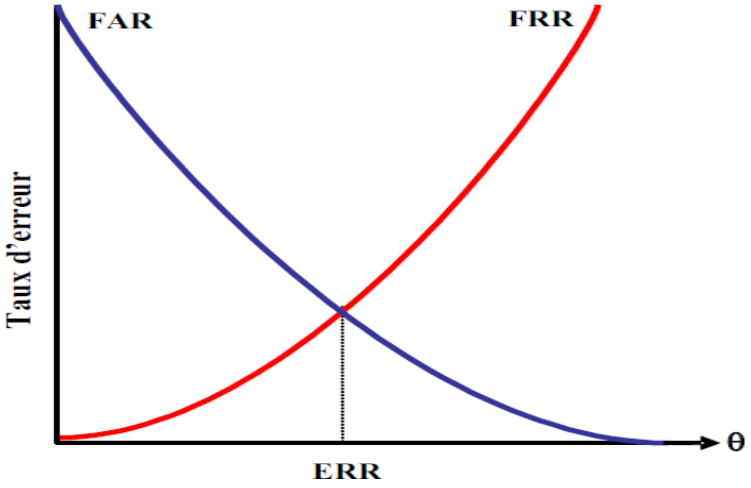


Figure I.16 : Courbe du point d'équivalence des erreurs dans un système biométrique. **[22]**

L'évaluation passe également par le tracé de statistiques complexes, comme la courbe « Detection Error Trade-off (DET) ». Cette courbe donne le FRR en fonction du FAR. Elle est tracée de manière paramétrique en fonction des valeurs du seuil. **[23]**

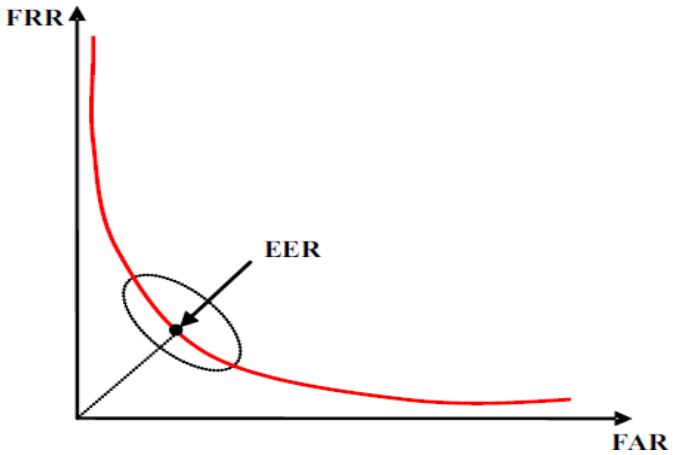


Figure I.17 : Courbe DET.

I.6.Les applications de la biométrie :

De nos jours, les systèmes biométriques sont de plus en plus utilisés dans des applications civiles, les applications de la biométrie peuvent être divisées en trois groupes principaux :

Applications commerciales:

Telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, la gestion des registres médicaux, l'étude à distance, l'accès d'internet, l'ATM, la carte de crédit, le contrôle d'accès physique, le téléphone portable, le PDA, la gestion des registres médicales, …etc.

Applications gouvernementales:

Telles quel a carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc.

Applications légales :

Telles que les enfants disparus, l'identification de corps, la recherche criminelle, l'identification de terroriste, etc. **[17]**

I.7.La multi modalité :

La multi modalité est la combinaison de plusieurs modalités biométriques différentes ce qui implique l'utilisation d'information complémentaires. En augmentant la quantité d'information discriminante de chaque personne, on souhaite augmenter le pouvoir de reconnaissance.

I.7.1.Système Biométrique multimodale:

La biométrie multimodale consiste à combiner plusieurs techniques biométriques au sein d'un même système.

L'utilisation de plusieurs systèmes a pour but premier d'améliorer les performances de reconnaissance. En augmentant la quantité d'informations discriminante de chaque personne, on souhaite augmenter le pouvoir de reconnaissance du système. De plus, le fait d'utiliser plusieurs modalités biométriques réduit le risque d'impossibilité d'enregistrement ainsi que les robustes seaux fraudes. **[24]**

I.7.2.Les différentes multi modalité possible:

Les systèmes biométriques multimodaux diminuent les contraintes des systèmes biométriques monomodaux en combinant plusieurs systèmes. On peut différencier 5 types des systèmes multimodaux selon les systèmes qu'ils combinent. **(Figure I.18)[25]**

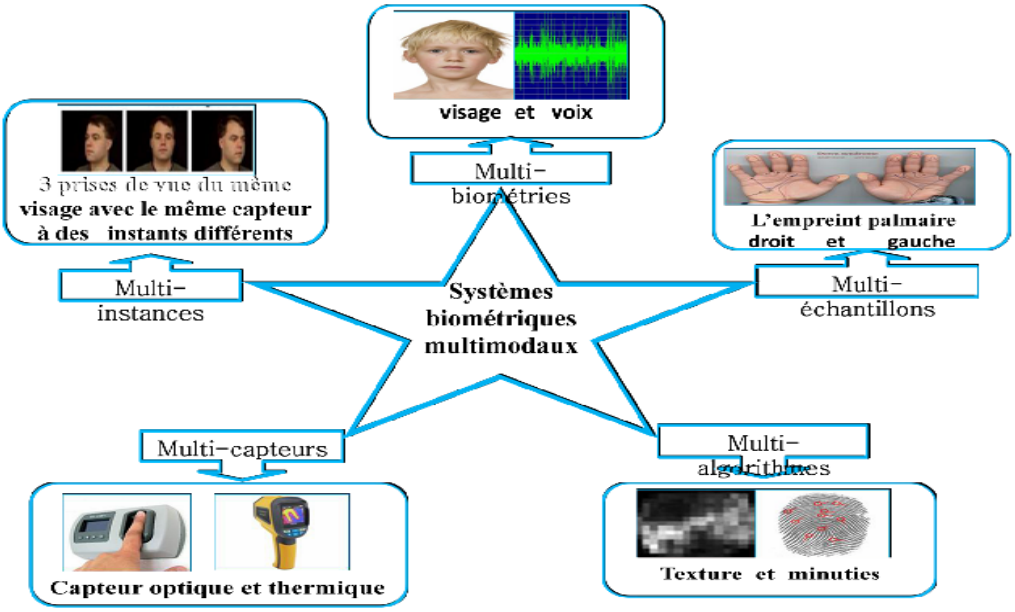


Figure I.18: Les différents systèmes multimodaux.

I.7.2.1. Systèmes multi algorithmes :

C'est le type de système le plus classique implicitement utilisé par de nombreuse s'approches. Les caractéristiques sont obtenues par différents algorithmes puis fusionnées. Par exemple, la fusion des caractéristiques extraites via un algorithme analysant les textures et un autre la forme d'un caractère biométrique entre dans ce cadre. **[26]**

I.7.2.2. Systèmes multi capteurs:

Plusieurs capteurs permettent de capturer le même caractère biométrique. Comme le capture d'un visage à l'aide d'une caméra classique et d'une caméra infrarouge entre dans ce scénario. Ce type de système permet la fusion au niveau capteur. **[27]**

I.7.2.3. Systèmes multi instances:

Ce type de système permet de capturer plusieurs instances du même caractère biométrique. L'acquisition de plusieurs images de même visage via le même capteur est l'exemple typique de ce type de système.

Ces systèmes n'entraînent pas de surcoût de capteurs, ni le développement de nouveaux algorithmes. À ne pas confondre avec les systèmes multi-échantillons. **[26]**

I.7.2.4. Systèmes multi échantillons :

Plusieurs échantillons différents de la même modalité sont capturés, par exemple deux empreintes digitales de doigts différents ou les deux iris. Dans ce cas, les différentes données sont traitées par le même algorithme.

I.7.2.5. Systèmes multi biométries:

Lorsque l'on considère plusieurs biométries différentes, par exemple visage et empreinte digitale. Un système multi modal peut bien sûr combiner ces différents types d'associations, par exemple l'utilisation du visage et de l'empreinte mais en utilisant plusieurs doigts. **[25]**

Tous ces types de systèmes peuvent pallier à des problèmes différents et ont chacun leurs avantages et inconvénients. Les quatre premiers systèmes combinent des informations issues d'une seule et même modalité ce qui ne permet pas de traiter le problème de la non-universalité de certaines biométries ainsi que la résistance aux fraudes, contrairement aux systèmes "multi-biométries".

En effet, les systèmes combinant plusieurs informations issues de la même biométrie permettent d'améliorer les performances en reconnaissance en réduisant l'effet de la variabilité intra-classe. Mais ils ne permettent pas de traiter efficacement tous les problèmes des systèmes monomodaux. C'est pour cette raison que les systèmes multi-biométries ont reçu beaucoup d'attention de la part des chercheurs **[25].**

Conclusion :

Dans ce chapitre, nous avons introduit le concept des systèmes biométriques, leur architecture et leurs différentes applications. Nous avons aussi constaté que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre. Parmi les critères d'évaluation de la qualité du système biométrique, nous avons présenté les taux des erreurs (FAR, FRR et ERR), nous avons parlé aussi de la biométrie multi modale et ses différents types.

CHAPITRE II

L’ETAT DE L’ART FINGER VEIN

Introduction

Nous allons présenter dans ce chapitre l'identification des personnes par finger Vein, nous présentons les différentes étapes qui constituent un système d'identification compris le prétraitement, l'extraction de caractéristiques et la classification.

II.1. Système d'identification :

Le système d'identification se compose de quatre étapes :

- L'acquisition (base de données)
- Le prétraitement (exemple : filtre gaussien, laplacien,....)
- L'extraction des caractéristiques (exemple : LPQ, LPB,...)
- La classification (exemple : SVM, KNN,…)

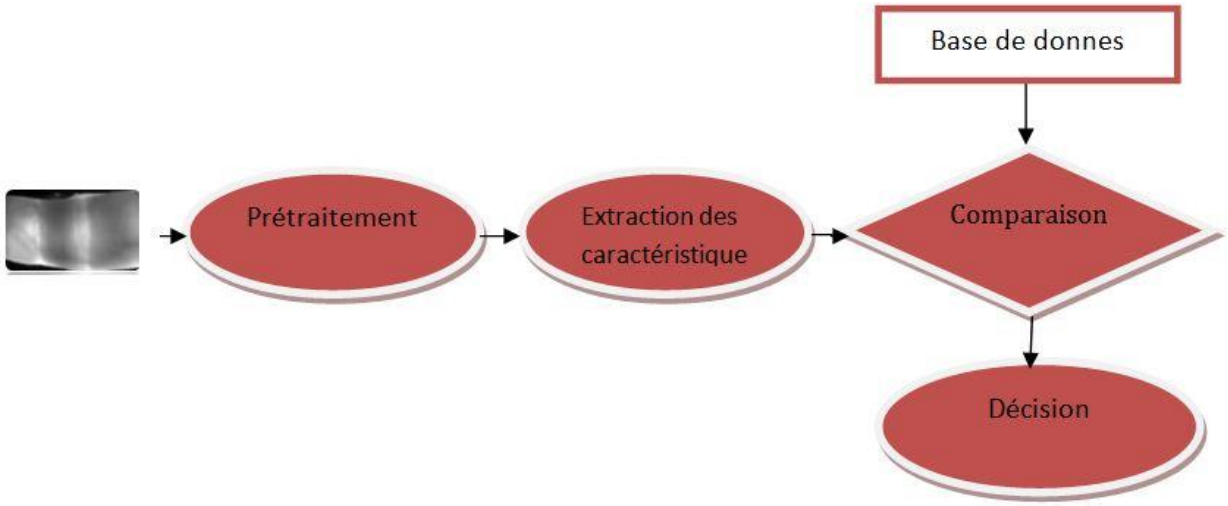


Figure II.1: Schéma synoptique de système d'identification biométrique

II.2. Les caractéristiques de la reconnaissance des veines des doigts :

- Les modèles de veine des doigts sont uniques à chaque individu, même parmi les jumeaux identiques. Le taux de fausse acceptation est très faible (proche de zéro).
- Placer une main ou un doigt est moins intrusif que d'autres technologies biométriques.
- Les veines sont situées à l'intérieur du corps, il est extrêmement difficile de voler et il y a peu de risques de contrefaçon.
- Les veines des doigts ne laissent aucune trace pendant le processus d'authentification et ne peuvent donc pas être dupliquées.

- Les schémas veineux des doigts restent relativement constants pendant les années adultes, de sorte que le ré enrôlement du schéma veineux ne sera pas nécessaire une fois inscrit.
- Les veines des doigts sont moins susceptibles d'être influencées par les changements du temps ou de la condition physique de l'individu.
- Les précipités, la peau craquelée et rugueuse n'affectent pas le résultat de l'authentification [**28**].

II.3. La reconnaissance des veines des doigts (finger Vein) :

La reconnaissance des veines des doigts est basée sur des images de modèles de veines des doigts humains sous la surface de la peau. La technologie est actuellement utilisée ou développée pour une grande variété d'applications, y compris l'authentification des cartes de crédit, la sécurité automobile, le suivi des heures et des présences des employés, l'authentification des ordinateurs et du réseau, la sécurité des terminaux et les guichets automatiques **[29].** Pour obtenir le motif de l'enregistrement de la base de données, un individu insère un doigt dans un terminal de testeur contenant une lumière à diode électroluminescente (LED) proche infrarouge et une caméra à dispositif à couplage de charge (CCD) monochrome. L'hémoglobine dans le sang absorbe la lumière **LED** proche infrarouge, ce qui fait apparaître le système veineux comme un motif de lignes sombres. L'appareil photo enregistre l'image et les données brutes sont numérisées, certifiées et envoyées à une base de données d'images enregistrées. À des fins d'authentification, le doigt est scanné comme auparavant et les données sont envoyées à la base de données des images enregistrées pour comparaison. Le processus d'authentification prend moins de deux secondes. Des dispositifs de lecture des doigts ont été déployés pour être utilisés dans les institutions financières japonaises, les kiosques et les tourniquets **[30]**. Mantra Softecha commercialisé un appareil en Inde qui scanne les veines des paumes pour l'enregistrement de la présence **[31]**. Fujitsu a développé une version qui ne nécessite pas de contact physique direct avec le scanner veineux pour une meilleure hygiène lors de l'utilisation d'appareils électroniques de point de vente **[32]**. Hitachi Ltd. (Tokyo, Japon) proposé un nouveau dispositif de capture des veines des doigts et des mains sans contact, avec modules

laser au lieu de LED NIR, une caméra industrielle spéciale NIR améliorée avec un Filtre traverser NIR pour obtenir la meilleure qualité d'image possible, un objectif et une distance optimaux entre le doigt/la main et l'appareil photo pour permettre des distorsions d'image minimales ainsi qu'un contrôle d'éclairage automatisé pour fournir un éclairage uniforme sur tout le doigt/la main surface et d'obtenir le meilleur contraste et la meilleure qualité d'image possible **[33]**.

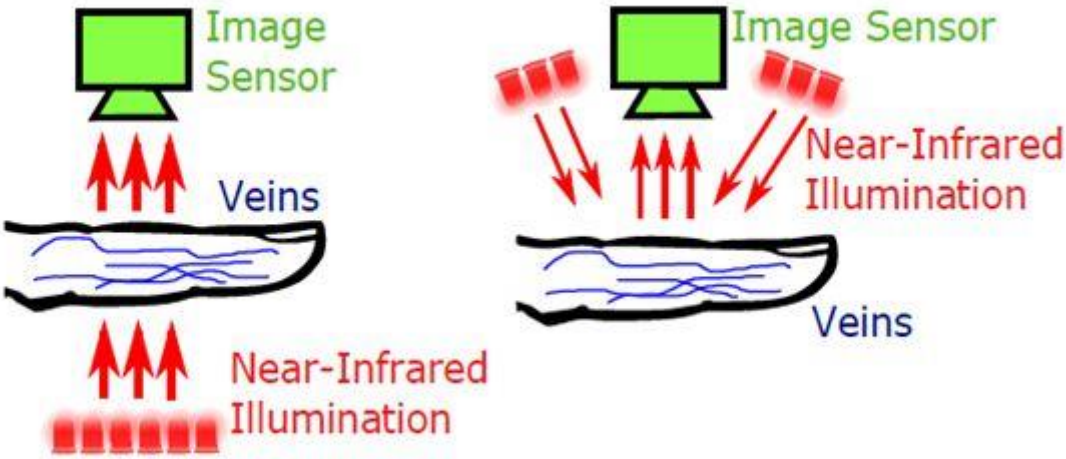


Figure II.2 : Positionnement de la source lumineuse et du capteur d'image, à gauche: transmission de la lumière, à droite : lumière réfléchie. **[**33**]**

Pour que des personnes soient reconnues par finger Vein, nous devons passer par deux étapes:

- Il est nécessaire d'avoir des images de référence, sous la forme d'une base de données de FV. A chaque image est associée un vecteur de caractéristiques, ces caractéristiques invariantes pour une même personne, sont différentes d'une personne à l'autre, donc deux personnes ne peuvent pas posséder exactement la même caractéristique.
- Comparer le vecteur de caractéristiques du FV à reconnaître avec celui de chacun des FV de la base de données. Ceci permet de retrouver la personne ayant le FV le plus ressemblant, qui est celui dont le vecteur est le plus similaire.

ROI Extraction :

Cette étape la plus importante est l'extraction de la région d'intérêt ROI (Région of Interest). Dans l'image de la veine du doigt FV, il y a des régions indésirables (arrière-plan de l'image) et la zone de valeur (zone du doigt) dans l'image. La zone de valeur s'appelle ROI, et l'extraction de ROI est le traitement permettant de localiser et d'extraire la zone de doigt de l'image capturée et de supprimer le fond de l'image **[34]**.

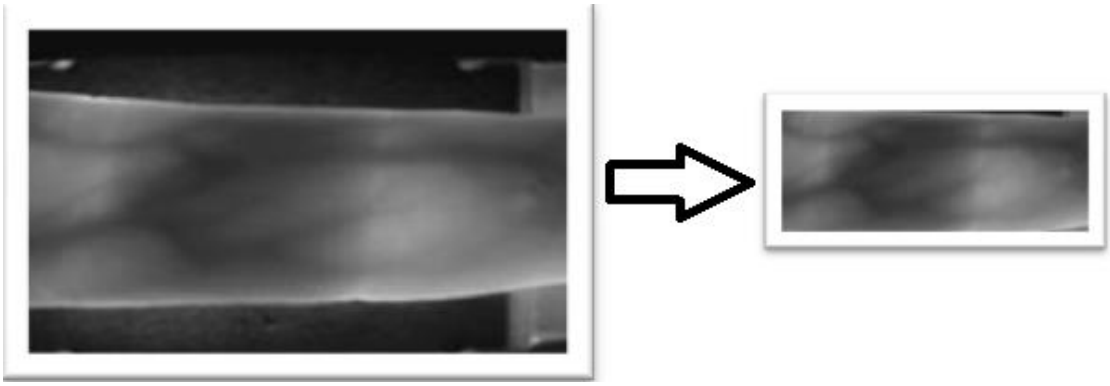


Figure II.3: ROI d'extraction.

II.4 .Les méthodes de prétraitement

II.4 .1.Filtre Dog (Difference of Gaussians):

En science de l'imagerie, la différence des gaussiens (DOG) est un algorithme d'amélioration des fonctionnalités qui implique la soustraction d'une version floue d'une image originale d'une autre version moins floue de l'original. Et c'est un filtre passe-bande qui rejette presque toutes les fréquences spatiales présentes dans l'image d'origine en niveaux de gris. Les images floues sont obtenues en convolant les images en niveaux de gris d'origine avec des noyaux gaussiens ayant des écarts types différents. Le flou d'une image à l'aide d'un noyau gaussien supprime uniquement l'espace à haute fréquence information. La soustraction d'une image de l'autre préserve les informations spatiales situées entre la plage de fréquences conservée dans les deux images floues **[35]**.

À la première ; l'image est lissée par convolution avec un noyau gaussien d'une certaine largeur $\sigma 1$:

	$$G\sigma 1\ (x, y) = \frac{1}{2\pi\sigma^2} e^{\left(-\frac{x^2+y^2}{2\sigma 1^2}\right)}$$	(II.1)

Obtenir :

	$$g_1(x,y) = G\sigma_1 (x,y) * f(x,y)$$	(II.2)

Avec une largeur différente $\sigma 2$, une seconde image lissée peut être obtenue :

	$$g_2(x,y) = G\sigma_2(x,y) * f(x,y)$$	(II.3)

Où : G : convolution avec un noyau gaussien d'une certaine largeur.

g : une image lissée gaussienne.

Nous pouvons montrer que la différence de ces deux images lissées gaussiennes, appelée différence de gaussienne(DOG), peut être utilisée pour détecter les contours de l'image.

	$$DOG = g1(x ,y)-g2(x ,y)=G\sigma 1 * f(x ,y) -G\sigma 2 * f(x ,y) = (G\sigma 1 -G\sigma 2)* f(x ,y)= DoG*f(x ,y)$$	(II.4)

Le DOG en tant qu'opérateur ou noyau de convolution est défini comme :

	$$\nabla^2=x\ (t_1, t_2) = \frac{\partial x(t_1,t_2)}{\partial^2 t_1} + \frac{\partial x(t_1,t_2)}{\partial^2 t_2}$$	(II.5)

En tant que différence entre deux images filtrées passe-bas différemment, le DoG est en fait un filtre passe-bande, qui supprime les composants hauts fréquence représentant le bruit, ainsi que certaine composante basse fréquence représentant les zones homogènes de l'image.

On suppose que les composantes de fréquence dans la bande passante sont associées aux bords des images.

II.4 .2.Filtre laplacien :

Dans le traitement d'image, le nom de filtre laplacien fait souvent référence au simple filtre FIR 3 × 3

$$\begin{bmatrix} 0 & -1 & 0 \\ -1 & 4 & -1 \\ 0 & -1 & 0 \end{bmatrix}$$

Utilisé comme une approximation du premier ordre du Laplacien d'une fonction d'espace continu sous-jacente supposée (x, y) **[36]**:

$$\nabla^2 E\,(x, y) = \frac{\partial^2 E(x,y)}{\partial x^2} + \frac{\partial^2 E(x,y)}{\partial y^2} \qquad \textbf{(II.6)}$$

II.4 .3.Technique de normalisation Tan et Triggs :

Le but est de prétraiter les images afin de les rendre robustes/invariantes aux changements d'éclairage en utilisant une étape de prétraitement. Le présent algorithme utilise une série d'étapes pour contrer les effets de la variation d'éclairage, de l'ombrage local et des hautes lumières. Les algorithmes de prétraitement présentent généralement distorsion dans l'image, cependant le but est de préserver les caractéristiques distinctives de l'image. La chaîne de prétraitement se compose des étapes suivantes : Gamma Correction, Différence de gaussien. **[41]**

II.4.4. Extraction de caractéristiques :

L'extraction de caractéristiques représente l'une des étapes les plus cruciales et les plus importantes du FVR. Au cours de cette étape, la propriété quantifiable du trait biométrique de base est créée, appelée modèle, ce qui est utile pour identifier l'individu. Une technique d'extraction efficace des caractéristiques est une étape qui améliore la précision de la reconnaissance des veines des doigts.

II.4.4.1. Méthode binaire locale (LBP) :

Le descripteur de motif binaire local (LBP) est une méthode efficace d'extraction des caractéristiques. Il extrait des informations des valeurs de pixel voisines et développe l'histogramme de l'image. Il s'agit d'un opérateur non paramétrique et décrit la structure spatiale locale d'une image. Il calcule un code binaire à partir de dérivées binaires de pixels puis trouve la différence du pixel central avec ses pixels voisins, arrange ces différences d'une forme ordonnée et finalement ce motif de bits est converti en valeur décimale qui est le nouveau code LBP pour le Pixel central **[38]**. L'opérateur LBP de base fonctionne pour 3 × 3 pixels est décrite par le diagramme suivant:

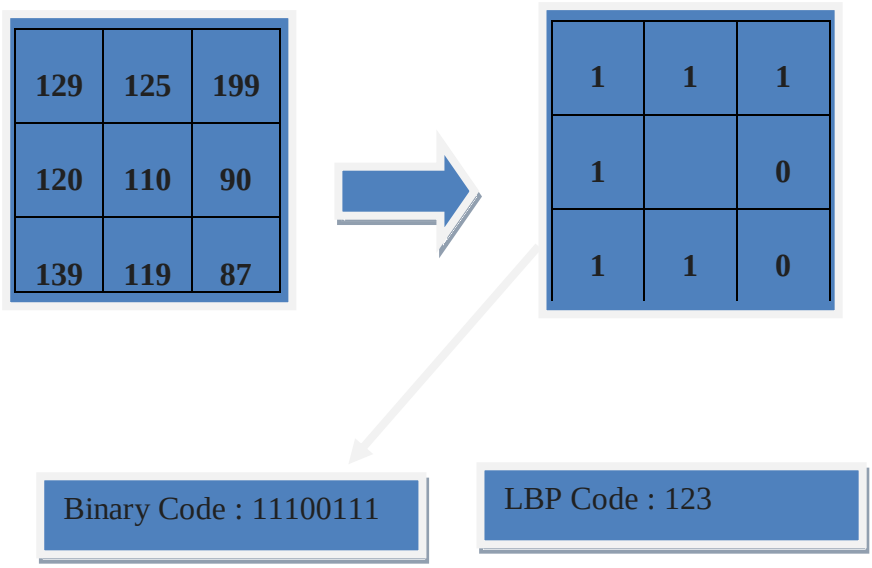


Figure II.4: Opérateur LBP de base.

La figure ci-dessus montre des valeurs d'échelle de gris de 3 × 3 pixels et le code LBP est calculé en utilisant la formule suivante:

n=0

$$(x_c,y_c) = \sum_{n}^{7} S(i_n - i_c)2_n \quad \text{(II.7)}$$

	$\mathbf{s(X)} = \begin{cases} \mathbf{1 \text{ if } (x \geq 0)} \\ \mathbf{0 \text{ if } (x < 0)} \end{cases}$	**(II.7)**

Ici x_c et y_c montrent la position du pixel central, i_n et i_c sont des valeurs d'échelle de gris des pixels environnants et du pixel central respectivement.

II.4.4.2. Quantification de la phase locale (LPQ):

La quantification de la phase locale ou le descripteur LPQ a été désigné pour la première fois par Ojansivu et Heikkilä pour l'utiliser dans la classification de textures pour les images floues. Il permet d'améliorer la classification de textures pour être robuste aux artéfacts générés par le flou présent dans une image. Le descripteur LPQ est construit de façon à ne retenir dans une image que l'information locale invariante à un certain type de flou. Il est insensible au flou central symétrique, tel que celui causé par le mouvement linéaire et hors du foyer du capteur.

L'opérateur LPQ est basé sur TF de la phase (TF : transformée de Fourier). L'extraction de l'information de la phase locale est utilisée par l'application de STFT (la transformée de Fourier à court terme) calculée sur un rectangle NX de M×M voisins pour chaque pixel x dans l'image f (x) définie par l'équation suivante **[39]** :

	$\mathbf{F\ (u, x) = \Sigma_{vEx} f(x-y) e^{2j\pi uTy} = w_u f_x}$	**(II.8)**

Où: wu correspond aux vecteurs de base de la décomposition à la fréquence u, fx contient toutes les valeurs de l'image appartenant au voisinage NX.

La seulement 4 fréquences transformée de Fourier est alors calculée pour :

	$\mathbf{u_i(i = 1,...,4): u_1=[a,0]^T, u_2=[0,a]^T, u_3=[a,a]^T \text{ et } u_4=[a,-a]^T}$	**(II.9)**

Où : représente la fréquence scalaire suffisamment élevée pour Hui Supérieur à 0, alors nous obtenons un vecteurs F_x où :

	$\boldsymbol{FXC} = [F(u_1,x), F(u_2,x), F(u_3,x), F(u_2,x)]$	**(II.10)**

Par la suite, un quantificateur scalaire simple est utilisé pour l'extraction des informations de la phase dans chaque coefficient de Fourier en observant les signes des parties réelles (Re) et imaginaires (Im). Le quantificateur scalaire est donné par l'équation suivante :

	$g_j(x) = \begin{cases} 1 & g_j(x) \geq 0 \\ 0 & \text{ailleurs} \end{cases}$	**(II.11)**

Où : $gj(x)$ représente la $jième$ composante du vecteur $gx = [Re\ \{Fx\}, Im\{Fx\}]$.

Les huit coefficients binaires obtenus $qj(x)$ sont représentés comme des valeurs entières entre 0 et 255 en utilisant un codage binaire simple pour obtenir les étiquettes de LPQ, $FLPQ$ qui est définie par :

	$F_{LPQ}(X) = \sum_{i=1}^{8} q_j(x)\ 2^{j=1}$	**(II.12)**

En conséquence, nous obtenons l'étiquette d'image, dont les valeurs sont invariantes pour le flou (barbouillage) **[39]**.

La figure suivante présente l'organigramme de l'ensemble des étapes nécessaires à la construction du descripteur LPQ pour une image :

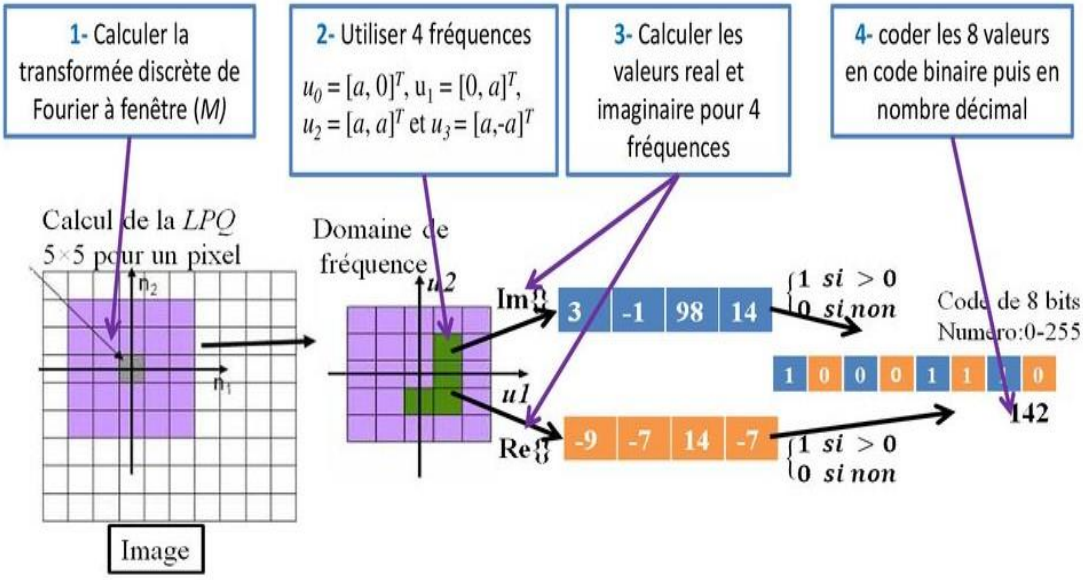


Figure II.5: Extraction de caractéristiques par LPQ et BSIF (34).

II.4.4.3. Inception v3

Inception v3 est un réseau neuronal convolutif d'aide à l'analyse d'images et à la détection d'objets, et fait ses débuts en tant que module pour Google net. Il s'agit de la troisième édition du réseau de neurones convolutif Inception de Google, présenté lors du défi de reconnaissance Image Net. Tout comme Image Net peut être considéré comme une base de données d'objets visuels classés, Inception aide à la classification d'objets dans le monde de la vision par ordinateur. Une de ces utilisations est dans les sciences de la vie, où il aide à la recherche sur la leucémie. Le nom d'origine (Inception) a été nommé de cette façon après qu'un populaire « « nous devons aller plus loin » même Internet » soit devenu viral, citant une phrase du film Inception de Christopher Nolan **[40]**.

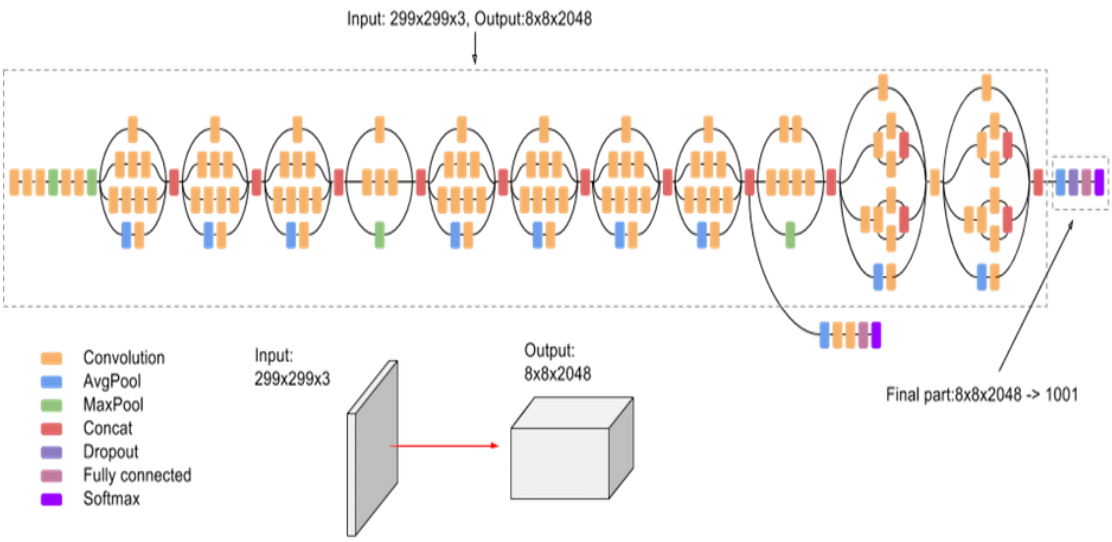


Figure II.6: Inception V3.

II.4.5. La classification

La classification est la catégorisation algorithmique d'objets. Elle consiste à attribuer une classe ou catégorie à chaque objet (ou individu) à classer, en se basant sur des données statistiques. Elle fait couramment appel à l'apprentissage automatique et est largement utilisée en reconnaissance de formes, il existe plusieurs méthodes de classification

II.4.5.1. Machine à Vecteurs de support (SVM)

Les machines à vecteurs de support, ou Séparateur à Vaste Marge (SVM) sont un ensemble de techniques d'apprentissage supervisé destinées à résoudre des problèmes de discrimination et de régression. Les SVMs sont une généralisation des classifier linéaires. Ils ont été développés dans les années 1990 par Valdimir Vapnik grâce à leur capacité de travailler avec des données de grande dimension, leur faible nombre d'hyper paramètre à régler, le fait qu'ils soient bien fondés théoriquement et leur pouvoir de généralisation **[41]**.

II.4.5.2. Définition de K voisin plus proche (K-NN) :

La méthode des K plus proches voisins (KNN) a pour but de classifier des points cibles en fonction de leurs distances par rapport à des points constituant un échantillon d'apprentissage (c'est-à-dire dont la classe est connue a priori).

KNN est une approche de classification supervisée intuitive, souvent utilisée dans le cadre de la machine Learning. Il s'agit d'une généralisation de la méthode du voisin le plus proche (NN). NN est un cas particulier de KNN, où k = 1.

L'approche de classification KNN se base sur l'hypothèse que chaque cas de l'échantillon d'apprentissage est un vecteur aléatoire issu de Rn. Chaque point est décrit comme x =< a1(x), a2(x), a3(x),.., an(x) > où ar(x) correspond à la valeur I du rème attribut. ar(x) peut être soit une variable quantitative soit une variable qualitative.

Afin de déterminer la classe d'un point cible, chaque chacun des k points les plus proches de xq procèdent à un vote. La classe de xq correspond à la classe majoritaire.

Choix de k :

a) **K est grand :** Moins sensible au bruit, une grande base d'apprentissage permet une plus grande plus grande valeur de k.

b) **K est petit :** Rend mieux compte de structure fine, nécessaire pour les petites bases d'apprentissage **[42]**.

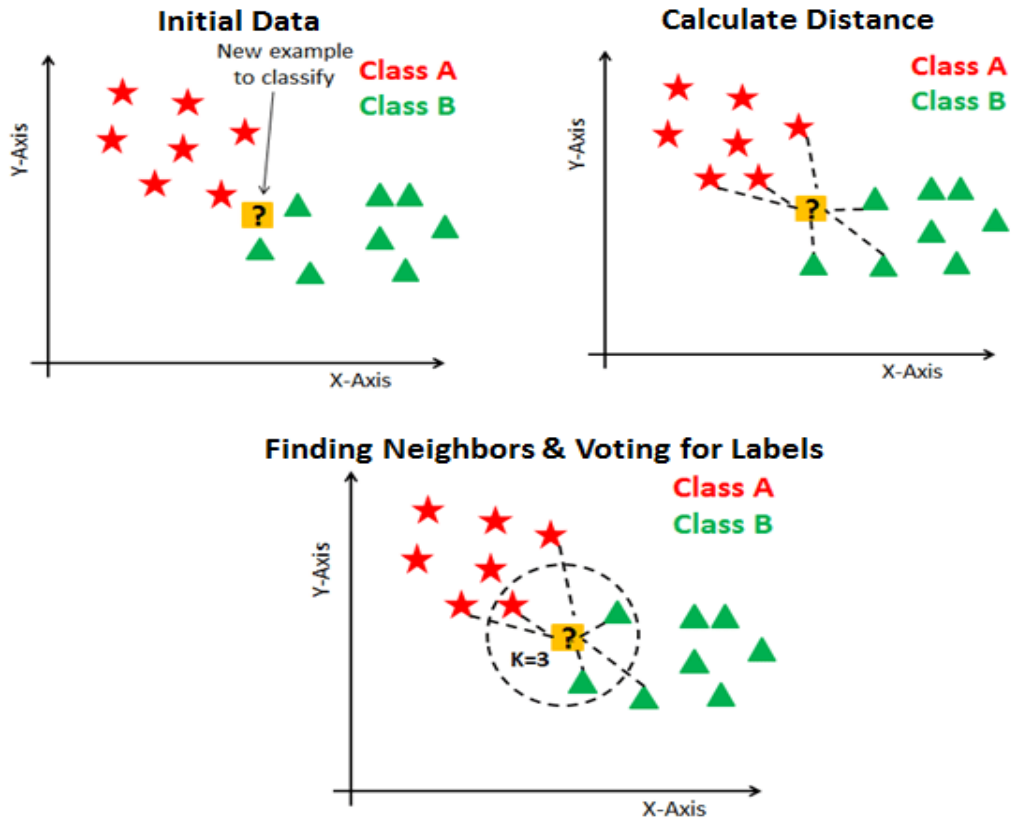


Figure II .7: Méthode des K plus proches voisins (KNN)

II.4.5.3. Random Forest :

Random Forest est un algorithme d'apprentissage automatique flexible et facile à utiliser qui produit, même sans réglage d'hyper-paramètres, un excellent résultat la plupart du temps. C'est également l'un des algorithmes les plus utilisés, en raison de sa simplicité et de sa diversité (il peut être utilisé à la fois pour des tâches de classification et de régression) **[43]**.

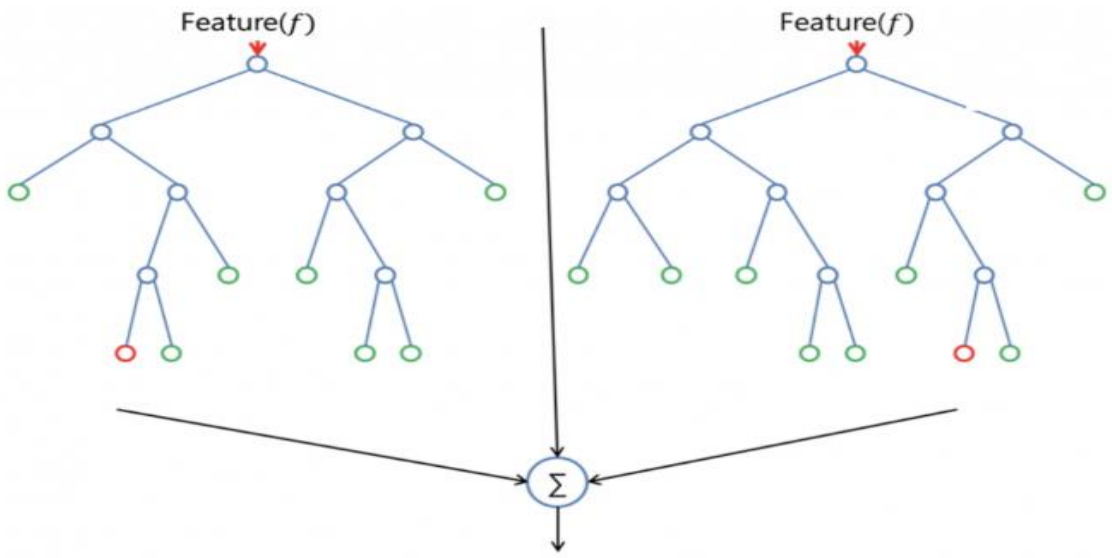


Figure II.8 : Algorithme de Random Forest.

Conclusion

Dans ce chapitre, nous avons présenté la méthode de reconnaissance de la veine du doigt (finger veine) et de ses étapes fiables, Lors de l'étape d'extraction, nous avons présenté algorithmes : LBP, LPQ et Inception v3 pour établir la différence entre eux. En ce qui concerne la classification, nous avons présenté la SVM, K-NN et Random Forest.

CHAPITRE III

APPLICATION ET RESULTATS

Introduction

Dans ce dernier chapitre nous allons présenter la simulation de reconnaissance des personnes par finger veine à l'aide de **Matlab scripte**, en utilisant notre méthode de prétraitement après l'étape de classification et on applique les 3 méthodes de classification qui sont détaillées dans le deuxième chapitre.

III.1. Que signifie MATLAB (Matrix Laboratory)

MATLAB est un logiciel de calcul matriciel à syntaxe simple. Avec ses fonctions spécialisées.

- ✓ Il peut être aussi considéré comme un langage de programmation adapté pour les problèmes scientifiques.
- ✓ Il est un interpréteur : les instructions sont interprétées et exécutées ligne par ligne et il fonctionne dans plusieurs environnements tels que Xwindows, Windows, Macintosh.

Il existe deux (02) modes de fonctionnement :

- ➢ Mode interactif : MATLAB exécute les instructions au fur et à mesure qui sont données par l'utilisateur.
- ➢ Mode exécutif : MATLAB exécute ligne par ligne un "fichier M" (programme en langage MATLAB) **[44]**.

III.2. Organigramme d'identification biométrique

Un système de reconnaissance automatique des finger Vein est une chaîne de traitement qui se divise en étapes qui suivent :

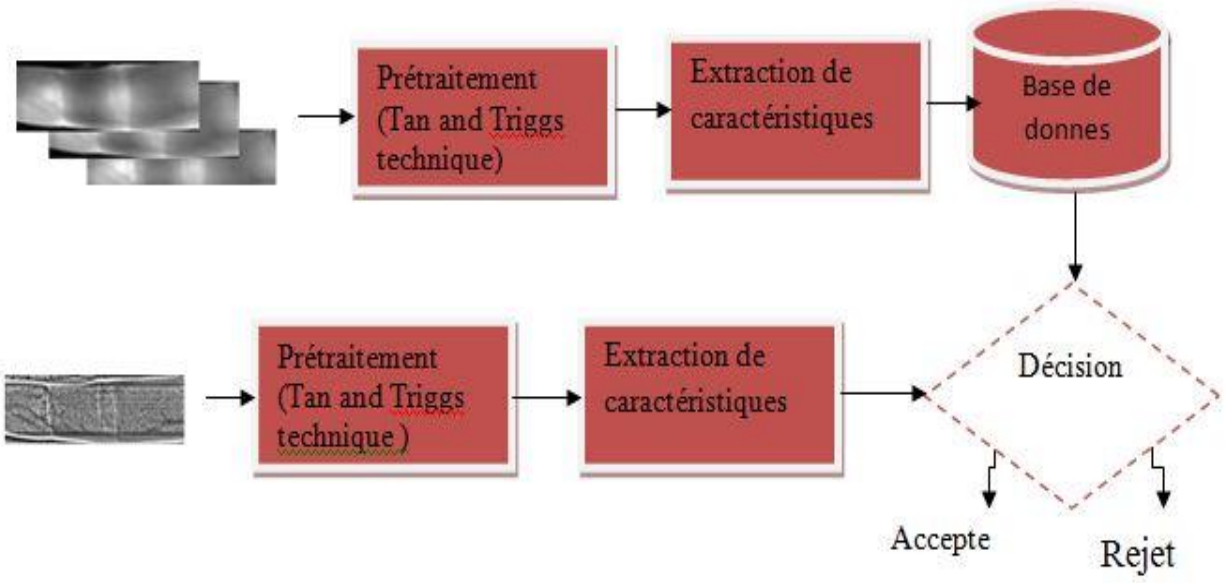


Figure III.1: Organigramme d'identification biométrique (finger Vein).

III.2.1. Technique de normalisation Tan et Triggs :

La technique TT a été introduite par Tan et Triggs dans le domaine de la reconnaissance faciale. Ici, la technique TT a été utilisée pour augmenter le contraste des régions sombres dans l'image de profondeur de la finger Vein et pour atténuer celui des régions lumineuses, pour supprimer le bruit et les gradients d'illumination et normaliser le contraste **[37]**.

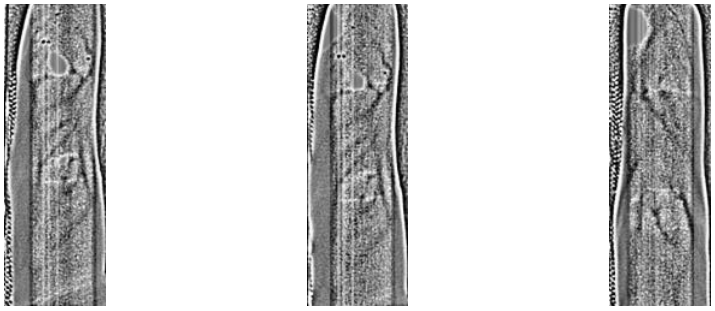


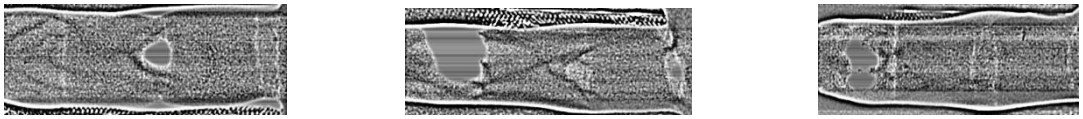
Figure III.2 : Technique de normalisation Tan et Triggs.

III.2.2. Gamma correction :

Le but est d'augmenter le contraste des zones sombres, tout en atténuant celui des zones claires. La première étape est décrite par la relation mathématique:

$$\mathbf{I}'(\mathbf{i},\mathbf{j}) = \begin{cases} \boldsymbol{I}(\mathbf{i},\mathbf{j})\mathbf{for}\boldsymbol{\tau} > 0 \\ \mathbf{log}\big(\boldsymbol{I}(\boldsymbol{i},\boldsymbol{j})\big)\,\boldsymbol{for}\boldsymbol{\tau} = \mathbf{0} \end{cases} \quad \textbf{(III.1)}$$

Où $\boldsymbol{I}$ $(\boldsymbol{i}, \boldsymbol{j})$ représente l'image d'entrée, $\boldsymbol{I}'$ $(\boldsymbol{i}, \boldsymbol{j})$ désigne l'image résultant de la première étape de prétraitement et $\boldsymbol{\tau}$ représente la valeur gamma.



Gamma 0.10 Gamma 0.50 Gamma 0.90

Figure III.3 : exemple d'image de profondeur corrigée avec différentes valeurs gamma.

III.2.3.Différence of Gaussians (DOG):

À la différence des Gaussiens (DOG), un filtre passe-haut a été appliqué pour réduire le crénelage et les bruits existant dans l'image sans raser plus le signal de reconnaissance sous-jacent, alors qu'un filtre passe-bas est appliqué pour supprimer les effets indésirables d'ombres. Le filtre passe-haut et le filtre passe-bas sont mis en œuvre à l'aide du filtre gaussien $\boldsymbol{G\sigma}$ $(\boldsymbol{i}, \boldsymbol{j})$ **[37]**.

$$\mathbf{G}\boldsymbol{\sigma}(\mathbf{i},\mathbf{j}) = \frac{\mathbf{1}}{\mathbf{2}\boldsymbol{\pi}\boldsymbol{\sigma}\mathbf{2}}\mathbf{e}^{-(\mathbf{i2}+\mathbf{j2})/\mathbf{2}}\boldsymbol{\sigma}\mathbf{2} \quad \textbf{(III.2)}$$

La différence de Gaussien (Dog) est obtenue par la différence de deux Gaussiens avec des valeurs de $\boldsymbol{\sigma}$ différentes ($\boldsymbol{\sigma}_1$ et $\boldsymbol{\sigma}_2$ avec $\boldsymbol{\sigma}_2 > \boldsymbol{\sigma}_1$) mais proches

	$g_1(i,j) = G\sigma_1(i,j) * I'(i,j)$	**(III.3)**

$\boldsymbol{I''(i,j)}$ est l'image résultante du filtre Dog, qui a été calculée par l'équation suivante:

	$I''(i,j) = g1(i,j) - g2(i,j) = (G\sigma1(i,j) - G\sigma2(i,j)) * I'(i,j)$	**(III.4)**

III.3. Expérience sur les images finger Vein :

III.3.1 base de donnes :

La base de données finger Vein comprend 42 sujets (personnes), 6 doigts par sujet et 5 images par doigt en une session **[33]**. Par conséquent, la base de données finger Vein contient1260 images. Les images brutes ont une résolution de 1280 × 1024 pixels et sont stockées en 8 bits. Le format PNG en niveaux de gris. La zone visible du doigt sur les images est de 600 × 180 pixels. Quelques exemples d'images sont illustrés à **Figure III.6.**

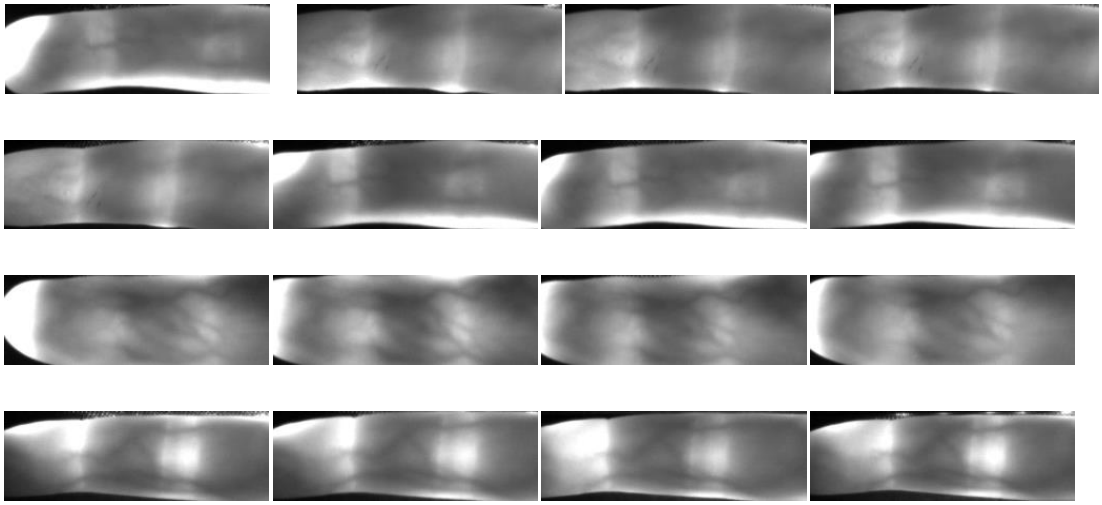


Figure III.4: Quelques exemples de Base de données.

III.3.2. Séparation de la base de données :

Les cinq images des veines des doigts sont divisées en deux groupes: le premier groupe pour effectuer l'apprentissage (2 images) , et le deuxième groupe pour tester les techniques et déterminer leurs performances (3 images).

III.4. Résultats Expérimentales

Dans cette partie on applique la Technique de normalisation Tan et Triggs pour le prétraitement des images finger Vein et **Inception v3** pour l'extraction de caractéristiques et différents classificateurs (KNN, SVM et Random Forest) sur les six finger (annulaire droit, majeur droit, index droit, annulaire gauche, majeur gauche, index gauche).

Les figures suivantes montrent les images des finger après l'application de Tan et Triggs :

Figure III.5:doigt annulaire droit avec la méthode tan et triggs.

Figure III.6:doigt majeur droit avec la méthode tan et triggs.

Figure III.7:doigt index droit avec la méthode tan et triggs.

Figure III.8 : doigt annulaire gauche avec la méthode tan et triggs.

Figure III.9:doigt majeur gauche avec la méthode tan et triggs.

Figure III.10:doigt index gauche avec la méthode tan et triggs.

Les tableaux suivant monteront les taux de reconnaissances (Accuracy) avec les différentes valeurs de Gamma correction pour les six finger.

- **Avec veine de doigt annulaire droit :**

	0.1	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**	**0.7**	**0.8**	**0.9**
KNN	89	89	**89**	87	87	87	81	50	89
SVM	75	64	**78**	35	34	34	34	50	66
Random Forest	85	85	**87**	81	81	81	81	50	86

Tableau III.1 : Le taux de reconnaissance de doigt annulaire droit avec les différentes valeurs de Gamma correction.

la meilleur valeur **gamma= (0.3)** , KNN=89% , SVM=78% , Random Forest=87% .

- **Avec veine de doigt majeur droit :**

	0.1	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**	**0.7**	**0.8**	**0.9**
KNN	92	92	**92**	91	91	90	90	91	91
SVM	36	33	**49**	46	42	40	37	49	46
Random Forest	76	75	**77**	75	76	75	76	76	76

Tableau III.2 : Le taux de reconnaissance de doigt majeur droit avec les différentes valeurs de Gamma correction.

la meilleur valeur **gamma= (0.3)** , KNN=92% , SVM=49% , Random Forest=77% .

- **Avec veine de doigt index droit :**

	0.1	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**	**0.7**	**0.8**	**0.9**
KNN	82	77	83	83	80	81	81	**83**	81
SVM	14	33	45	40	58	46	58	**58**	54
Random Forest	72	69	69	66	71	72	72	**73**	73

Tableau III.3 : Le taux de reconnaissance de doigt index droit avec les différentes valeurs de Gamma correction.

la meilleur valeur **gamma= (0.8)** , KNN=83% , SVM=58% , Random Forest=73% .

- **Avec veine de doigt annulaire gauche :**

	0.1	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**	**0.7**	**0.8**	**0.9**
KNN	84	86	88	86	85	**89**	88	85	86
SVM	15	16	37	16	17	**44**	35	30	16
Random Forest	70	71	74	71	71	**75**	75	71	71

Tableau III.4 : Le taux de reconnaissance de doigt annulaire gauche avec les différentes valeurs de Gamma correction.

la meilleur valeur **gamma= (0.6)** , KNN=89% , SVM=44% , Random Forest=75% .

- **Avec veine de doigt majeur gauche :**

	0.1	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**	**0.7**	**0.8**	**0.9**
KNN	81	84	81	**86**	80	83	81	84	82
SVM	59	22	16	**59**	49	34	45	56	55
Random Forest	72	67	66	**73**	71	69	72	71	72

Tableau III.5 : Le taux de reconnaissance de doigt majeur gauche avec les différentes valeurs de Gamma correction.

la meilleur valeur **gamma= (0.4)** , KNN=86% , SVM=59% , Random Forest=73% .

- **Avec veine de doigt index gauche :**

	0.1	**0.2**	**0.3**	**0.4**	**0.5**	**0.6**	**0.7**	**0.8**	**0.9**
KNN	91	90	88	89	90	91	91	91	**92**
SVM	16	20	13	17	17	19	20	22	**23**
Random Forest	45	45	44	43	43	40	45	50	**55**

Tableau III.6 : Le taux de reconnaissance de doigt index gauche avec les différentes valeurs de Gamma correction.

la meilleur valeur **gamma= (0.9)** , KNN=92% , SVM=23% , Random Forest=55% .

Dans cette étape les tableaux suivent monté les différentes valeurs de Dog et les résultats de l'Accuracy qui obtenez, dans les premiers tableaux, nous avons fixé une valeur et changé l'autre Dog=(x, 0.6, **2**) pour les six doigts.

- **Avec veine de doigt annulaire droit :**

	(0.6,**2**)	(1,**2**)	(1.2,**2**)	**(1.6, 2)**	(2, **2**)	(2.2, **2**)	(2.6, **2**)	(3,**2**)
KNN	86	86	86	**87**	86	86	86	86
SVM	34	37	36	**37**	36	36	36	34
Random Forest	81	80	80	**81**	81	80	81	79

Tableau III.7 : Le taux de reconnaissance de doigt annulaire droit avec les différentes valeurs de Dog (2 fixé).

la meilleur valeur de **Dog=(x, 1.6, 2)**, KNN=87% , SVM=37% , Random Forest= 81%.

- **Avec veine de doigt majeur droit :**

	(0.6,**2**)	(1,**2**)	(1.2,**2**)	**(1.6, 2)**	(2, **2**)	(2.2, **2**)	(2.6, **2**)	(3,**2**)
KNN	75	75	75	**75**	75	75	75	75
SVM	33	37	34	**37**	35	34	34	46
Random Forest	69	69	67	**69**	69	64	64	67

Tableau III.8 : Le taux de reconnaissance de doigt majeur droit avec les différentes valeurs de Dog(2 fixé).

la meilleur valeur de **Dog=(x, 1.6, 2)**, KNN=75% , SVM=37% , Random Forest= 69%.

- **Avec veine de doigt index droit :**

	(0.6,**2**)	(1,**2**)	(1.2,**2**)	(1.6, **2**)	(2, **2**)	**(2.2, 2)**	(2.6, **2**)	(3,**2**)
KNN	80	81	81	81	80	**82**	81	81
SVM	45	42	42	37	40	**45**	42	39
Random Forest	75	77	74	75	75	**77**	73	75

Tableau III.9 : Le taux de reconnaissance de doigt index droit avec les différentes valeurs de Dog (2 fixé).

la meilleur valeur de **Dog=(x, 2.2, 2)**, KNN= 82% , SVM=45% , Random Forest=77%.

- **Avec veine de doigt annulaire gauche :**

	(0.6,**2**)	(1,**2**)	(1.2,**2**)	**(1.6, 2)**	(2, **2**)	(2.2, **2**)	(2.6, **2**)	(3,**2**)
KNN	92	90	92	**92**	91	90	90	90
SVM	16	50	44	**50**	23	45	46	45
Random Forest	80	80	81	**81**	80	81	81	80

Tableau III.10 : Le taux de reconnaissance de doigt annulaire gauche avec les différentes valeurs de Dog (2 fixé).

La meilleur valeur de **Dog=(x, 1.6, 2)**, KNN=92%, SVM=50%, Random Forest= 81%.

- **Avec veine de doigt majeur gauche :**

	(0.6,**2**)	(1,**2**)	(1.2,**2**)	**(1.6, 2)**	(2, **2**)	(2.2, **2**)	(2.6, **2**)	(3,**2**)
KNN	86	82	82	**89**	76	86	86	83
SVM	36	36	33	**37**	16	34	36	13
Random Forest	79	79	76	**79**	74	74	74	72

Tableau III.11 : Le taux de reconnaissance de doigt majeur gauche avec les différentes valeurs de Dog (2 fixé).

La meilleur valeur de **Dog=(x, 1.6, 2)**, KNN=89%, SVM=37%, Random Forest= 79%.

- **Avec veine de doigt index gauche :**

	(0.6,**2**)	(1,**2**)	(1.2,**2**)	**(1.6, 2)**	(2, **2**)	(2.2, **2**)	(2.6, **2**)	(3,**2**)
KNN	82	83	83	**83**	83	83	81	81
SVM	50	50	50	**55**	51	55	51	51
Random Forest	77	76	76	**79**	76	77	77	79

Tableau III.12 : Le taux de reconnaissance de doigt index gauche avec les différentes valeurs de Dog (2 fixé).

La meilleur valeur de **Dog=(x, 1.6, 2)**, KNN=83%, SVM=55%, Random Forest= 79%.

La même opération pour les tableaux suivant. Nous gardons la valeur qui nous a donné le meilleur résultat de l'accuracy **(1.6)** et changeons l'autre jusqu'à ce que nous obtenions le meilleur résultat de l'accuracy.

- **Avec veine de doigt annulaire droit :**

	(**1.6,**0.6)	(**1.6,**1)	(**1.6,**1.2)	(**1.6,**1.6)	(**1.6,**2)	(**1.6,**2.2)	(**1.6,**2.6)	**(1.6,3)**
KNN	86	86	83	86	84	86	86	**86**
SVM	38	34	37	34	37	37	37	**38**
Random Forest	80	81	80	81	81	80	80	**81**

Tableau III.13 : Le taux de reconnaissance de doigt annulaire droit avec les différentes valeurs de Dog (1.6 fixé).

la meilleur valeur de **Dog=(x, 1.6, 3)**, KNN=86%, SVM=38%, Random Forest= 81%.

- **Avec veine de doigt majeur droit :**

	(**1.6,**0.6)	(**1.6,**1)	(**1.6,**1.2)	(**1.6,**1.6)	(**1.6,**2)	(**1.6,**2.2)	(**1.6,**2.6)	**(1.6,3)**
KNN	81	80	88	75	79	88	89	**89**
SVM	16	27	22	15	35	35	35	**40**
Random Forest	69	67	69	69	69	68	69	**70**

Tableau III.14 : Le taux de reconnaissance de doigt majeur droit avec les différentes valeurs de Dog (1.6 fixé).

la meilleur valeur de **Dog=(x, 1.6, 3)**, KNN=89%, SVM=40%, Random Forest= 70%.

- **Avec veine de doigt index droit :**

	(**1.6,**0.6)	(**1.6**,1)	**(1.6,1.2)**	(**1.6,**1.6)	(**1.6,**2)	(**1.6,**2.2)	(**1.6,**2.6)	(**1.6,**3)
KNN	92	92	**92**	91	90	90	90	91
SVM	36	33	**49**	46	42	40	37	49
Random Forest	76	75	**77**	75	76	75	76	76

Tableau III.15 : Le taux de reconnaissance de doigt index droit avec les différentes valeurs de Dog (1.6 fixé).

La meilleur valeur de **Dog=(x, 1.6, 1.2)**, KNN=92%, SVM=49%, Random Forest=77%.

- **Avec veine de doigt annulaire gauche :**

	(**1.6,**0.6)	**(1.6,1)**	(**1.6,**1.2)	(**1.6,**1.6)	(**1.6,**2)	(**1.6,**2.2)	(**1.6,**2.6)	(**1.6,**3)
KNN	88	**90**	88	86	89	89	89	89
SVM	50	**58**	56	44	54	51	50	55
Random Forest	79	**81**	80	79	79	79	80	79

Tableau III.16 : Le taux de reconnaissance de doigt annulaire gauche avec les différentes valeurs de Dog (1.6 fixé).

la meilleur valeur de **Dog=(x, 1.6, 1)**, KNN=88%, SVM=58% , Random Forest= 81%.

- **Avec veine de doigt majeur gauche :**

	(**1.6,**0.6)	(**1.6,**1)	(**1.6,**1.2)	(**1.6,**1.6)	**(1.6,2)**	(**1.6,**2.2)	(**1.6,**2.6)	**(1.6,**3)
KNN	86	84	88	85	**89**	88	85	86
SVM	16	37	16	17	**44**	35	30	16
Random Forest	70	71	74	71	**75**	71	71	71

Tableau III.17 : Le taux de reconnaissance de doigt majeur gauche avec les différentes valeurs de Dog (1.6 fixé).

la meilleur valeur de **Dog=(x, 1.6, 2)**, KNN=89% , SVM=44% , Random Forest=75%.

- **Avec veine de doigt index gauche :**

	(1.6,0.6)	(**1.6,**1)	(**1.6,**1.2)	(**1.6,**1.6)	(**1.6,**2)	(**1.6,**2.2)	(**1.6,**2.6)	**(1.6,**3)
KNN	**81**	84	81	78	77	81	77	77
SVM	**59**	22	16	34	44	17	16	16
Random Forest	**72**	67	66	69	69	66	66	66

Tableau III.18 : Le taux de reconnaissance de doigt index gauche avec les différentes valeurs de Dog (1.6 fixé).

La meilleur valeur de **Dog=(x, 1.6, 0.6)**, KNN=81%, SVM=59%, Random Forest= 72%.

Discussion :

Veine du doigt de la main gauche:

On remarque que la meilleure méthode de classification KNN qui donne un accuracy de 91%, soit environ 92% pour le doigt index par rapport aux deux autres méthodes, qui donnent un taux accuracy : Random Forest= 81%, SVM=76%.

Veine du doigt de la main droite:

On observe d'après les résultats que la meilleure méthode d'identification est KNN aussi qui donne un accuracy de 88% pour le doigt index par rapport aux deux autres méthodes, qui donnent un accuracy : Random Forest= 84%, SVM=69%.

C'est à travers ces deux comparaisons on conclut que la meilleure méthode de classification est 'KNN' et que le bon doigt et le plus proche pour la reconnaissance est 'l'index'.

Conclusion :

Dans ce chapitre, nous avons présenté les résultats du système d'identification des veines des doigts basées sur les méthodes de classification KNN, SVM et Random Forest: grâce aux différents résultats obtenus par chaque méthode à chaque doigt, La méthode KNN s'est plus efficace pour identifier la veine du doigt par rapport aux deux autres méthodes.

CONCLUSION GENERALE

CONCLUSION GENERALE

Le travail réalisé dans le cadre de ce mémoire a pour objectif d'étudier l'un des systèmes biométriques permettant d'identifier les individus en fonction de la veine du doigt, car la précision de la reconnaissance joue un rôle important, cette technologie biométrique est considérée comme étant très forte en termes de sécurité.

A cause de ces caractéristiques biométriques qui sont uniques à l'individu, avec une possibilité presque nulle, que d'autres individus peuvent avoir les mêmes caractéristiques. Même pour le cas de jumeaux identiques.

Nous avons travaillé sur la façon d'identifier les individus dans le système biométrique (veines des doigts) à l'aide des méthodes de classification :
Nous avons choisi les méthodes : KNN, SVM, Random Forest.

Grâce à ces méthodes, nous avons atteint un accuracy idéal en particulier pour KNN, ce qui est très intéressant car il fiabilise notre système et nous permet d'atteindre le but que nous nous avions fixé au départ : développer un système permettant la reconnaissance des individus.

Dans la dernière partie, nous avons utilisé la technique de la veine du doigt pour extraire des caractéristiques individuelles avec des résultats très satisfaisants et nous avons acquis une bonne réputation dans ce domaine.

BIBLIOGRAPHIE

[01] Rania Bba, chapitre 1 système de reconnaissance de visage, Academia.

[02] DIB Soumeya, identification des individus par la technique multimodale, UNIVERSITE ORAN, (2014-2015)

[03] Halaimia Nabil, reconnaissance biométrique via l'apprentissage approfond, UNIVERSITE TEBESSA, (2017-2018).

[04] https://www.memoireonline.com/02/13/6979/Reconnaissance-de-visages-par-Analyse-Discriminante-LineaireLDA-.html par Amira Chiheb Université du 8 mai 45 de Guelma Algérie - Licence en informatique 2003. Academia

[05] BENCHNNANE Ibtissame, Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus, UNIVERSITE ORAN, 2015.

[06] CHAKOUR Alla Eddine, Identification biométriques des personnes par les empreintes d'articulation du doigt, UNIVERSITE ANNABA ,2019.

[07] BOURENEB Aziza, Identification des personnes par leurs empreintes palmaire, UNIVERSITÉ GUELMA ,2019

[08] http://www.journaldunet.com/solutions/0611/061127-biometrie/8.shtml.

[09] TELIB Lina, BENAGGA, Abderahmane, Reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt, UNIVERSITÉ KASDI MARBEH OUARGLA, 2015-2016.

[10] CHAA Mourad, thèse, système de reconnaissance de personne par des technique biométrique, UNIVERSITE Ferhat Abbas – SETIF ,2017

[12] MOHEMED ELabed, Évaluation de système biométrique. Cryptographie et sécurité [cs.CR]. Université de Caen, 2011.

[13] HAFS Toufik, thése, Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne UNIVERSITE ANNABA ,2016

[14] Wang, H., Li, S. Z., Wang, Y., & Zhang, J. (2004, October). Self-quotient image for face recognition. In Image Processing, 2004. ICIP'04. 2004 International Conference on (Vol. 2, pp. 1397-1400). IEEE

[15] Vitomir struc, the IN face toolbox v2.1 the Matlab toolbox for illumination invariant face recognition, faculty of Electrothechnical Engineering- university of Ljubljana, 2012

[**16] BERREDJEM Achref**, La reconnaissance des individus par leur empreinte des articulations des doigts, UNIVERSITÉ GUELMA,2019

[17] Douidi Dahbia , **Grini Soumia**. Identification et Reconnaissance Biométrique par l'Utilisation des Empreintes Palmaires, Master Académique, université Akli Mohnad Oulhadj , Bouira 24.09.2017 .

[18] https://builtin.com/data-science/step-step-explanation-principal-component-analysis.

[19] ChihebAmira, **Bouhalit Nasereddine**. Reconnaissance de Visages par Analyse Discriminante Linéaire (LDA).Licence Informatique, Université du 8 Mai 45, Guelma, 2003.

[20] https://en.wikipedia.org/wiki/Log_Gabor_filter

[21] https://www.peterkovesi.com /matlabfns/Phase Congruency/Docs/convexpl.html

[22] Bilal Attallah, Amina Serir, Youssef Chahir, Abdelwahhab Boudjelal. Histogram of gradient and binarized statistical image features of wavelet subband-based palmprint features extraction. Journal of Electronic Imaging, SPIE and IS&T, 2017, 26 (06), ff10.1117/1.JEI.26.6.063006ff. ffhal-01823153f

[23] https://en.wikipedia.org/wiki/Difference_of_Gaussians

[24] OUAMANE, Abdelmalik, Reconnaissance Biométrique par Fusion Multimodale duVisage 2D et 3D. Université Mohamed Khider - Biskra.2015

[25] CHOUCHANE Ammar, Analyse d'images d'expressions faciales et orientation de la tête basée sur la profondeur, Doctorat LMD en Génie Electrique, Université Mohamed Khider Biskra 2016.

[26] SRZhou, JP Yin, JM Zhang, Motif binaire local (LBP) et quantification de phase locale (LBQ) basée sur le filtre de Gabor pour la représentation de visage, 2013

[27] David RECHAL, 'Analyse du potentiel des classifications de type SVM pour l'identification des parcelles arborées dans les images de télédétection à très haute résolution spatiale ' . Université Pierre et Marie Curie – Paris VI, 17 Mars 2008 – 12 Septembre 2008

[28] "Barclays – Hitachi Digital Security". Retrieved 17 May 2018.

[29] "Archived copy" (PDF). Archived from the original (PDF) *on 19* March 2012. Retrieved 6 July 2011

[30] "Finger Vein Authentication Technology". Hitachi America, Ltd. Retrieved 21 January 2011.

[31] "PV2000". India*:* Mantra Softech Pvt. Ltd. Retrieved 21 January 2011.

[32] "Your hand is the key: The world's first contactless palm vein authentication technology". PalmSecure. Fujitsu. Retrieved 21 January 2011.

[33] sensoras article " Combined Fully Contactless Finger and Hand Vein Capturing Device with a Corresponding Dataset" 17 November 2019.

[34] mémoire Seddiki Amel+Halimi Abir "Système Biométrique pour la Reconnaissance des Articulations des Doigts et la Méthode de Quantification de phase Local", Université Kasdi Merbah Ouargla 2019.

[35] R.A. Haddad and A.N. Akansu, "A Class of Fast Gaussian Binomial Filters for Speech and Image Processing," IEEE Transactions on Acoustics, Speech and Signal Processing, vol. 39, pp 723-727, March 1991.

[36] " John W. Woods, in Multidimensional Signal, Image, and Video Processing and Coding" (Second Edition), 2012.

[37] "**Chaa Mourad**" 3D Palmprint Recognition using Tan and Triggs Normalization Technique and GIST Descriptors Université Kasdi Merbah Ouargla.

[38] harpreet kaur1, lakhwinder kaur,< performance comparison of different feature detection methods with gabor filter >, department of computer engineering, punjabi university, patiala, punjab, india; disponible [https://pdfs.semanticscholar.org/e375/e5aabc37af5f5b0d0803e880f5252dda6d61.pdf].

[39] " Mark S. Nixon and Alberto S. Aguado. Feature Extraction and Image Processing". Academic Press, 2008, p. 88.

[40]anil,k.j.;arun,a.r.;nandakumar,k.introduction to biometric; springer: berlin, germany, 2011;disponible,<<https://www.mdpi.com/2078-2489/9/9/213/htm>>.

[41] Tan and Triggs Illumination Normalization Pi19404 January 23, 2014 Contents.

[42] mémoire Identification biométrique des personnes par les veines des doigts Douali Faiza Université Badji Mokhtar Annaba.

[43] benagga Abderrahmane et telib lina- reconnaissance des personnes basée sur l'empreinte de l'articulation de doigt- université kasdi merbah Ouargla-2016.

[44] Heckbert, Paul S. (novembre 1986). "Enquête sur la cartographie des textures" (PDF) . Infographie et applications IEEE . 6 (11): 56–67. doi : 10.1109 / MCG.1986.276672. Récupéré 20/10/2017.