REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE YAHIA FARES DE MEDEA



Faculté de **T**echnologie

Mémoire de fin d'études de Master

Filière : Electronique
Spécialité : Electronique des systèmes embarqués

Utilisation du modèle LBP pour l'extraction des caractéristiques des images veines des doigts

---

Présenté par :

Elmohri Madani

Proposé et Dirigé par :

BOUCHERIT ISMAIL

Promotion 2020

.ملخص

.الهدف من هذه الدراسة هو تطوير نظام لتحديد الأفراد من عروق أصابعهم التي هي فريدة من نوعها للأفراد

يعتمد نظامنا على مبدأ التعلم الآلي، الذي استخرجنا منه المعلمات المميزة

مثل.LPQ و LLBP و LBP

بعد هذه الخطوة، سيكون نظامنا قادرا على تقرير ما إذا كان شخص جديد ينتمي إلى القاعدة أم لا

حيث وجدنا ان المعلومات LBPتعطي أفضل معدل تعرف اذ يصل الى 95 ٪

الكلمات المفتاحية: نظام لتحديد الأفراد، عروق أصابعهم، التعلم الآلي، النمط الثنائي المحلي، ميزات صورة إحصائية ثنائية , تكميم المرحلة المحلية , المصنف , القاعدة , معدل التعرف

Résumé:

L’objectif de ce étude 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 LBP, LLBP et LPQ. Ces paramètres seront l’entré du classificateur K-NN (K-voisins plus proches). Après cette étape notre système sera capable de décider es ce que une nouvelles personne appartient à la base ou non. Nous avons trouvé que les paramètres LBP présentent le meilleur taux de reconnaissance qui atteint les 99%.

Mots-clés: système d’identification, veines de doigts, apprentissage, LBP, LLBP, LPQ, classificateur K-NN, la base, taux de reconnaissance.

Abstract:

The objective of this study is to develop a system of identifying individuals from their finger veins that are unique to the individual. Our system is based on the principle of automatic learning, from which we extracted characteristic parameters such as LBP, LLBP and LPQ. These parameters will be the input of the KNN classifier (K-nearest neighbors). After this step our system will be able to decide whether a new person belongs to the base or not. We found that the LBP parameters have the best recognition rate of 99%.

Keywords: system of identifying, finger veins, learning, LBP, LLBP, LPQ, KNN classifier, the base, recognition rate.

شكر وتقدير:

اللهم لك الحمد حمدا كثيرا طيبا مباركا فيه، ملء السماوات وملء الأرض، وملء ما شئت من شيء بعد، أهل الثناء والمجد، أحق ما قال العبد، وكلنا لك عبد، أشكرك ربي على نعمك التي لا تعد، وآلائك التي لا تحد، أحمدك ربي وأشكرك على أن يسرت لي إتمام هذا البحث على الوجه الذي أرجو أن ترضى به عني.

ثم أتوجه بالشكر إلى من رعاني طالبا في برنامج الماستر، ومعدا هذا البحث أستاذي ومشرفي الفاضل الأستاذ: بوشريط اسماعيل، الذي له الفضل - بعد الله تعالى- على البحث والباحث مذ كان الموضوع عنوانا وفكرة إلى أن صار رسالة وبحثا. فله مني الشكر كله والتقدير والعرفان.

وأتوجه بالشكر الجزيل إلى جميع الأساتذة الفضلاء بجامعة يحي فارس الذين لم يألوا جهدا ويوجب علي الاعتراف بالفضل

وأتقدم بشكري الجزيل في هذا اليوم إلى أساتذتي الموقرين في لجنة المناقشة رئاسة وأعضاء لتفضلهم علي بقبول مناقشة هذه الرسالة، فهم أهل لسد خللها وتقويم معوجها وتهذيب نتوآتها والإبانة عن مواطن القصور فيها، سائلا الله الكريم أن يثيبهم عني خيرا.

Liste des abréviations

PIN : Personal Identification Number **(**Numéro d'Identification Personnel).

ADN : Acide Désoxyribose Nucléique.

IBG : International Biometric Group.

FVR : Finger Vein Recognition **(**Reconnaissance des Veines des Doigts).

ROI : Region of Interest (Région d'intérêt).

LBP : Méthode Binaire Locale.

LLBP: Local Line Binary Pattern.

LLBPh: Local Line Binary Pattern horizental.

LLBPv: Local Line Binary Pattern

vertical. **LLBPm:** Local Line

Binary Pattern magnitude. **LPQ :**

Quantification de la Phase Locale.

2DWFT : Transformée Discrète de Fourier à Fenêtre à Deux Dimensions.

SVM : Machine à Vecteurs de Support.

ADD : Arbre De Décision.

KNN : K-Nearest Neighbors (K plus Proches Voisines).

Sommaire

INTRODUCTION GENERALE_____ 2

CHAPITRE I : LA BIOMETRIE_____ 5

I-1 INTRODUCTION_____ 6

I-2DEFINITION : _____ 7

I-3 UN BREF HISTORIQUE DE LA BIOMETRIE :_____ 7

I-4 QU'EST CE QUE LA BIOMETRIE ?_____ 9

I – 5 LES SYSTEMES BIOMETRIQUES ET LEURS MODES DE FONCTIONNEMENTS :_____ 11

I – 5 -1-LE MODULE DE CAPTURE_____ 11

I-5- 2-LE MODULE D'EXTRACTION DE CARACTERISTIQUES_____ 11

I-5-3-LE MODULE DE CORRESPONDANCE_____ 11

I-5-4-LE MODULE DE DECISION _____ 11

I-6 LES DIFFERENTES TECHNIQUES BIOMETRIQUES _____ 12

- LA PERFORMANCE, _____ 14

- L'ACCEPTABILITE, _____ 14

- LE CONTOURNEMENT,_____ 14

I.7. ANALYSES BIOLOGIQUES : _____ 14

I.7. 1. L'ODEUR CORPORELLE : _____ 14

I-7- 2. L'A.D.N. (SUPPORT MATERIEL DE L'HEREDITE):_____ 14

I. 7-. 3. LA RECONNAISSANCE DE LA THERMOGRAPHIE FACIALE : 15

I. 8.1. ANALYSES MORPHOLOGIQUES : 15

I. 8.1. 1. LES EMPREINTES DIGITALES : 15

I.8.2. 2. LA GEOMETRIE DE LA MAIN : 16

I-9 RECONNAISSANCE DE RESEAU VEINEUX DE LA MAIN 17

EST-CE QUE LE RESEAU VEINEUX DE LA MAIN EST UNE BONNE MODALITE BIOMETRIQUE ? 18

UNIVERSALITE: 18

LA FACILITE DE MESURE: 18

LA PERMANENCE: 18

UNICITE : 18

I-9-1 RECONNAISSANCE DES EMPREINTES DIGITALES : 19

I-9-2 RECONNAISSANCE FACIALE : 19

I-9-3 RECONNAISSANCE DE LA MAIN : 20

I-9-4 RECONNAISSANCE DE L'IRIS : 20

I-9-5 RECONNAISSANCE DE LA RETINE: 21

I-9-6 RECONNAISSANCE DE LA VOIX : 21

I-10 STRUCTURE D'UN SYSTEME COMPLET DE RECONNAISSANCE DE RESEAU VEINEUX DE LA MAIN 22

I-10-1 L'ACQUISITION D'IMAGE ET PRETRAITEMENT 22

I-10-2 LA SEGMENTATION 23

I-10-3 L'EXTRACTION DES PARAMETRES ET LA RECONNAISSANCE 23

I-10-4 LES PROBLEMES POSES PAR L'UTILISATION DE LA BIOMETRIE 23

I-11 AVANTAGES DE LA BIOMETRIE POUR LA SECURITE 25

I-11-1 IDENTIFICATION ET AUTHENTIFICATION : 25

I-11-1-1 VITESSE ET PRECISION 25

I-11-1-2 UN GRAND SENS DES RESPONSABILITES 25

I-11-1-3 EFFICACITE MAXIMALE 25

I-11-1-4 MOT D'ORDRE : L'ASPECT PRATIQUE 25

I-11-1-5 ÉVOLUTIF POUR ACCOMPAGNER LA CROISSANCE 26

I-11-1-6 SECURITE ET RENTABILITE 26

I-11-1-7 UTILISATION SIMPLE ET ERGONOMIQUE 26

I-12 CONCLUSION 27

CHAPITRE II : DESCRIPTION D'UNSYSTEME D'IDENTIFICATION 28

II.1. INTRODUCTION : 29

II.2. SYSTEME D'IDENTIFICATION : 30

II.3. BIOMETRIE DES VEINES DU DOIGT, PRINCIPE ? 30

II.4. RECONNAISSANCE DES VEINES DES DOIGTS (FVR) : 31

II.4.1. PRETRAITEMENT : 31

II.4.1.1. ROI EXTRACTION : 31

II.4.2. EXTRACTION DE CARACTERISTIQUES : 31

II.4.2.1. METHODE BINAIRE LOCALE (LBP) : 32

II.4.2.2. LOCAL LINE BINARY PATTERN (LLBP): 33

II.4.2.3. QUANTIFICATION DE LA PHASE LOCALE (LPQ): 36

II.4.3. LA CLASSIFICATION : 37

II-5 APPRENTISSAGE 37

II-5.1. APPRENTISSAGE SUPERVISE 38

II-5.2. APPRENTISSAGE NON-SUPERVISE 38

II-6.3.1. MACHINE A VECTEURS DE SUPPORT (SVM) : 38

II-6.3.2. ARBRE DE DECISION (ADD) : 39

II.6.3.3. DEFINITION DE K VOISIN PLUS PROCHE (K-NN) : 39

II.6.3.3.1. LE PRINCIPE DE LA CLASSIFICATION DU PLUS PROCHE VOISIN : 39

II.6.3.3.2. CALCUL DE SIMILARITE DANS L'ALGORITHME K-NN : 40

LA DISTANCE EUCLIDIENNE : 41

LA DISTANCE MANHATTAN : 41

LA DISTANCE HAMMING _____ 41

II.7. CONCLUSION: _____ 42

CHAPITRE III : APPLICATION ET RESULTATS _____ 43

III 1. INTRODUCTION _____ 44

III 2- DESCRIPTION DE LA BASE DE DONNEE FIGNER VIEN USM (FV-USM) _____ 45

III 3. LA METHODE LBP _____ 45

III 3-1QU'EST-CE QUE LE LBP? _____ 45

QU'EST-CE QUE LE MODELE BINAIRE LOCAL DANS LE TRAITEMENT D'IMAGE? _____ 46

III 3-2 COMMENT CALCULEZ-VOUS LE LBP? _____ 46

III 3-3 QU'EST-CE QUE L'ALGORITHME LBPH? _____ 46

III 3-4 QU'EST-CE QUE LBP CASCADE? _____ 46

III 3- 5 QUELLES SONT LES FONCTIONNALITES LBP? _____ 46

III 4. APPLICATION _____ 47

III 5 CONCLUSION _____ 51

CONCLUSION _____ 52

GENERALE : _____ 52

CONCLUSION GENERALE ET PERSPECTIVES : _____ 53

LISTE DES ABREVIATIONS _____ 5

FIGURE 1: EVOLUTION DU MARCHE INTERNATIONAL DE LA BIOMETRIE SELON LE RAPPORT DE L'IBG._____ 9

FIGURE 2 ILLUSTRE DES EXEMPLES DE MODALITES BIOMETRIQUES : _____ 12

FIGURE 3: DIFFERENTES MODALITES BIOMETRIQUES. _____ 13

FIGURE 4 : L'ADN [CHA09]._____ 15

FIGURE 5 : LA RECONNAISSANCE DE L'EMPREINTE DIGITALE_____ 16

FIGURE 6 : LA RECONNAISSANCE DE LA MAIN_____ 17

FIGURE.7: EMPREINTE DIGITALE_____ 19

FIGURE 8 RECONNAISSANCE FACIALE : _____ 19

FIGURE 9 UNITE D'AUTHENTIFICATION DE LA PAUME DE LA MAIN. _____ 20

FIGURE 10 RECONNAISSANCE DE L'IRIS_____ 20

FIGURE 11: PHOTOGRAPHIES DES DEUX RETINES D'UN INDIVIDU._____ 21

FIGURE 12: RECONNAISSANCE DE LA VOIX._____ 21

FIGURE 13: SCHEMA DU SYSTEME DE RECONNAISSANCE DES VEINES _____ 22

FIGURE 14: LIENS ENTRE TFR ET TFA._____ 24

FIGURE 15: SCHEMA SYNOPTIQUE DE SYSTEME D'IDENTIFICATION BIOMETRIQUE._____ 30

FIGURE 16: OPERATEUR LBP DE BASE._____ 32

FIGURE 17: EXEMPLE D'OPERATEUR LLBP._____ 35

FIGURE 18: ORGANIGRAMME DE L'ENSEMBLE DES ETAPES NECESSAIRE A LA CONSTRUCTION DU DESCRIPTEUR LPQ. _____ 37

FIGURE 19 IMAGE VEINE B) IMAGE LBP _____ 47

FIGURE 20 IMAGE VEINE B) IMAGE LBP _____ *47*

*FIGURE 21 : CALCULE DE SEUIL FAR ET FRR*_____ *49*

FIGURE 22 FRR EN FONCTION FAR _____ *49*

TABLEAU ; EER POUR D'AUTRE BASE DE DONNEES _____ *50*

Introduction Générale

Introduction générale

La sécurité est devenue aujourd'hui une préoccupation majeure au niveau international. L'identification des personnes constitue un élément clé dans les systèmes de sécurité. Cependant, les systèmes classiques de sécurité présentent des lacunes facilitant l'adaptation de l'identité d'une autre personne. La biométrie est une technologie émergente qui peut résoudre certaines anomalies inhérentes aux systèmes classiques de vérification de l'identité.

La biométrie est un terme dont on entend de plus en plus parler dans notre vie quotidienne. Cependant, la biométrie n'est pas vraiment récente. En effet, son apparition remonte au 19ème siècle. Dès lors, plusieurs modalités biométriques ont été étudiées pour la vérification d'identité. De nos jours, les modalités les plus employées comprennent le visage, la voix, l'empreinte, le réseau veineux, etc.

De nombreux systèmes biométriques sont envisagés dans les futurs systèmes en relation avec la sécurité. Particulièrement, un déploiement à large échelle des passeports et des cartes d'identités biométriques pour le contrôle de l'identité est prévu pour les années à venir au niveau mondial. Des délais sont alors imposés par les gouvernements pour la mise en place de ces systèmes. Dans notre pays, par exemple, il est prévu de finaliser généraliser le passeport biométrique vers 2025.

La maîtrise des systèmes biométriques devient alors une nécessité stratégique afin de pouvoir surmonter les défis relatifs aux applications pratiques. Le présent travail s'inscrit dans ce contexte. Nous nous intéressons à l'emploi de réseau veineux de la main et plus précisément les veines de doigt comme modalité biométrique pour l'authentification.

Les systèmes biométriques à base de réseau veineux de la main ou de doigt sont relativement nouveaux, ils ont attirés un intérêt croissant dans les deux communautés industries et recherche. Les vaisseaux sanguins sont cachés sous la peau, ils sont invisibles à l'œil humain et donc la biométrie par le réseau veineux est beaucoup plus difficile à copier par rapport à d'autres éléments d'identification biométriques. Le réseau veineux est unique, stable et a une forte immunité contre la contrefaçon, il peut devenir un bon potentiel biométrique qui offre des fonctionnalités sécurisées et fiables pour la vérification de l'identité d'une personne

Ce mémoire est organisé de la manière suivante:

Le premier chapitre présente les caractéristiques principales d'un système biométrique. Nous abordons les principes généraux de fonctionnement des systèmes biométriques, les différentes modalités biométriques, ainsi que l'évaluation des performances des systèmes biométriques.

Le second chapitre nous avons présenté les principaux modules de la biométrie, ainsi qu'une étude théorique détaillée des étapes de la reconnaissance doigt-veine : extraction de

paramètres, pré-traitement dans lequel nous avons utilisé trois méthodes différentes (LBP, LLBP, LPQ) parmi les méthodes connues et utilisées et enfin la classification utilisée par le k-nn.

Le chapitre 3 Dans ce chapitre nous avons réussie à appliquer la méthode LBP sur la base de donnée FV-USM. les résultats présentées montre une variation de résultat de l'EER d'une base à l'autre d'où les algorithmes de reconnaissance par veines de doigt doivent être choisi selon la valeur de L'ERR la plus petite.

Chapitre I :

La Biométrie

I-1 Introduction

Depuis quelques décennies l'explosion de l'informatique et des réseaux de communication a fait augmenter de manière significative le besoin d'identification des personnes. Jusqu'à présent les méthodes usuelles d'identification sont basées sur ce que l'on possède (carte d'identité, carte à puce, badge magnétique…) ou sur ce que l'on sait (mot de passe, code PIN), mais ces méthodes posent de gros problèmes de fiabilité (falsification de document, oubli de code, décryptage du mot de passe via des logiciels spécifiques). Depuis les récentes menaces qui pèsent sur de nombreux pays, une identification fiable des personnes est devenue un problème majeur pour des raisons de sécurité (contrôle aux frontières, accès aux lieux publics, transport…). Tous ces problèmes ont ainsi provoqués un développement accru des techniques biométriques d'identification [3], [4]. La Figure 1 montre les prévisions d'évolution du chiffre d'affaires du marché mondial de la biométrie dans les cinq prochaines années. Ces prévisions ont été publiées dans un rapport édité par l'IBG [5] (International Biometric Group).

I-2Définition :

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques: comportementales (exemple de la dynamique de frappe au clavier), physiques ou physiologiques (exemple de l'ADN)

Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance des personnes dans un grand nombre d'applications diverses.

Le mot biométrie est une traduction du mot anglais « biométrics » qui correspond en français à l'anthropométrie. Il désigne dans un sens très large l'étude quantitative des êtres vivants, mais dans le contexte de la reconnaissance d'individus il est défini par :

1. Selon le CLUSIF (Club de la Sécurité des systèmes d'Information Français) La biométrie est la science qui étudie à l'aide des mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé.

2. Selon la RAND (Public Safety and Justice), la biométrie est définie comme toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier son identité.

3. Pour reconnaître un individu, on extrait des paramètres de l'image photographiée (empreinte, face, iris...) puis on compare le gabarit obtenu avec tous les paramètres précédemment extraits et sauvegardés. Les techniques biométriques permettent la mesure et la reconnaissance de ce que l'on est, à la différence d'autres techniques de même finalités, mais permettant de mesurer ou vérifier ce que l'on possède (cadre, badge, document,…) ou ce que l'on sait (mot de passe, code pin,…).

Un système biométrique peut fonctionner en deux modes distincts : en mode de vérification, le système confirme ou nie une identité réclamée, alors qu'en mode d'identification, il détermine l'identité d'un individu.

I-3 Un bref historique de la biométrie :

Dans la Chine des dynasties, les documents étaient signés à l'aide d'empreintes digitales. Selon le rapport de l'explorateur Joao de Barros. Il a écrit que les marchands chinois relevaient les empreintes des mains et des pieds des enfants de jeune âge sur du papier en utilisant de l'encre afin de les distinguer les uns des autres.

C’est une des méthodes les plus anciennes de la biométrie en pratique et elle est toujours utilisée de nos jours. Dans les échanges commerciaux de Babylone, 3000 ans avant-J.-C., le même système était utilisé. En Amérique précolombienne, nombre d'architectes laissèrent également la trace de leurs mains colorées sur les parois de grottes aménagées. [Cha09].

Mais ce n'est qu'au début du XVIIIème siècle que le Docteur Henri Faulds développe l'utilisation de traces de doigt pour l'identification des personnes. A la même époque, l'anglais Francis Galton réalise des travaux de mesures de corps humains et crée une table de statistiques basée sur les tailles et les poids des personnes. Il met au point la méthode "Fingerprints" qui établit l’unicité et la permanence des figures cutanées.

En 1881, le médecin italien Cesare Lombroso tente de prouver que l'humain criminel présente des caractéristiques repérables et stables. Ainsi, le poids du cerveau des honnêtes gens pèserait entre 1475 et 1550 grammes tandis que celui des criminels serait d'à peu près 1455 grammes. Ces théories, non fondées scientifiquement, sont vite abandonnées. En 1885, Alphonse Bertillon ne laisse cependant pas de côté cette hypothèse, responsable de l'identité

judiciaire en France, il construit "le Bertillonage" qui s'appuie sur les mensurations des criminels. Le principe connaît un vif succès jusqu'au jour où une erreur judiciaire grave vient détruire le rêve de ségrégation. Après l'échec du Bertillonage, la police a commencé à utiliser la technique des empreintes digitales, qui a été développée par Richard Edward Henry de Scotland Yard, ressemblant essentiellement aux mêmes méthodes employées par les Chinois durant des années. Au XIXème siècle, la police criminelle fait considérablement avancer la recherche du fait de la multiplication des Analyses d'Indices Biologiques (ADN) [Mor 09]

Dans les trois dernières décennies, la biométrie a évolué d’une seule méthode simple (empreintes digitales) vers plus de dix méthodes discrètes. Les sociétés de biométrie comptent des centaines de nouvelles méthodes appliquées et continuent à améliorer leurs méthodes de sécurité tant que la technologie répond à leurs exigences. Les prix du hardware requis continuent à baisser rendant des systèmes faisables pour de faibles et moyens budgets. Cependant le développement de l'industrie, fait ainsi le souci du public concernant les libertés et l'intimité. Des lois et des règlements continuent à être rédigés et des normes commencent à être mises en place. Tandis qu'aucune autre technique biométrique n'a encore atteint le succès de l'utilisation de l'empreinte digitale, certaines commencent à être employées dans des secteurs d'activité judiciaire et commerciale.

Aujourd'hui, la biométrie est une technologie à part entière qui utilise des critères permanents, uniques et infalsifiables. Elle permet de garantir la sécurité des accès aux environnements physiques et numériques et révolutionne du même coup le ebusiness et le e-commerce.

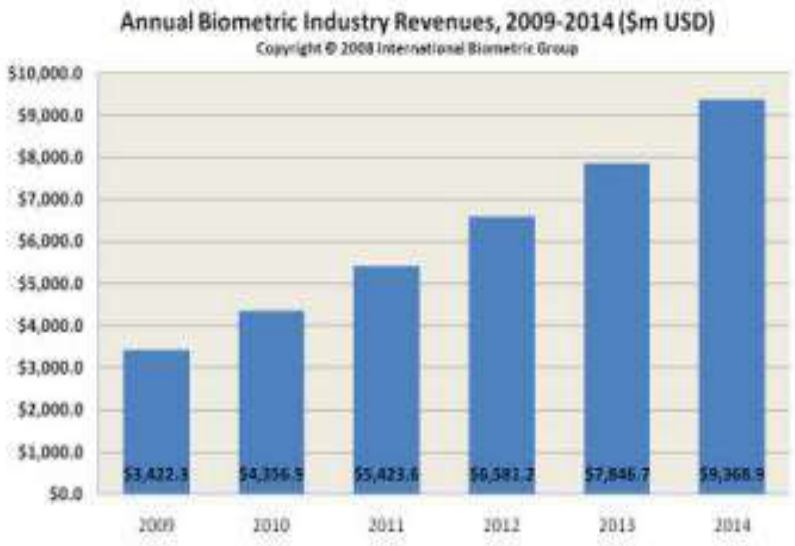


Figure 1: *Evolution du marché international de la biométrie selon le rapport de l'IBG.*

Le développement du marché de la biométrie repose principalement sur les nombreuses innovations technologiques réalisées durant les deux dernières décennies. Ce développement est également rendu possible par des évolutions notables dans les domaines social et juridique.

I-4 Qu'est ce que la biométrie ?

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

On distingue deux catégories de technologies biométriques : les mesures physiologiques, et les mesures comportementales.

Les mesures physiologiques peuvent être morphologiques ou biologiques. Ce sont surtout les empreintes digitales, la forme de la main, du doigt, le réseau veineux, l'œil (iris et rétine), ou encore la forme du visage, pour les analyses morphologiques.

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

Les mesures comportementales les plus répandues sont la reconnaissance vocale, la dynamique des signatures (vitesse de déplacement du stylo, accélérations, pression exercée, inclinaison), la dynamique de frappe au clavier d'un ordinateur, la façon d'utiliser des objets, la démarche, le bruit des pas, la gestuelle…

Les différentes techniques utilisées font l'objet de recherches régulières, de développements et bien entendu, d'améliorations constantes.

Toutefois, les différentes sortes de mesures n'ont pas le même niveau de fiabilité.

On estime que les mesures physiologiques ont l'avantage d'être plus stables dans la vie d'un individu. Par exemple, elles ne subissent pas autant les effets du stress, contrairement à l'identification par mesure comportementale.

La biométrie permet l'identification et l'authentification d'une personne à partir de données reconnaissables et vérifiables, qui lui sont propres et qui sont uniques.

L'identification consiste à déterminer l'identité d'une personne. Il s'agit de saisir une donnée biométrique de cette personne, en prenant par exemple une photo de son visage, en enregistrant sa voix, ou en captant l'image de son empreinte digitale. Ces données sont ensuite comparées aux données biométriques de plusieurs autres personnes qui figurent dans une base.

Dans ce mode, on pose une question simple : « qui êtes-vous ? ».

L'authentification, appelée également vérification, est le processus qui consiste à comparer les données caractéristiques provenant d'une personne, au modèle de référence biométrique de cette dernière (« template »), afin de déterminer la ressemblance. Le modèle de référence est préalablement enregistré et stocké dans une base de données, dans un équipement ou objet personnel sécurisé. On vérifie ici que la personne présentée est bien la personne qu'elle prétend être..

Dans ce mode, on pose la question : « êtes-vous bien Monsieur ou Madame X ? ».

I – 5 Les Systèmes biométriques et leurs modes de fonctionnements :

En général un système biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à un individu : physique ou comportementale. Il est basé sur l'analyse de données liées à l'individu qui peuvent être classées en trois grandes catégories : analyse basée sur la morphologie, analyse de traces biologiques, l'analyse comportementale.

Il peut être représenté par quatre modules principaux :

I – 5 -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.,)

I-5- 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. Généralement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classes,

I-5-3-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.

I-5-4-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).

I-6 Les différentes techniques biométriques

Les techniques biométriques peuvent être classées en deux catégories. La première repose sur les techniques d'analyse des comportements. Cette dernière concerne l'étude des actions répétitives et usuelles des personnes. Par exemples, l'analyse de la dynamique de la signature (vitesse de déplacement du stylo, accélérations, pression exercée, inclinaison) ou la façon d'utiliser un clavier d'ordinateur (la pression exercée, la vitesse de frappe, les suites de caractères répétitives).

En revanche, la seconde catégorie est basée sur les techniques d'analyse de la morphologie humaine. Ces dernières utilisent comme moyens d'analyse les empreintes digitales, la forme géométrique de la main, les traits du visage, le dessin du réseau veineux, etc. Ces éléments ont l'avantage d'être stables dans la vie d'un individu.

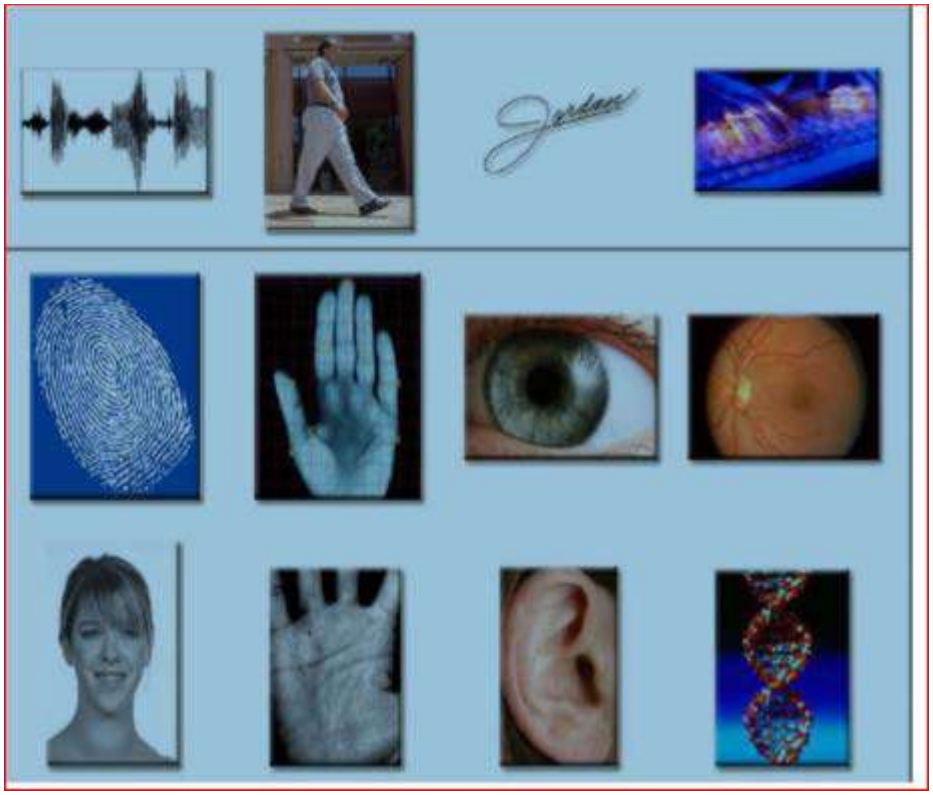


figure 2 illustre des exemples de modalités biométriques :

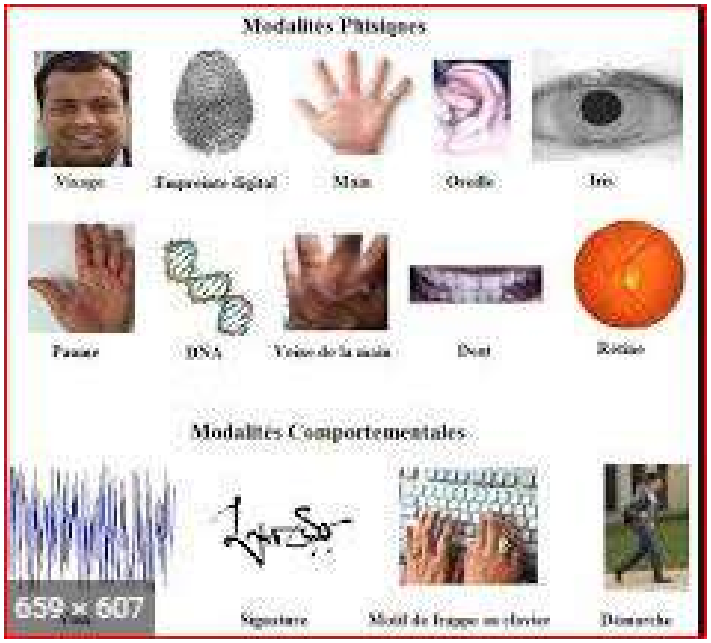


Figure 3: *Différentes modalités biométriques.*

Nous donnons maintenant un rapide aperçu des technologies biométriques les plus courantes.

On peut classer les techniques biométriques en trois catégories :

1- Celles basées sur l'analyse de traces biologiques : ce type de biométrie se fait à l'aide de l'ADN d'une personne, de son sang, ou de sa salive…

2- Celles basées sur l'analyse comportementale : se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, l'empreinte de sa voix, sa démarche et sa façon de taper sur le clavier.

3- Celles basées sur l'analyse morphologique : est basée sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance de la forme du visage, de la forme de la main, des empreintes digitales, de la rétine et de l'iris de l'œil.

Ces éléments ont l'avantage d'être stables dans la vie d'un individu et ne subissent pas autant les effets du stress par exemple, que l'on retrouve dans l'identification comportementale

Toutefois, dans un système biométrique pratique (à savoir, un système qui utilise la biométrie à des fins personnelles de reconnaissance), il y a un certain nombre d'autres questions qui devraient être considérées, y compris:

- La performance,

qui se réfère à la précision de la reconnaissance et de la vitesse possible ainsi que les ressources nécessaires pour obtenir cette précision de la reconnaissance et de la vitesse désirées. La performance se réfère également au fonctionnement et aux facteurs environnementaux qui influent sur la précision et la vitesse;

- L'Acceptabilité,

qui indique la mesure dans laquelle les gens sont prêts à accepter l'utilisation notamment d'un identifiant biométrique (caractéristique) dans leur vie quotidienne;

- Le contournement,

ce qui reflète la façon dont le système peut facilement être dupe en utilisant des méthodes frauduleuses.

Les technologies les plus fréquemment utilisées sont les suivantes :

I.7. Analyses biologiques :

I.7. 1. L'odeur corporelle :

Chaque personne dégage une odeur qui lui est particulière. Les systèmes biométriques qui exploitent cette technologie analysent les composantes chimiques contenues dans l'odeur pour ensuite les transformer en données comparatives.

I-7- 2. L'A.D.N. (Support matériel de l'hérédité):

Présent dans les cellules du corps, il est spécifique d'un individu à un autre et permet de l'identifier de manière certaine à partir d'un simple fragment de peau, d'une trace de sang ou d'une goutte de salive. Actuellement, le temps requis pour une analyse et le coût associé à celle-ci restreignent son utilisation dans des domaines autres que celui de l'identification judiciaire. Cependant, ce procédé biométrique fait l'objet de recherche intensive puisqu'il représente la technologie d'identification par excellence avec une marge d'erreur bien en dessous des autres moyens biométriques.

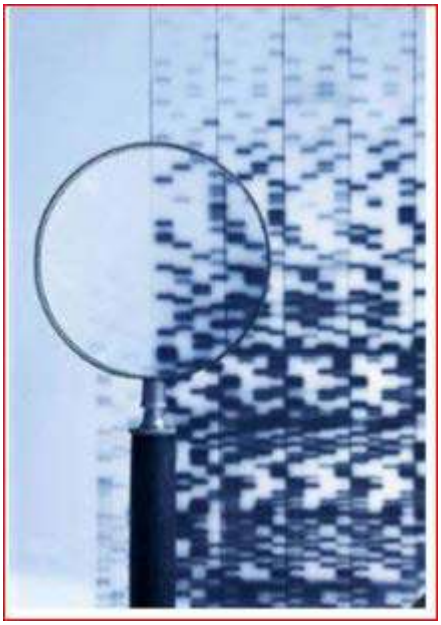


Figure 4 : L'ADN [Cha09].

I. 7-. 3. La reconnaissance de la thermographie faciale :

Une caméra infrarouge capte la chaleur émise par la peau. Contrairement à la reconnaissance faciale, on peut donc l'utiliser même dans l'obscurité ou de mauvaises conditions de visibilité. Mais les conditions de prise de vue peuvent conduire à des erreurs

I. 8.1. Analyses morphologiques :

I. 8.1. 1. Les empreintes digitales :

Un système biométrique utilisant l'empreinte digitale comme moyen d'identification ou de vérification ne procède pas de la même façon, ce n'est pas l'image de l'empreinte digitale qui sert de point de comparaison, mais l'ensemble des données biométriques qui est tiré à partir des minuties de l'empreinte digitale. Les minuties représentent les fins de crêtes, les bifurcations,

les lacs, les Lots et les points qui composent l'empreinte digitale. La combinaison des minuties est quasi infinie. données est faite par un capteur électronique de type optique, thermique, capacitif ou à ultrasons. Cette dernière est considérée comme la plus fiable, mais aussi la plus coûteuse

Le recours à l'empreinte digitale compte pour plus du tiers du marché des procédés bi nettement la solution préférée des entreprises œuvrant dans ce domaine. La force de ce procédé tient au fait que l'utilisatio l'empreinte digitale est plus facile à accepter qualité d'image de l'empreinte digitale peut varier selon que la peau du doigt est sale, trop humide ou trop sèche, huileuse ou affligée d'une coupure.



Figure 5 : La reconnaissance de l'empreinte digitale

I.8.2. 2. La Géométrie de la main :

La reconnaissance de la forme de la main est considérée comme l'ancêtre des des années soixante, Robert P. Miller déposa un brevet pour un appareil permettant de mesurer des caractér de la main et de les enregistrer pour comparaison ultérieure, l'utilisateur place sa main sur un gabarit. Le tout est éclairé par une lumière infrarouge et l'image est captée par une caméra digitale. Prés d'une centaine de caractéristiques sont extirpées de l'image et converties en données la phase d'identification. Ces données concernent la longueur, la largeur et la forme des articulations et la longueur inter articulations.



Figure 6 : La reconnaissance de la main

I-9 Reconnaissance de réseau veineux de la main

Cette technique récente semble prometteuse. Elle sonde par infrarouge le dessin du réseau veineux, soit du doigt, soit de la main. L'idée d'utiliser le réseau vasculaire sous-cutané de la partie supérieure de la main pour la biométrie remonte à 1991 avec les investigations de MacGregor et Welford [6]. Les premiers produits de cette technique viennent d'être mis sur le marché. Des espoirs peuvent être fondés sur cette technologie qui présente de nombreux avantages, car elle permet de prendre une empreinte sans contact et sans laisser de trace, elle est en outre très difficile à déjouer par un imposteur.

Depuis son introduction, la technologie de la biométrie par le réseau veineux a été élargie pour les systèmes basés sur les doigts et la paume de la main et a été adoptée en 2007 par l'ISO (International Standard Organization) où le stockage et la transmission des images biométriques vasculaires ont été normalisés.

Est-ce que le réseau veineux de la main est une bonne modalité biométrique ?

Comme dit précédemment, une modalité biométrique a besoin de cesqualités: l'universalité, l'unicité, la facilité de mesure et la permanence.

En ce qui concerne ces qualités, ce qui suit peut être conclu sur la reconnaissance biométrique par les veines de la main:

Universalité:

- Il est sûr que (sauf dans de cas rares) tout le monde a les mains et les vaisseaux sanguins de la main. Le réseau veineux peut donc être considéré comme universel.

La facilité de mesure:

- à l'aide des techniques de l'imagerie NIR (proche infrarouge) le modèle et les caractéristiques mesurées peuvent être extraites.

La permanence:

- Le développement du modèle de veine de la main s'arrête vers l'âge de 20 ans. Des petites modifications se produisent en raison du vieillissement des os. Considérant une personne en bonne santé et sans maladies vasculaires, il est prudent de supposer que les seuls changements survenant aux veines sont les rétrécissements et l'expansion du diamètre des veines en raison de la température, l'activité, etc. Par conséquent, il peut être conclu que le dessin des vaisseaux sanguins des mains est permanent [7].

Unicité :

- Aucune recherche n'a été faite avec l'intention de prouver l'unicité de la structure de veine de l'humain. Cependant, beaucoup de recherches existent qui sont indirectement liées à cette unicité. Eichmann et al [8] ont étudié le développement du système vasculaire humain,

Ils concluent que le développement du système vasculaire est complexe et tout à fait aléatoire. En raison d'une telle complexité et le caractère aléatoire, le réseau veineux est unique pour chaque individu.

Sur la base de cette discussion, le réseau vasculaire de la main peut être considéré comme un bon élément biométrique.

I-9-1 Reconnaissance des empreintes digitales :

La plus ancienne des technologies d'identification. Cette technique nécessite que l'utilisateur pose un doigt sur un capteur d'empreinte spécifique. Ensuite, un traitement est effectué sur l'image. Cette modalité est résistante jusqu'à un certain seuil, elle présente néanmoins quelques problèmes de fiabilité. En effet, les empreintes digitales d'un travailleur manuel le rendent réfractaire à toute identification. Elle se caractérise aussi par des problèmes de contraste (doigt propre et sec devient trop clair tandis qu'un doigt humide et recouvert d'un film gras devient foncé) d'autre part le dispositif de capture d'image.



Figure.7: *Empreinte digitale*

I-9-2 Reconnaissance faciale :

C'est la technologie qui monte. Elle s'appuie sur les caractéristiques principales du visage, l'éloignement des yeux, la taille de la bouche, etc., pour construire une carte du facies. L'identification d'un sujet fixe dans de bonnes conditions de luminosité peut être considérée comme mûre. 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.

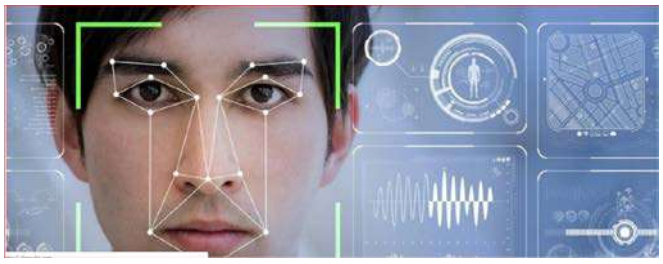


Figure 8 Reconnaissance faciale :

I-9-3 Reconnaissance de la main :

La reconnaissance de la main s'appuie sur une image en trois dimensions. Quelques traits caractéristiques sont gardés en mémoire : la taille et la largeur des doigts, l'espace entre les différentes parties de la main. Cette technologie présente l'avantage d'être moins capricieuse que la reconnaissance d'empreintes digitales : la saleté et les petites coupures n'empêcheront pas le système de fonctionner.

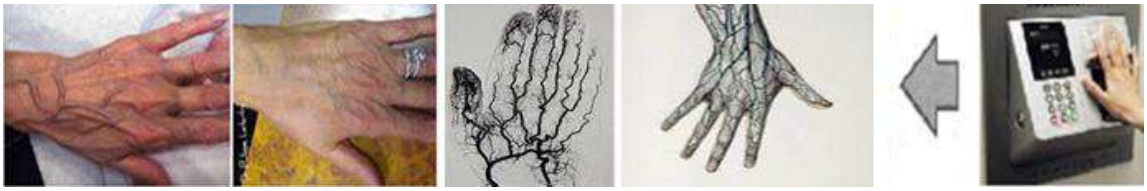


Figure 9 *Unité d'authentification de la paume de la main.*

I-9-4 Reconnaissance de l'iris :

C'est le fleuron de la biométrie, notre iris est unique et extrêmement complexe. Le taux d'erreur des produits disponibles sur le marché est proche de 0%. La fraude étant néanmoins possible en utilisant des lentilles. De plus, ce système est mal accepté psychologiquement par l'utilisateur à cause des problèmes d'hygiène et des contraintes de prise de vue (coopération du sujet). Les Contraintes d'éclairage risquent aussi de perturber la phase d'acquisition.

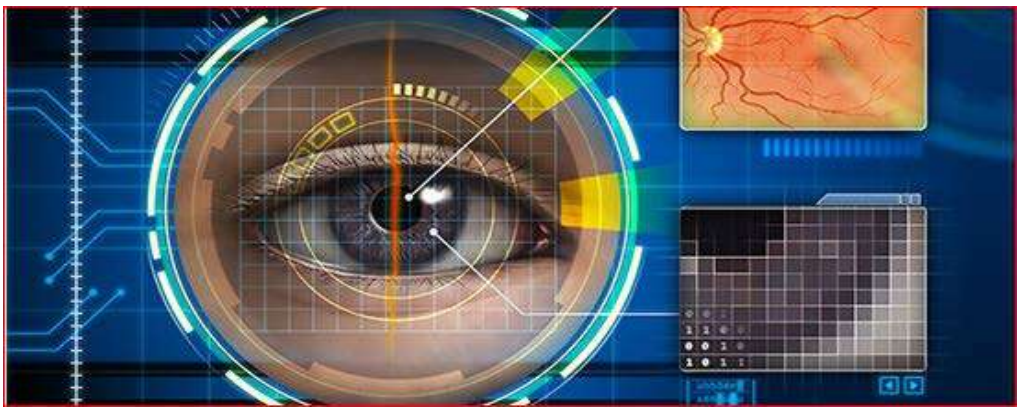


Figure 10 *Reconnaissance de l'iris*

I-9-5 Reconnaissance de la rétine:

Technologie très efficace mais assez contraignante pour les individus que l'on veut reconnaître : une lumière infrarouge de forte intensité scanne l'iris. Le procédé est non seulement invasif, mais il est de plus assez difficile à mettre en œuvre.

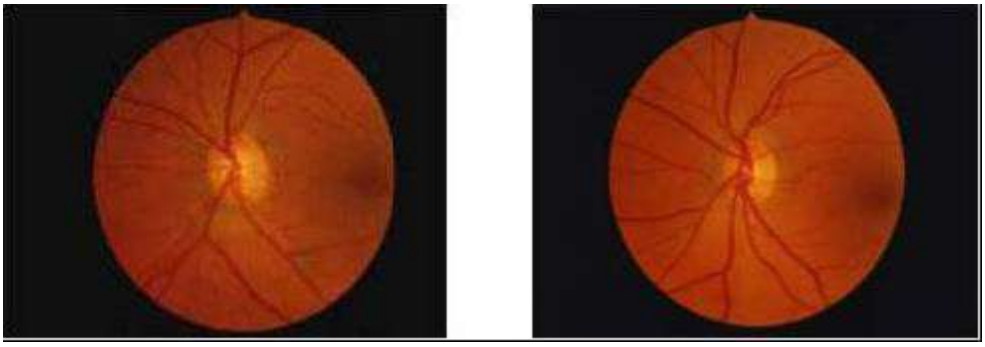


Figure 11: *Photographies des deux rétines d'un individu.*

I-9-6 Reconnaissance de la voix :

C'est la seule technologie qui permet à l'heure actuelle de reconnaitre un individu a distance. Cependant, la reconnaissance vocale reste empêtrée dans ses limites : il est très difficile d'enregistrer et de reproduire une voix. La reconnaissance vocale nécessite une excellente qualité audio. Il est inenvisageable d'installer cette technologie dans un lieu où les bruits de fond sont très présents. Dernier défaut : le faible niveau de différenciation entre deux voix rend la technique peu fiable.

Il existe d'autres méthodes biométriques telles que celles basées sur l'A.D.N, l'odeur corporelle, la forme de l'oreille, la forme des lèvres, le rythme de frappe sur un clavier, la démarche, etc. Il est important de noter qu'il n'existe aucune caractéristique biométrique idéale. A chaque application correspond une ou plusieurs mesures biométriques appropriées.



Figure 12: *Reconnaissance de la voix.*

I-10 Structure d'un système complet de reconnaissance de réseau veineux de la main

Les systèmes de reconnaissance de formes peuvent exister sous des formes infinies, traiter les problèmes dans de nombreux domaines et utilisant des méthodes différentes pour atteindre leurs objectifs. Malgré cela, la plupart, sinon la totalité, des systèmes tendent à suivre la même structure générale. La structure d'un système de reconnaissance de veine de la main peut se résumer par le diagramme général montré dans la figure 13

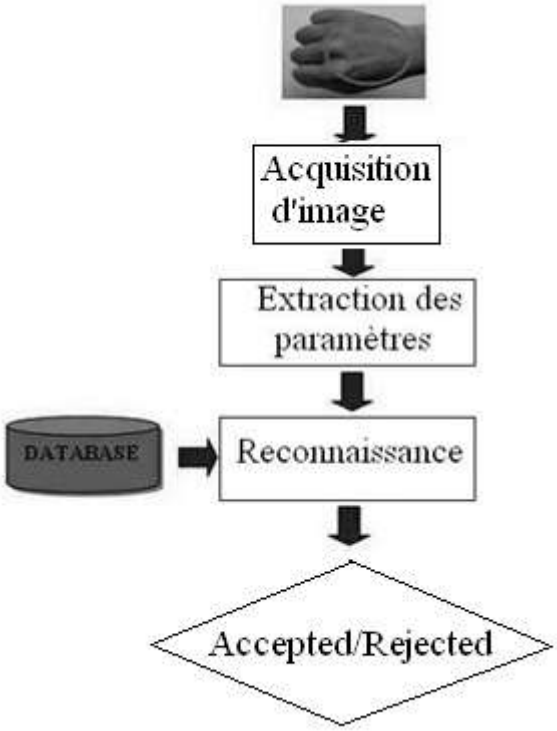


Figure 13: *schéma du système de Reconnaissance des veines*

Le système de reconnaissance des veines de la main de ce mémoire est conçu en fonction de cette structure générale. Les paragraphes suivants expliquent le but de chaque bloc.

I-10-1 L'Acquisition d'image et prétraitement

Avec le développement de l'informatique et de la microélectronique, de nouveaux moyens d'acquisition ont fait leur apparition, permettant ainsi d'accélérer la chaîne de traitement en l'automatisant (un capteur dédié fournit directement une image numérique).Une installation permet de normaliser les images et limiter les mouvements et la rotation de la main. Après avoir acquis l'image, le prétraitement est appliqué. Le but de cette étape est d'améliorer la qualité de l'image de telle sorte que le réseau veineux puisse être plus facilement détecté lors de la segmentation.

I-10-2 La segmentation

Une fois que le bruit a été réduit et le contraste amélioré, la segmentation permet de séparer le réseau veineux de l'arrière plan (la main). En effet, le dessin de veines est situé et isolé du reste de l'image, ainsi il est binarisé. La segmentation est l'étape la plus essentielle dans le processus de reconnaissance entier. Si les veines ne sont pas correctement détectées, le risque d'erreur augmente considérablement. La méthode choisie joue un rôle important dans la performance globale du système.

L'image de sortie de l'étape de segmentation est une image binaire avec quelques informations indésirables telles que le bruit, les ombres et les petites veines. Par conséquent, elle n'est pas toujours une vraie représentation de la structure de veine réelle. L'application des opérateurs morphologiques (ouverture, fermeture, squelettisation …) permet de nettoyer l'image et d'extraire un squelette de dessin de veines.

I-10-3 L'extraction des paramètres et la reconnaissance

Cette étape vise à extraire les paramètres de la structure de veines à partir d'une image, ensuite ils seront enregistrés dans une base de données pour être utilisés dans la comparaison.

Une fois les paramètres extraits, ils sont comparés avec ceux de la base de données pour prendre une décision, l'image est identifiée si les caractéristiques d'entrée sont semblables à celles enregistrées dans la base de données, sinon elle est rejetée.

I-10-4 Les problèmes posés par l'utilisation de la biométrie

Dans les systèmes biométriques la phase finale d'appariement estime le degré de similitude (taux d'appariement) entre deux signatures et le compare à un seuil fixé à l'avance, ainsi le résultat n'est jamais fiable à 100% mais s'en approche selon le réglage du seuil. L'évaluation des performances de ces systèmes fait apparaître deux types d'erreur [9]:

- l

e Taux de Faux Rejets (TFR) correspondant au pourcentage de personnes rejetées par erreur.

- le Taux de Fausses Acceptations (TFA) correspondant au pourcentage de personnes qui ont été acceptées et qui n'auraient pas du l'être.

La relation liant TFA et TFR est illustrée sur la Figure 14. On peut voir que plus le TFR est faible, plus le TFA est élevé et inversement. Ces deux éléments dépendent du réglage du seuil qui est le résultat d'un compromis selon le choix de l'application. Pour des applications de haute sécurité (accès au coffre fort de la banque centrale par exemple),

on cherchera à limiter au maximum la possibilité d'intrusion, ce qui se traduit par un TFA faible. Au contraire, dans le cadre d'applications médicales, on ne pourra pas se permettre de rejeter une personne par erreur ce qui implique un TFR le plus faible possible.

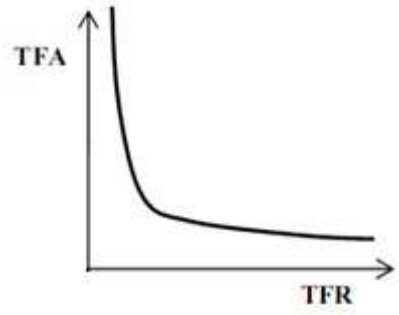


Figure 14: *Liens entre TFR et TFA.*

Les systèmes biométriques posent aussi des problèmes de sécurité car il n'est jamais vérifié que les données biométriques en entrée proviennent de leur réel possesseur. En effet les moyens de flouer un tel système existent [10], et de plus les caractères biométriques ne sont pas secrets. Il est relativement facile de se procurer une photo du visage, une empreinte digitale ou un enregistrement audio d'une personne. Le problème vient de l'absence de vérification que la donnée entrée provient bien d'un être vivant.

I-11 avantages de la biométrie pour la sécurité

I-11-1 Identification et authentification :

I-11-1-1 vitesse et précision

L'utilisation de mots de passe et de codes pour accéder de manière sécurisée à un site physique ou virtuel est assez simple, mais générique. Toute personne munie d'une carte ou d'un laissez-passer peut accéder au site ainsi protégé. En revanche, la technologie de sécurité biométrique désigne les mots de passe biologiques qui ne peuvent être falsifiés. En d'autres termes, l'identification et l'authentification d'un individu donné sont fiables. La reconnaissance d'iris ou faciale est de plus en plus souvent intégrée aux processus de sécurité, du fait de la rapidité et de la simplicité de la détection.

I-11-1-2 Un grand sens des responsabilités

Avec la biométrie, l'entreprise dispose d'informations exactes sur les entrées et les sorties – signe qu'elle prend ses responsabilités très au sérieux. En cas d'incident malheureux, l'entreprise peut s'appuyer sur des preuves plus fiables, car étayées par des données. Les données sont également faciles à configurer, à analyser et à transmettre en cas de besoin.

I-11-1-3 Efficacité maximale

Chaque entreprise exige de ses systèmes de sécurité une efficacité à toute épreuve. Les systèmes de contrôle biométrique renforcent non seulement la sécurité, mais ils facilitent et améliorent également l'efficacité de la gestion de fonctions clés comme le suivi de présence pour l'établissement des fiches de paye. Ce système est même pratique pour les employés qui n'ont plus besoin d'avoir leur badge ou carte d'accès sur eux en permanence.

I-11-1-4 Mot d'ordre : l'aspect pratique

L'un des principaux avantages d'un système de contrôle biométrique tient à sa commodité. Les mots de passe n'ont pas besoin d'être réinitialisés. Une fois le test biométrique activé, la reconnaissance des empreintes digitales, de l'iris et du visage peut s'effectuer — et les employés vaquer à leurs occupations. On peut même enregistrer les données et les vérifier selon les besoins. Pratique.

I-11-1-5 Évolutif pour accompagner la croissance

Au fur et à mesure que les entreprises grandissent, la sécurité doit impérativement évoluer avec elles. L'évolutivité constitue d'ailleurs l'un des principaux avantages des contrôles biométriques. La flexibilité de ces systèmes leur permet d'accepter facilement des données supplémentaires sur les employés. En clair, la sécurité grandit avec l'entreprise.

I-11-1-6 Sécurité et rentabilité

Une fois le système de contrôle biométrique intégré, il n'y a plus besoin d'investissements infrastructurels supplémentaires. Les coûts d'investissement initiaux et récurrents chutent par conséquent de manière très nette. Ces systèmes contribuent en outre à prévenir les pertes dues à la fraude et aux entrées illégales. À lui seul, cet avantage permet d'économiser de l'argent et d'accroître la rentabilité.

I-11-1-7 Utilisation simple et ergonomique

La gestion, l'ajustement, et même l'analyse des contrôles biométriques se distinguent par leur ergonomie — avec des résultats technologiques et précis qui ne requièrent qu'un minimum d'intervention. La capture de nouvelles données et l'analyse des journaux s'effectuent rapidement. Une fois le tableau des entrées et des sorties créé, l'analyse et la gestion des données deviennent un jeu d'enfant.

I-12 Conclusion

Dans ce chapitre nous avons décrit personnes, leurs architectures et leurs différentes applications, ainsi des performances des systèmes biométriques et et les inconvénients de chacune. Nous avons plusieurs facteurs et qu'elles varient d'un système a un autre

La biométrie s'impose rapidement comme une pièce maîtresse de l'infrastructure de sécurité et de l'authentification multi-facteurs, avec au programme : contrôles simples et rapides, journaux d'audit et analyses. Ces systèmes revêtent une importance cruciale à l'heure où le secteur continue à évoluer et à se complexifier. On peut d'ailleurs s'attendre à ce que le phénomène prenne de l'ampleur dans les prochaines années.

Curieux d'en savoir plus sur les subtilités de ces infrastructures de sécurité complexes et l'authentification multi-facteurs ?

N'hésitez pas à parcourir les liens ci-après pour en savoir plus.

Chapitre II :

Description d'unsystème d'identification

II.1. Introduction :

Nous devons donc étudier les caractéristiques physiologiques et comportementales de l'individu. Parmi ces études, nous abordons l'identification des personnes par les veines de doigt, source de validation correcte en tant que méthode biologique permettant d'analyser les structures de la veine avec le doigt.

Dans ce chapitre, nous présentons les différentes étapes qui constituent un système d’identification y compris le prétraitement, l'extraction de caractéristiques et la classification.

II.2. Système d'identification :

Le système se compose de quatre étapes : l'acquisition, prétraitement, l'extraction des caractéristiques, et la classification.

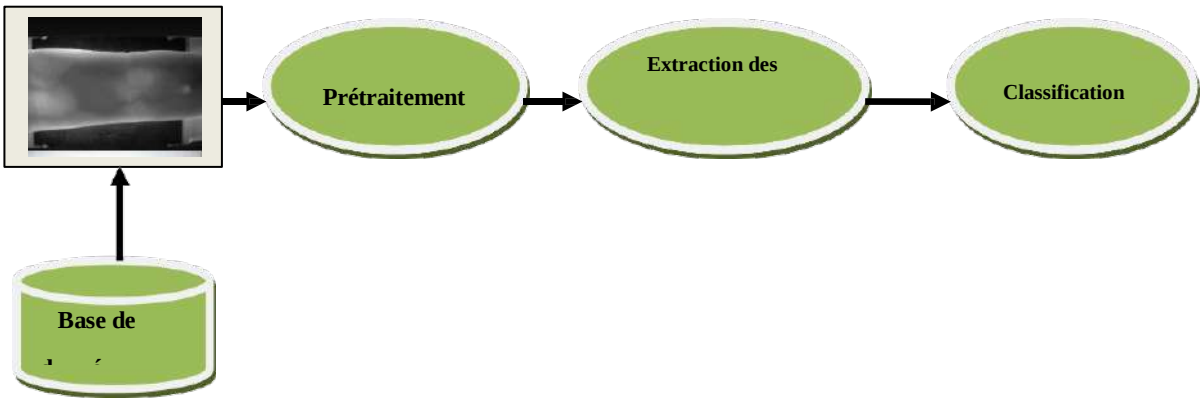


Figure 15: Schéma synoptique de système d'identification biométrique.

II.3. Biométrie des veines du doigt, principe ?

Acquisition des données : Cette phase collecte les données biométriques des personnes clients. Plusieurs processus industriels peuvent être utilisés pour l'acquisition telle qu'un appareil photo, un lecteur d'empreintes digitales, etc. [17]

Le lecteur biométrique est composé d'un système qui émet une lumière infrarouge et d'un capteur récupérant une image reflétée :

1. Le lecteur biométrique émet une lumière infrarouge.
2. Le sang chargé d'oxygène a pour caractéristique d'absorber les ondes proches de l'infrarouge.
3. Le capteur biométrique récupère une image reflétée représentant la cartographie des veines des doigts.
4. La puissance du lecteur biométrique consiste à effectuer des mesures entre les différentes intersections des veines.
5. A partir des mesures, il recherche l'identité de la personne dans sa base de données locale.
6. En fonction des autorisations d'accès horaires préprogrammés, le lecteur active l'ouverture de l'accès. [18]

II.4. Reconnaissance des veines des doigts (FVR) :

La reconnaissance des veines des doigts est une méthode d'authentification biométrique qui utilise des techniques de reconnaissance des motifs basées sur des images de motifs de veines des doigts sous la surface de la peau. La reconnaissance des doigts dans les veines est l'une des nombreuses formes de biométrie utilisées pour identifier les individus et vérifier leur identité. [19]

II.4.1. Prétraitement :

Avant l'étape d'extraction des caractéristiques, les données du dispositif de capteur d'image doivent être prétraitées. Le prétraitement d'images a pour objectif de fournir une image de région d'intérêt (ROI) robuste pour l'extraction de caractéristiques. Les bonnes performances d'une image de la veine du doigt dépendent de la qualité de l'image de la veine du doigt. [20]

II.4.1.1. ROI Extraction :

Cette étape la plus importante est l'extraction du retour sur investissement. Dans les images de la veine du doigt, 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. [21]

II.4.2. 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. Par exemple, dans un système biométrique à empreintes digitales [22], la position et l'orientation des points de minutie dans une image d'empreinte digitale constituent l'élément clé qui doit être différent de celui d'une autre personne. Une technique d'extraction efficace des caractéristiques est une étape qui améliore la précision de la reconnaissance des veines des doigts. Sur cette base, nous disposons des méthodes d'extraction de paramètres:

II.4.2.1. 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. L'opérateur LBP de base fonctionne pour 3 × 3 pixels est décrite par le diagramme suivant:[23]

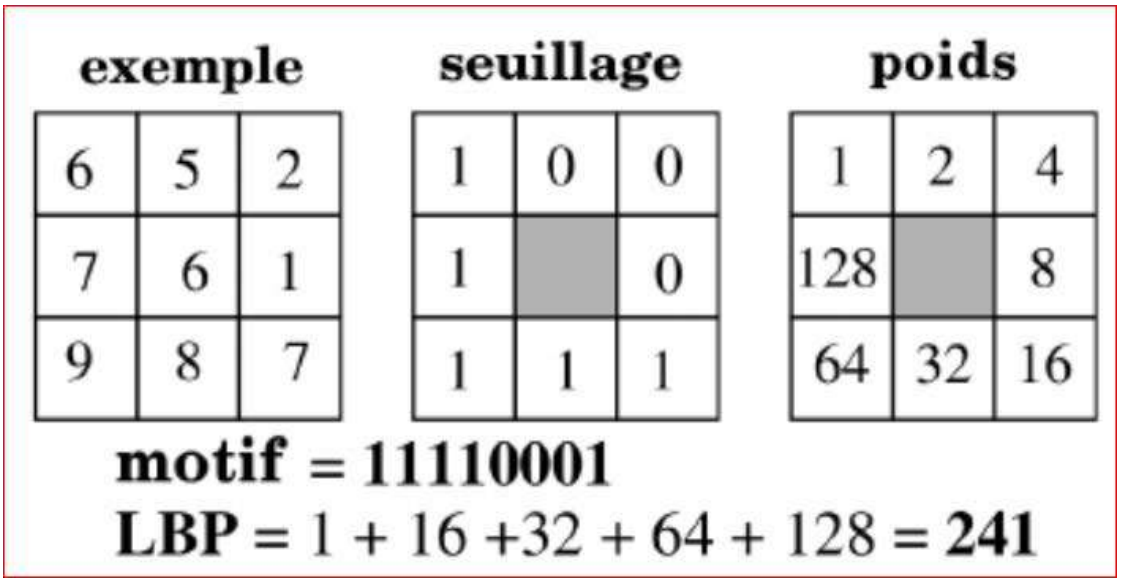


Figure 16: *Opérateur LBP de base.*

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:

Illustration du calcul des caractéristiques LBP pour un voisinage de rayon R = 1 . Les niveaux de gris des 8 voisins du pixel central sont seuillés par la valeur du ndg du pixel central. La valeur de LBP est ensuite calculée en tenant compte des poids de chaque pixel du voisinage selon l'équation

$$LBP(x_c, y_c) = \sum_{n=0}^{7} S(i_n - i_c)\, 2^n$$

$$S(x) = \begin{cases} 1 \; if \; (x \geq 0) \\ 0 \; if \; (x < 0) \end{cases}$$

Ici xc et yc montrent la position du pixel central, in et ic sont des valeurs d'échelle de gris des pixels environnants et du pixel central respectivement.

➢ Avantage:

- Tolérance vis-à-vis des changements d'illumination et simplicité.

➢ Inconvénient:

- l'opérateur produit un Histogramme assez long et n'est pas trop robuste sur l'image plane. [24]

II.4.2.2. Local line binary pattern (LLBP):

Le modèle binaire de ligne local (LLBP) est dérivé du modèle binaire local (LBP) et révèle la structure spatiale locale d'une image par le processus de seuillage. La présentation de la texture, désignée par un nombre décimal, est lancée à partir de la fenêtre locale avec un poids binaire. LLBP a un coût de calcul très faible. L'idée fondamentale de LLBP et de LBP est la même mais les principales différences sont les suivantes:

1. La région LLBP est une ligne droite avec un pixel de longueur N, la région LBP ayant une forme carrée.

2. La distribution de poids binaire est démarrée à partir des pixels adjacents gauche et droit du pixel central, alors que dans LLBP, elle est démarrée à partir des pixels adjacents supérieur et inférieur du pixel central. .

L'algorithme LLBP obtient le code binaire de la ligne avec les directions horizontale et verticale séparément et aussi sa magnitude, qui différencie les changements d'intensité d'image tels que les coins et les bords. [25]

LLBPh, LLBPv et LLBPm sont respectivement LLBP sur la direction horizontale, la direction verticale et sa magnitude. N est la longueur de la ligne en pixel, hn est le pixel avec la ligne horizontale et vn est le pixel avec la ligne verticale. c = N / 2 est la position du pixel central, hc sur la ligne horizontale et vc sur la ligne verticale. [26]

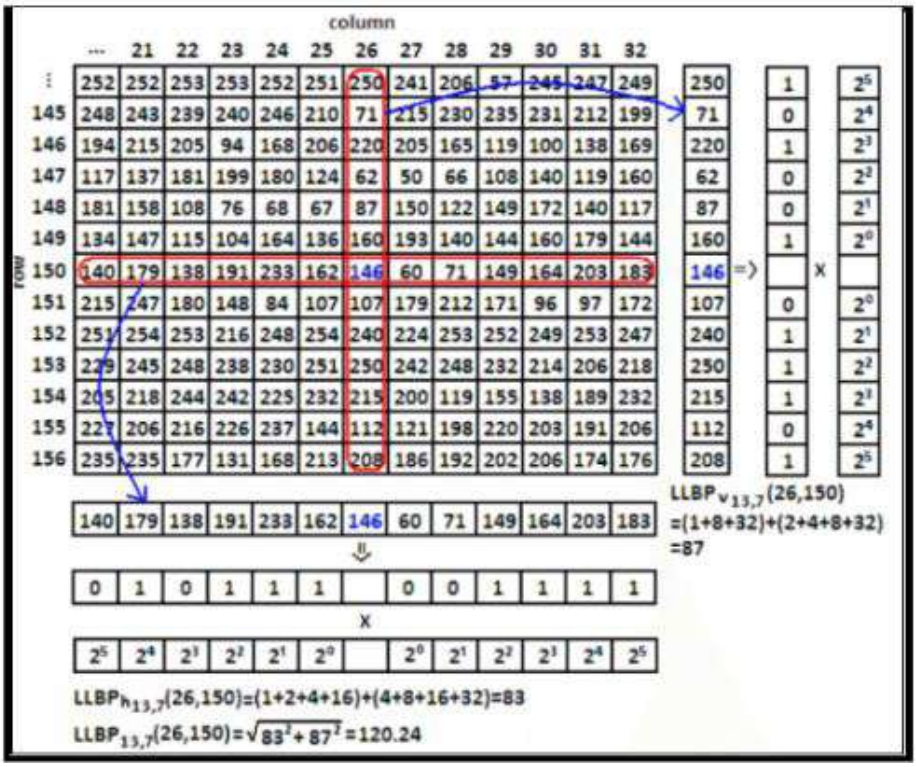


Figure 17: Exemple d'opérateur LLBP.

$$LLBP_{h,N,c}(x,y) = \sum_{n=1}^{c-1} s(h_n - h_c).2^{c-n-1} + \sum_{n=c+1}^{N} s(h_n - h_c).2^{c-n-1}$$

$$LLBP_{v,N,c}(x,y) = \sum_{n=1}^{c-1} s(v_n - v_c).2^{c-n-1} + \sum_{n=c+1}^{N} s(v_n - v_c).2^{c-n-1}$$

$$LLBP_m = \sqrt{LLPB_h^2 + LLPB_V^2}$$

II.4.2.3. Quantification de la phase locale (LPQ):

La quantification de la phase locale (en anglais Local Phase Quantization (LPQ)) est un algorithme très utilisé pour l'extraction de caractéristiques dans plusieurs technologies biométrique telle que le visage, l'empreinte palmaire et l'iris. Cette méthode a été introduite pour la première fois par Ojansivu et al, ils divisent l'image en petites zones égales NN, dans chaque zone, les informations locales et utiles de l'image sont extraites. LPQ extrait l'information par l'utilisation de la transformée en Fourier discrète de chaque pixel x, illustré dans l'équation (2.5).

$$F_u(x) = \sum_{m \in Nx} h(m-x) f(m) e^{-2j\pi\theta^T m} = E_u^T f_x$$

Où Eu, de taille = 1 × M^2 est un vecteur de base de 2DWFT avec la fréquence u, et fx,

aille =M^2 × N, est un vecteur contenant les valeurs des pixels d'image dans Nx à chaque position x. La fonction fenêtre, h (x) est une fonction rectangulaire. [16]

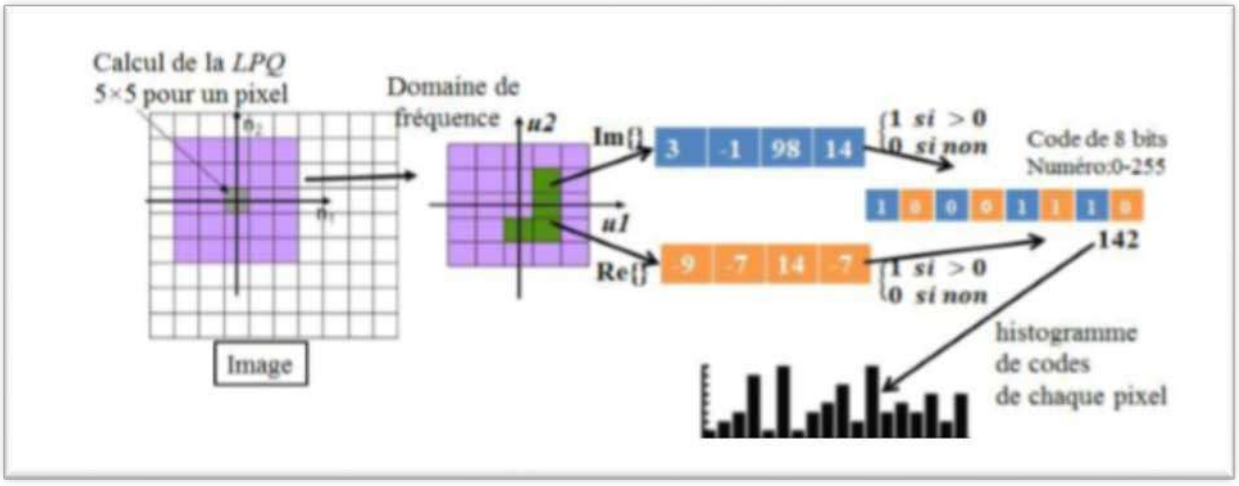


Figure 18: Organigramme de l'ensemble des étapes nécessaire à la construction du descripteur LPQ.

II.4.3. 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-5 Apprentissage

C'est l'étape où nous faisons apprendre les individus au système, elle consiste à mémoriser les paramètres, après l'extraction des caractéristiques, dans une base de données bien ordonnées pour faciliter la phase de reconnaissance et la prise d'une décision, elle est en quelque sorte la mémoire du système. Nous distinguons deux types d'apprentissages : apprentissage supervisé, et apprentissage non supervisé.

II-5.1. Apprentissage supervisé

L'apprentissage supervisé a pour but d'apprendre de l'exemple. Il faut fournir au préalable une liste d'objets avec leurs étiquettes de classe (appelée ensemble d'apprentissage) afin que le système soit capable d'expliquer et ensuite de prédire l'appartenance d'un nouvel objet à une classe connue. Beaucoup d'algorithmes d'apprentissage supervisé sont utilisés pour faire de la reconnaissance d'objets telle que la méthode la plus classique est certainement l'algorithme des « KPlus Proches Voisins (KPPV)

II-5.2. Apprentissage non-supervisé

L'apprentissage non-supervisé est seulement composé d'exemples, sans aucune étiquette de classe. C'est l'algorithme de trouver des dépendances des structures entre les différents exemples. Le « clustering » ou partitionnement de données regroupe un ensemble de méthodes d'apprentissage non-supervisé, comme l'algorithme des K-means ou l'Isodata. Les classes (ou « clusters » en anglais) sont créées par l'algorithme qui regroupe dans une même classe des objets ayant des caractéristiques communes entre elles et différentes avec les objets n'appartenant pas aux mêmes classes. Prenons un exemple de classification par les K-means. L'algorithme est initialisé aléatoirement avec un certain nombre de clusters pour lesquels un point moyen, appelé centroïde, est évalué.

A chaque itération, la distance entre chaque exemple aux différents centroïdes est calculée; chaque exemple est alors associé au cluster dont la distance au centroïde est la plus proche. Puis les centroïdes sont réévalués. L'algorithme se termine lorsqu'il n'y a plus aucun changement

II-6.3.1. 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 classifieurs linéaires. Ils ont été développés dans les années 1990 par ValdimirVapnik 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.

II-6.3.2. Arbre de décision (ADD) :

L'arbre de décision (ADD) est un outil utilisé dans différents domaines : sécurité, fouille de données, médecine, etc. Sa popularité est due à sa lisibilité, sa rapidité d'exécution, le peu d'hypothèses nécessaires qu'il propose, et son interopérabilité que souhaiterait avoir tous les médecins a priori, expliquent sa popularité actuelle. L'apprentissage par ADD se situe dans le cadre de l'apprentissage supervisé, où la classe de chaque objet dans la base est donnée. [29]

Dans ce travail on utilise le classificateur K-NN :

II.6.3.3. Définition de K voisin plus proche (K-NN) :

La méthode des K plus proches voisins (KNN) a pour but de classifier des points cibles (classe méconnue) 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. [30]

II.6.3.3.1. Le principe de la classification du plus proche voisin :

Consiste à trouver un nombre prédéfini, c'est-à-dire le «k» - échantillons d'entraînement, qui se rapproche le plus de la distance par rapport à un nouvel échantillon, qui doit être classé. L'étiquette du nouvel échantillon sera définie à partir de ces voisins. Les classificateurs k-plus proches voisins ont une constante définie par l'utilisateur fixe pour le nombre de voisins à déterminer.

Il existe également des algorithmes d'apprentissage des voisins basés sur le rayon, qui ont un nombre variable de voisins basé sur la densité locale de points, tous les échantillons situés à l'intérieur d'un rayon fixe. La distance peut, en général, être n'importe quelle mesure métrique: la distance euclidienne standard est le choix le plus courant. Les méthodes basées sur les voisins sont connues sous le nom de méthodes d'apprentissage automatique non généralisantes, car elles "se souviennent" simplement de toutes ses données d'apprentissage.

L'algorithme k-NN est l'un des plus simples de tous les algorithmes d'apprentissage automatique, mais malgré sa simplicité, il a rencontré beaucoup de succès dans un grand nombre de problèmes de classification et de régression, tels que la reconnaissance de caractères ou l'analyse d'images. [31]

II.6.3.3.2. Calcul de similarité dans l'algorithme K-NN :

Comme on vient de le voir dans notre écriture algorithme, K-NN a besoin d'une fonction de calcul de distance entre deux observations. Plus deux points sont proches l'un de l'autre, plus ils sont similaires et vice versa.

Il existe plusieurs fonctions de calcul de distance, notamment, la distance euclidienne, la distance de Manhattan, la distance de Minkowski, celle de Jaccard, la distance de Hamming…etc. On choisit la fonction de distance en fonction des types de données qu'on manipule. Ainsi pour les données quantitatives (exemple : poids, salaires, taille, montant de panier électronique etc…) et du même type, la distance euclidienne est un bon candidat. Quant à la distance de Manhattan, elle est une bonne mesure à utiliser quand les données (input variables) ne sont pas du même type (exemple : âge, sexe, longueur, poids etc…).

Il est inutile de coder, soi-même ces distances, généralement, les librairies de Machine Learning comme Scikit Learn, effectue ces calculs en interne. Il suffit juste d'indiquer la mesure de distance qu'on souhaite utiliser. Pour les curieux, voici les définitions mathématiques des distances qu'on vient d'évoquer.

La distance euclidienne :

distance qui calcule la racine carrée de la somme des différences carrées entre les coordonnées de deux points :

$$D_e(x,y) = \sqrt{\sum_{j=1}^{n}(x_j - y_j)^2}$$

La distance Manhattan :

la distance de Manhattan: calcule la somme des valeurs absolues des différences entre les coordonnées de deux points :

$$D_m(x,y) = \sum_{i=1}^{k} |x_i - y_i|$$

La distance Hamming

$$D_h(x,y) = \sum_{i=1}^{K} |x_i - y_i|$$

Avec

$$x = y \Rightarrow D = 0$$
$$x \neq y \Rightarrow D = 1$$

Notez bien qu'il existe d'autres distances selon le cas d'utilisation de l'algorithme, mais la distance euclidienne reste la plus utilisée. [32]

II.7. Conclusion:

Dans ce chapitre, nous avons présenté la méthode de reconnaissance de la veine du doigt et de ses étapes fiables, Lors de l'étape de d’extraction, nous avons utilisé trois algorithmes : LBP et LLBP, LPQ pour établir la différence entre eux. En ce qui concerne la classification, nous avons détaillé le -classificateur k-nn.

Chapitre III :

Application et résultats

III 1. Introduction

Le présent chapitre est consacré à la présentation de quelques tests effectués et les résultats obtenus. Nous présentons d'abord la base de données utilisée. Les différents algorithmes de notre système ainsi que le déroulement de tous les tests sont traités sous Matlab7.4. Matlab qui est un environnement de calcul scientifique et de visualisation de données très puissant et largement utilisé dans la valorisation des travaux de recherche. Sa facilité d'apprentissage et d'utilisation en ont fait un standard adapté pour les divers problèmes de l'ingénierie. Ceci est grâce à ses nombreux avantages, comme ses nombreuses fonctions prédéfinies prêtes à l'emploi, sa programmation simplifiée, sa rapidité de calcul, sa fiabilité, sa robustesse, etc.

III 2- Description de la Base de donnée Figner Vien USM (FV-USM)

Puisqu'il existe un nombre limité de bases de données accessibles au public pour la reconnaissance des veines des doigts, nous avons développé une base de données d'images infrarouges des doigts. La base de données comprend les informations sur la veine des doigts et également la géométrie des doigts. Il peut être utilisé pour vérifier les systèmes biométriques unimodaux (veine des doigts et géométrie des doigts) ou biométriques bimodaux (fusion des veines et géométrie). Complète avec le ROI (région d'intérêt) extrait pour la reconnaissance des veines des doigts, cette base de données est mise à disposition sur le Web afin d'aider d'autres chercheurs dans les domaines connexes à tester et évaluer leurs algorithmes sur la base d'une base de données de référence standard. Notre base de données

Les images de la base de données ont été recueillies auprès de 123 volontaires, dont 83 hommes et 40 femmes, qui étaient membres du personnel et étudiants de l'Universiti Sains Malaysia. L'âge du sujet variait de 20 à 52 ans. Chaque sujet a fourni quatre doigts: index gauche, milieu gauche, index droit et majeur droit, soit un total de 492 classes de doigts obtenues. Les images des doigts capturées ont fourni deux caractéristiques importantes: la géométrie et le motif de la veine. Chaque doigt a été capturé six fois en une seule séance et chaque individu a participé à deux séances, séparées par plus de deux semaines. Lors de la première session, un total de 2952 (123 x 4 x 6) images ont été collectées. Par conséquent, à partir de deux séances, nous avons obtenu un total de 5904 images de 492 classes de doigts. La résolution spatiale et la profondeur des images des doigts capturées étaient de 640 x 480 et 256 niveaux de gris, respectivement. Nous fournissons également les images ROI extraites pour la reconnaissance des veines des doigts en utilisant notre algorithme proposé décrit dans [1]

III 3. La méthode LBP

III 3-1Qu'est-ce que le LBP?

Les modèles binaires locaux (LBP) sont un type de descripteur visuel utilisé pour la classification en vision par ordinateur. Le LBP est le cas particulier du modèle Texture Spectrum proposé en 1990. ... Une comparaison de plusieurs améliorations du LBP original dans le domaine de la soustraction de fond a été faite en 2015

Qu'est-ce que le modèle binaire local dans le traitement d'image?

Le modèle binaire local (LBP) est un opérateur de texture simple mais très efficace qui étiquette les pixels d'une image en seuillant le voisinage de chaque pixel et considère le résultat comme un nombre binaire. ... En utilisant le LBP combiné avec des histogrammes, nous pouvons représenter les images de visage avec un simple vecteur de données

III 3-2 Comment calculez-vous le LBP?

Pour calculer le LBP, le code LBP pour chaque pixel est calculé et l'histogramme des codes LBP est construit comme la caractéristique LBP. Pour calculer le code lbp, pour chaque pixel p, les 8 voisins du pixel central sont comparés au pixel p et les voisins x se voient attribuer une valeur 1 si $x \geq p$

III 3-3 Qu'est-ce que l'algorithme LBPH?

Résumé: L'algorithme d'histogramme de modèle binaire local (LBPH) est une solution simple au problème de reconnaissance de visage, qui peut reconnaître à la fois la face avant et la face latérale. ... Pour résoudre ce problème, un algorithme LBPH modifié basé sur la médiane de gris de voisinage de pixels (MLBPH) est proposé

III 3-4 Qu'est-ce que LBP Cascade?

Cependant, j'ai remarqué qu'il existe également plusieurs cascades LBP. Après avoir fait quelques recherches, j'ai trouvé que LBP signifie Local Binary Patterns, et il peut également être utilisé pour la détection de visage, selon la documentation de détection de visage Open CV

III 3- 5 Quelles sont les fonctionnalités LBP?

Le modèle binaire local (LBP) est un opérateur de texture simple mais très efficace qui étiquette les pixels d'une image en seuillant le voisinage de chaque pixel et considère le résultat comme un nombre binaire. Il a été décrit pour la première fois en 1994 (LBP) et s'est depuis révélé être une caractéristique puissante pour la classification des textures.

III 4. Application

la figure 19 et 20 montre une image veine de doigt avec sa représentation LBP

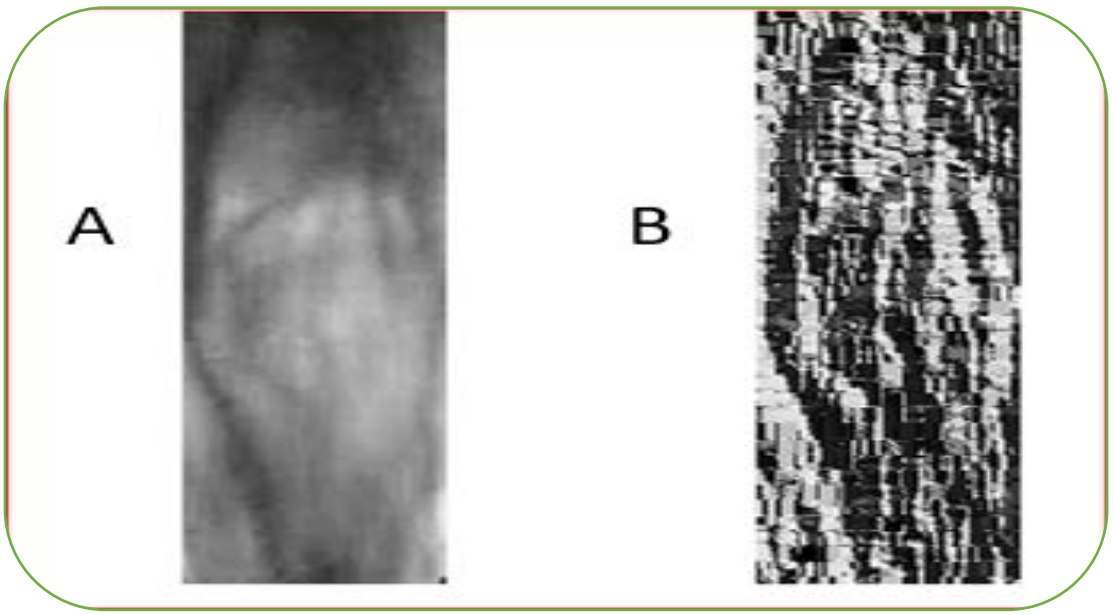


figure 19 A) image veine B) image LBP

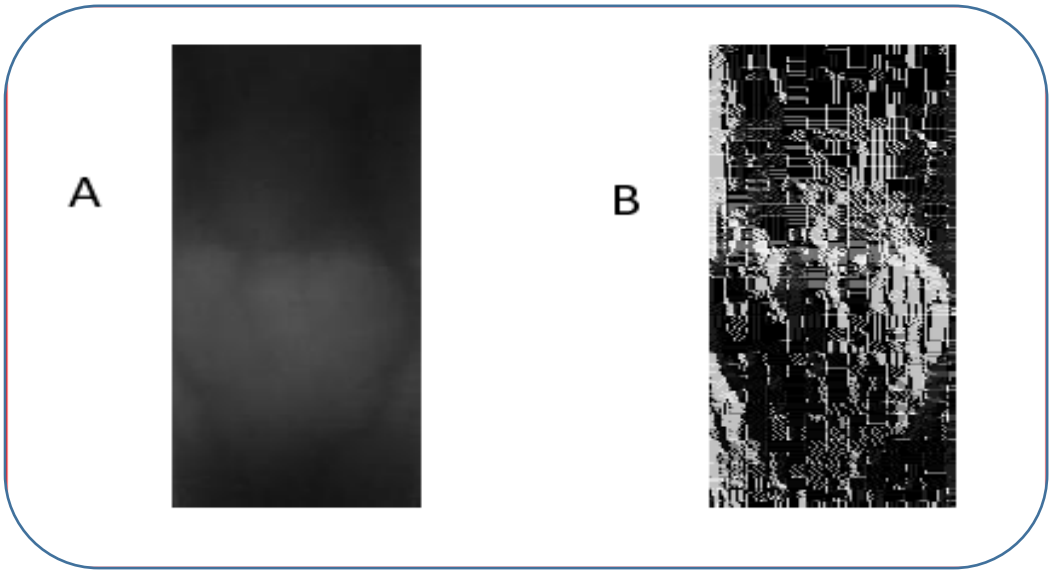


figure 20 A) image veine B) image LBP

le score de similarité entre ces deux image est M1 = 0.3212. pour deux images identiques le score est M2 = 0 à cause de l'opérateur XOR dans l'équation. il est claire que à partir de cette exemple que le pouvoir discriminatif de cette méthode n'est pas assez fort , c'est à dire la différence entre les deux valeurs (M1-M2) est faible. Dans ce travail nous avons pris comme mesure de similarité la valeur 1-M, d'où le score devient 1 pour deux images similaires, et 0.6788 pour le cas des deux images différentes présenté ci-dessus.

nous avons appliqué le modèle LBP sur la base de donnée FV-USM. les résultat de calcule de FAR et FRR sont montré dans la figure 21. la valeur de EER est la valeur où FAR=FRR , donc c'est l'intersection entre les deux courbes FAR et FRR. une autre représentation pour calculer la valeur de EER est la représentation de FRR en fonction de FAR comme montrée sur la figure 22. à partir des deux figures 3 et 4, nous avons trouvé la valeur de EER = 26.52. pour un seuil égale 0.64.

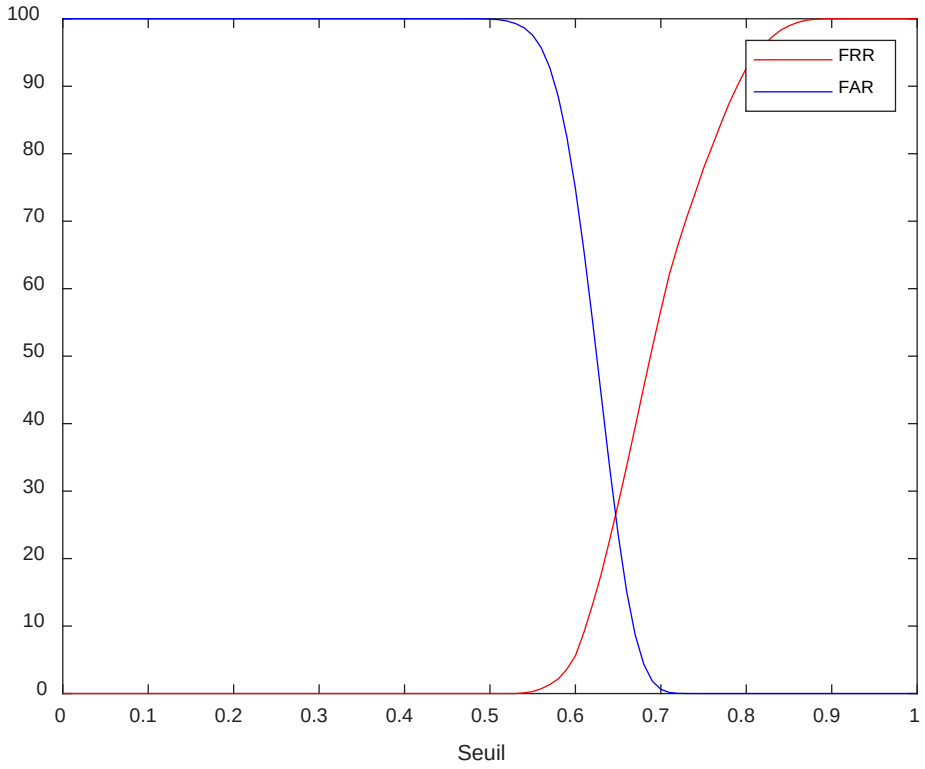


Figure 21 : calcule de seuil FAR et FRR

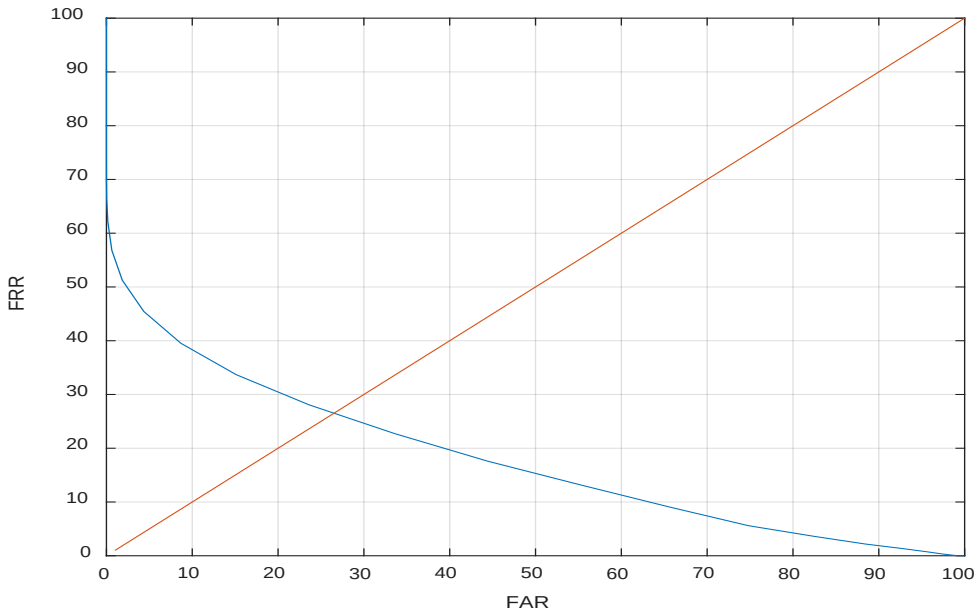


Figure 22 FRR en fonction FAR

Le tableau suivant donne le EER pour d'autre base de données

Base de donnée	FV-USM	SDUMLA-FV[**ref**]	PolyU [**ref**]
EER	26.52	10.27%	7.44%

tableau ; EER pour d'autre base de données

[il est claire que le ERR varie considérablement entre une base de donnée à l'autre. où on remarque que la valeur de l'erreur la plus petite est pour la base Poly U.

III 5 Conclusion

Dans ce chapitre nous avons réussie à appliquer la méthode LBP sur la base de données FV-USM. les résultats présentées montre une variation de résultat de l'EER d'une base à l'autre d'où les algorithmes de reconnaissance par veines de doigt doivent être choisi selon la valeur de L'ERR la plus petite.

Conclusion Générale :

Conclusion Générale et perspectives :

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 ses 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 :

Nous avons choisi les trois méthodes suivantes : LBP, LLBP, LPQ

Grâce à ces méthodes, nous avons atteint un taux de reconnaissance idéal en particulier pour LPQ, ce qui est très intéressant car il fiabilise notre système et nous permet d'atteindre le but que nous nous étions 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 avons acquis une bonne réputation dans ce domaine

Bibliographie

[1] L.Wang, G. Leedham, "Near- and- Far- Infrared Imaging for Vein Pattern Biometrics", Proceedings of the IEEE International Conference on Video and Signal Based Surveillance, 2006

[2] L.Wang, G. Leedham, et D.Cho "Minutiae feature analysis for infrared hand vein pattern biometrics, The Journal of the pattern recognition society, Vol. 41, Issue 3, pp. 920-929, 2008

[3] A.K. Jain, L. Hong et S. Pankanti, "Biometrics: Promising Frontiers for Emerging Identification Market", Comm. ACM, pp. 91-98, 2000.

[4] L. Dugelay et al., " Recent Advances in Biometric Person Authentication ", IEEE Int. Conf. on Acoustics Speech and Signal Processing (ICASSP), Orlando, 2002.

[5] http://www.biometricgroup.com/

[6] P. MACGREGOR et R. WELFORD, " Vein check : imaging for security and personnel identification ", Advanced Imaging, Vol. 9, No. 7, pp.52-56, 1991.

[7] M. Nadort, " The hand vein pattern used as a biometric feature ", Master's thesis, Free University, Amsterdam, 2007.

[8] Eichmann, L. Yuan, D. Moyon, F. Lenoble, L. Pardanaud, et C. Breant, "Vascular development: from precursor cells to branched arterial and venous networks", International Journal of Developmental Biology, No. 49, pp. 259-267, 2005. [9] S. Prabhakar, S. Pankanti, et A. K. Jain, "Biometric Recognition: Security and Privacy Concerns", IEEE Security & Privacy Magazine, Vol. 1, No. 2, pp.33-42, 2003.

[10] L. O Gorman, " Comparing passwords, tokens, and biometrics for user authentication " , Proceedings of the IEEE, Vol. 91, No. 12, pp. 20-40, 2003.

[11] L. Wang and G. Leedham, " Near- and Far- Infrared Imaging for Vein Pattern Biometrics", Proceedings of the IEEE International Conference on Video and Signal, pp. 52-59, 2006.

[12] A. M. Badawi, " Hand Vein Biometric Verification Prototype: A Testing Performance and Patterns Similarity ", IPCV, pp. 3-9, 2006.

[13] L. Wang, G. Leedham, and D. S.-Y. Cho, "Minutiae feature analysis for infrared hand vein pattern biometrics" , Pattern Recognition, vol. 41, pp. 920-929, 2008.

[14] L. Wang and G. Leedham, "A thermal hand vein pattern verification system", Lecture Notes in Computer Science, pp. 58-65, 2005.

[15] J. Serra. " Introduction à la morphologie mathématique ". Ecole des mines, Paris, 1960.

[16] Steven W.Smith. The Scientist and Engineer's Guide to Digital Signal Processing. California Technical Publishing. 2007.

[17] T.J., Zhang and C.Y. Suen, "A fast parallel algorithm for thinning digital pattern" , Comm. Of ACM 27 , pp. 236-239

Bibliographie

[18] F. Zernike, "Diffraction theory of the cut procedure and its improved form, the phase contrast method". Physica, pp. 689-704, 1934.

[19] M.R. Teague, " Image Analysis via the general theory of moments". J.Opt,Soc., vol 23, 1975.

[20] E. Davalo et P. Naïm, "Des réseaux de neurones, 2eme ed ", Paris: Eyrolles, 1993.

[21] P.D.Power, " Non linear Multilayer Perceptron channel equalization ", PHD Dissertation, University of Belfast, 2001.

[22] S. Haykin, " Neural Networks: A Comprehensive Foundation, 2and ed ", New York: Macmillan College Publishing, 1998.

[23] G. Dreyfus, "Réseaux de neurones: Méthodologie et application", Paris: Eyrolles, 2002.

[24] S. Siu, G.J. Gibson,and C.F.N. Cowan, " Decision feedback equalisation using neural network structures and performance comparison with standard architecture ", IEE Proceedings, Vol. 137, Pt. I, No. 4, pp. 221-225, 1990.

[25] M.Ibnnkahla, "Application of neural networks to digital communication", Signal processing 80, pp. 1185-1215, 2000.

[26] K. Hornik, "Multilayer feed forward networks are universal approximators ", Neural Networks, vol. 2, pp .359-366. 1989.

[27] K. Levenberg "A Method for the Solution of Certain Non–linear Problems in Least Squares ", Quarterly Journal of Applied Mathematics II (2), pp. 164–168, 1944

[28] D. W. Marquardt "An Algorithm for Least-Squares Estimation of Nonlinear Parameters", Journal of Soc. Indust. Appl. Math, Vol. 11, No. 2, pp. 431-441, June 1963

[28]-https://fr.wikipedia.org/wiki/classement_automatique. [29]belaidi asma et bassaid imane - classification de l'hypothyroidie par approche, mono classifieur et multi classifieurs-université abou bakr belkaïd de tlemcen- 2015.

[30]-https://www.xlstat.com/fr/solutions/fonctionnalites/k-nearest-neighbors knn.

[31]-https://www.python-course.eu/k_nearest_neighbor_classifier.ph

[ref] : [08240902.pdf] Liu, H., Yang, L., Yang, G., & Yin, Y. (2017). Discriminative binary descriptor for finger vein recognition. IEEE Access, 6, 5795-5804.