République Algérienne Démocratique et populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de M'Hamed Bougara Boumerdes

Faculté des Sciences de l'Ingénieur

Département Maintenance Industrielle

Option : Génie Electrique

MEMOIRE DE FIN D'ETUDES

Pour l'obtention du diplôme de Master en génie électrique

Spécialité : signal et communications

THEME

Identification de personnes par la géométrie de la main

Réalisé par:

Khaled NOUREDDINE

Encadré par:

Mr. HARRAR khaled

Promotion : 2015/ 2016

Remerciements

Tous d'abord, je tiens à remercier la faculté des sciences de l'ingénieur de l'université de M'hamed Bougara, BOUMERDES, pour m'accepter cette année au sein de département de génie électrique.

Je remercie sincèrement Monsieur Khaled HARRAR, qui, en tant que directeur de ce mémoire, s'est toujours montré à l'écoute et très disponible tout au long de la réalisation de ce mémoire de Master, ainsi pour l'aide et le temps qu'il a bien voulu me consacrer.

Je remercie vivement les membres du jury d'avoir accepté évaluer ce travail.

Enfin, j'adresse mes plus sincère remerciements à ma famille, tous mes proches et amis, qui m'ont toujours soutenu et encouragé au cours de la réalisation de ce travail.

Merci à tous.

Dédicaces

A mon père, à ma mère.

A mes frères et sœurs.

A tous mes amis.

A tous mes maitres et professeurs : du primaire au supérieur.

ملخص

التقنيات البيومترية أصبحت أساسا ذو مجال واسع لحلول تحديد الهوية والتحقق الشخصي. تبين التجارب أن الأبعاد الهندسية لید الإنسان (طول الأصابع، وعرض الأصابع، ...) تحتوي على معلومات قادرة على تحديد هوية الفرد. في هذا العمل، تم تطبيق في برنامج ماتلاب نظام لتحديد هوية الأشخاص على أساس هندسة اليد (ملامس وبدون دبابيس). الذي هو، في التطبيقات الأمنية ذات الدرجة المتوسطة والمنخفضة، قادر على تعويض الطرق التقليدية (كلمة السر، شارة، ...) التي يمكن أن تنسى، تفقد أو تسرق. هذا النظام ذو ثمن منخفض وملائم للمستعمل مقارنة مع الأنظمة ذات الدبابيس. وهذا النظام يستعمل المسافة الإقليدية لقياس الخصائص البيومترية لتحديد هوية الأشخاص. النتائج المتحصل عليها تكشف أن الخصائص البيومترية لهندسة اليد تختلف بحسب درجة التمييز. وأن أطوال الأصابع أكثر تمييزا من أعراض الأصابع.

الكلمات المفتاحية : الأمن، البيومترية، هندسة اليد، تحديد الهوية، معالجة الصورة.

Résumé

Les technologies biométriques deviennent le fondement d'une vaste gamme des solutions d'identification et vérifications personnelles. Des expériences montrent que les dimensions physiques de la main humaine (Longueur des doigts, largeur des doigts, …) contiennent des informations qui sont capables de vérifier l'identité d'un individu. Dans ce travail, nous avons réalisé sous MATLAB un système d'identification par la géométrie de la main, sans contrainte et avec contacte qui, dans les applications de niveau de sécurité moyen et faible, est capable de remplacer les méthodes traditionnelles (mot de passe, badge, …) qui peuvent être oubliés, volés ou perdus. Ce système est moins couteux et aimable pour l'utilisateur par rapport aux systèmes d'identification par la géométrie de la main avec contrainte et avec chevillés (pegs). Ce système utilise une fonction de similarité (distance euclidienne) pour la reconnaissance des personnes. Les résultats obtenus montrent que les caractéristiques biométriques de la main diffèrent selon le degré de discrimination. Par ailleurs, les longueurs des doigts sont plus discriminatives que leurs largeurs.

Mots Cles : Sécurité, biométrie, géométrie de la main, reconnaissance, traitement d'image.

Abstract

Biometric technologies are becoming the foundation for a wide range of identification and personal verification solutions. Experiments show that the physical dimensions of the human hand (length of the fingers, width of the fingers, ...) contain information that are capable of verifying the identity of an individual. In this work, we have developed an unconstrained and contact based hand geometry identification system which, in the medium and low security applications, is able to replace traditional methods (password, badge, ...) that can be forgotten, lost or stolen. This system also cheaper and user-friendly in comparison with constrained and contact based hand geometry identification systems. This system uses the Euclidean distance as similarity function for recognizing people. The results obtained show that the biometric characteristics of the hand differ from each other by the degree of discrimination. In addition, the lengths of the fingers are more discriminative than the widths of the fingers.

Keywords : Security, biometric, hand geometry, recognition, image processing.

SOMMAIRE

Chapitre III : Implémentation

Chapitre IV : Résultats et Interprétations

LISTE DES FIGURES

Chapitre IV

LISTE DES TABLEAUX

Chapitre IV

Introduction Générale

La sécurité des systèmes d'information est devenue un domaine de recherche d'une très grande importance. La conception d'un système d'identification fiable, efficace et robuste est une tâche prioritaire. L'identification de l'individu est essentielle pour assurer la sécurité des systèmes et des organisations. Elle correspond à la recherche de l'identité de la personne qui se présente dans une base de données et peut servir à autoriser l'utilisation des services.

Pour répondre à ces besoins, la biométrie semble être une solution pratique, efficace et dont le coût en effort et en argent est en constante diminution. En effet, cette technique connaît un développement remarquable. Grace à la puissance de calcul grandissante des ordinateurs, les applications biométriques sont devenues de plus en plus nombreuses et efficaces. Elles permettent d'apporter un niveau de sécurité supérieur en ce qui concerne des accès logiques (ordinateurs, comptes bancaires, données sensibles, etc.), ou des accès physiques (bâtiments sécurisés, aéroports, laboratoires, etc.) [1].

Dans ce travail, nous développons un procédé d'identification biométrique par la géométrie de la main, sans contrainte et avec contact. Notre étude se base à différencier les mains des utilisateurs par les longueurs et les largeurs des doigts et les classifier en utilisant le minimum de distance euclidienne.

Le mémoire est organisé comme suit :

Le premier chapitre, présente les raisons qui mènent à l'utilisation de la biométrie, et l'importance de la biométrie en général.

Dans le deuxième chapitre, nous avons introduit l'architecture globale des systèmes biométriques et comment évaluer ces systèmes, nous avons classé les systèmes biométriques de reconnaissance par la géométrie de la main selon le mode d'acquisition, et nous avons donné leurs avantages et inconvénients.

Dans le troisième chapitre, nous avons présenté les méthodes de traitement nécessaires sous MATLAB, pour l'enrôlement des utilisateurs à partir d'une base d'images que nous avons créée, ainsi que les étapes pour identifier les utilisateurs.

Le quatrième chapitre donne les résultats obtenus à partir des tests de performances effectuées, et les interprétations.

Enfin, une conclusion générale terminera notre travail.

Généralités Sur 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. De plus, les actes terroristes et les menaces qui pèsent sur de nombreux pays obligent une identification fiable des personnes (contrôle aux frontière, accès aux lieux publics, transport, …). Jusqu'à présent les méthodes usuelles d'identification sont basées sur *ce que l'on possède* (carte d'identité, carte à puce, …) 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 son code, décryptage du mot de passe via des logiciels spécifiques, …) [2].

I.2 La biométrie

Le terme "biométrie" provient des mots grecs, « bios » qui veut dire la vie et du mot « métrique » qui veut dire mesure. La biométrie englobe les technologies utilisées pour mesurer et analyser les caractéristiques d'une personne et pour objectif de déterminer son identité de manière irréfutable. Contrairement à *ce que l'on sait* ou *ce que l'on possède* la biométrie est basée sur *ce que l'on est*, [2].

I.2.1 Les modalités biométriques

Les applications de la biométrie se sont développées de plus en plus ces dernières décennies. Elles sont réparties en trois groupes majeurs d'utilisation :

- **Commerciale :** utilisation pour la sécurisation d'accès physique ou virtuel tel que le contrôle d'accès physique, la sécurisation des transactions électroniques, l'accès à Internet ou à un réseau local, les cartes de crédit, etc.
- **Gouvernementale :** application dans les cartes d'identité, le permis de conduire, la carte de sécurité sociale, le passeport, etc.
- **Sécuritaire :** reconnaissance dans les investigations criminelles, l'identification terroriste, etc.

Pour chacune de ces utilisations, les contraintes biométriques sont différentes. Aucune biométrie unique ne peut répondre à toutes ces exigences. Ainsi, le type de biométrie utilisée dépend essentiellement de l'application envisagée, [2].

Les propriétés biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en trois catégories :

- **Analyses biologique :** ADN, …
- **Analyses comportementales :** dynamique de la frappe au clavier, démarche, signature, …
- **Analyses morphologiques :** empreintes digitales, géométrie de la main, iris …

Pratiquement, n'importe quelle modalité morphologique, comportementale ou biologique peut être considérée comme une modalité biométrique, dans la mesure où elle satisfait les propriétés suivantes :

- Universelle : chaque personne doit posséder la caractéristique.
- Distinctive : deux personnes doivent avoir des caractéristiques différentes.
- Permanente : la caractéristique doit être invariante au cours du temps.
- Collectionnable : la caractéristique doit être acquise.
- Performance : le système biométrique doit permettre une reconnaissance précise, rapide et robuste à des changements opérationnels et environnementaux.
- Acceptabilité : la caractéristique biométrique doit être bien accepté par les utilisateurs.
- Infalsifiabilité : le système doit être difficilement utilisable par des méthodes frauduleuses et des attaques.

Les modalités biométriques ne possèdent pas toutes ces propriétés, ou les possèdent mais à des degrés différents. Le choix de la modalité est ainsi effectué selon un compromis entre la présence ou l'absence de certaines de ces propriétés selon les besoins de chaque application, [2].

I.2.1.1 ADN (Acide DésoxyriboNucléique)

L'ADN est un code unique pour chaque individu, excepté pour les jumeaux homozygotes. Il peut être extrait à partir de sang, de peau ou de cheveux. L'identification par ADN est une méthode très répandue dans les utilisations sécuritaires. Cette reconnaissance possède trois limites majeures : il est facile de voler un « morceau » d'ADN pouvant être utilisé de façon

frauduleuse, le processus de reconnaissance est lent et couteux et L'ADN contient des informations telles que les maladies génétiques qui pourraient être utilisées à mauvais escient, [3].

I.2.1.2 Dynamique de la frappe au clavier

La dynamique de la frappe au clavier est le processus qui analyse la façon de frapper au clavier en surveillant le nombre et le rythme de frappe par seconde. Cette caractéristique n'est pas unique à chaque individu mais présente un fort confort d'utilisation tout en supprimant l'acquisition d'un équipement supplémentaire. Cette méthode est une biométrie comportementale, elle n'est donc pas stable au cours du temps ce qui peut limiter son utilisation, [3].

I.2.1.3 Empreinte digitale

Les empreintes digitales sont la technologie biométrique la plus mature. Cette technologie est utilisée depuis plus d'un siècle et de très nombreuses recherches ces dernières décennies ont permis d'obtenir de très bons taux de reconnaissance. Une empreinte digitale est une structure composée de vallées et de crêtes, de points caractéristiques appelés minuties (bifurcation, fin de lignes, lac, etc.) et de pores de la peau uniques à chaque individu (même pour les jumeaux homozygotes). La précision de la reconnaissance par empreinte digitale permet l'utilisation dans des bases de données de grandes tailles (de plusieurs millions d'individus). Le faible cout et la petite taille des capteurs permettent en plus une utilisation dans les téléphones et les ordinateurs portables. Cependant, une partie de la population ne peut pas utiliser la reconnaissance par les empreintes digitales à cause de l'âge, de facteurs génétiques, environnementaux ou de travail (les travailleurs manuels n'ont souvent plus d'empreintes digitales) , [3].

I.2.1.4 Empreinte palmaire

La paume de la main est une technologie récente. Elle contient comme les empreintes digitales des vallées, des rides sur une surface cependant plus large. Cette technologie est ainsi supposée plus caractéristique que les empreintes digitales, [3].

I.2.1.5 Géométrie de la main

La géométrie de la main ou des doigts est une méthode physique de reconnaissance très simple s'appuyant sur la taille de la paume, la largeur, la longueur, et la courbure des doigts. Bien que les méthodes d'extraction et de comparaison de caractéristiques soient très simple, la géométrie de la main permet une reconnaissance relativement robuste et de nombreux systèmes sont installés pour des contrôles physiques. L'avantage de cette technique est qu'elle est complètement robuste aux facteurs environnementaux tels que l'humidité ainsi qu'à des facteurs individuels tels que des coupures ou la peau sèches. Les principales limitations consistent à extraire des informations géométriques pertinentes même lorsque les utilisateurs portent des bagues ou sont limités dans leurs mouvements à cause d'une arthrite par exemple, [3].

I.2.1.6 Iris

L'iris est la région annulaire colorée de l'œil située derrière la cornée. La texture visuelle de l'iris est unique et très stable au cours du temps ; elle est stabilisée dès deux ans. La précision et la vitesse de la reconnaissance par l'iris permettent une identification efficace sur de très larges bases de données. Chaque iris est distincte entre deux individus même pour les vrais jumeaux et il est très difficile de modifier son iris ou de faire un faux (contrairement à l'empreinte digitale par exemple). La limite de cette approche vient du cout du capteur et d'une utilisation non intuitive du capteur d'acquisition (même si ces deux facteurs tendent à largement s'améliorer) , [3].

I.2.1.7 Rétine

Le réseau sanguin de la rétine est très riche en structure et est réputé caractéristique pour chaque individu. La reconnaissance par la rétine requiert une coopération de l'utilisateur plus forte que l'iris avec un contact entre le capteur et l'œil. Cependant, ce principe de reconnaissance est réputé être le système le plus sécurisé puisqu'il est impossible de modifier le réseau vasculaire de la rétine sans danger physique et qu'il est également très difficile de répliquer un réseau rétinien, [3].

I.2.1.8 Thermographie de la main

Les motifs de peau (de la main, d'un doigt ou du visage) capturées par infrarouge de longueur d'onde proche de celle de la chaleur corporelle sont caractéristiques de chaque individu.

L'avantage principale de ce type de méthode est l'acquisition qui s'effectue sans contact mais qui peut s'avérer très difficile dans le cas d'environnement incontrôlé pour lequel la température est très variable. Cependant, les veines du dos de la main peuvent être obtenues avec une longueur d'onde adéquate afin de caractériser un individu. Le prix très élevé des capteurs infrarouge reste prohibitif pour une utilisation grand public, [3].

I.2.1.9 Visage

La reconnaissance faciale est la méthode d'identification la plus naturelle ; c'est celle que tout le monde utilise tous les jours pour se reconnaître. De très nombreuses recherches se concentrent sur ce secteur biométrique très porteur car pouvant être effectué à distance avec ou sans la coopération de l'utilisateur. La reconnaissance du visage reste cependant l'une des méthodes biométriques dont l'extraction des caractéristiques est la plus difficile. En effet, le visage dans l'image d'acquisition est très variable à cause des occlusions partielles (lunettes, foulards, etc), des changements d'illumination, des expressions du visage (joie, tristesse, etc.) et des positions d'acquisition changeantes. Les caractéristiques sont définies suivant deux approches. La première est une méthode géométrique s'appuyant sur la localisation et la forme des yeux, des lèvres ou du nez. D'autres méthodes plus robustes s'appuient sur des études complètes du visage principalement par approches statistiques, [3].

I.2.1.10 Voix

La voix est la seule technologie biométrique existante s'appuyant sur une combinaison des approches physiques et comportementales. La voix est basée sur la forme et la taille des tractus vocaux (cordes vocales, pharynx, larynx, luette et lèvres). Ces caractéristiques physiques sont invariantes pour chaque individu mais très variables au cours du temps à cause de l'âge, de raisons médicales (gros rhume par exemple) ou de l'état émotionnel. De plus, la voix n'est pas très distinctive entre chaque individu et ne permet pas d'identifier deux jumeaux. Cependant, la reconnaissance par la voix reste la méthode la plus adéquate pour l'authentification biométrique par téléphone, [3].

I.2.2 Les modèles biométriques

Un modèle biométrique (appelé aussi référence, gabarit ou template) est l'ensemble des données utilisées pour représenter un utilisateur. Les modalités biométriques acquises ne sont pas

enregistrées et utilisées telles quelles. Une phase de traitement est effectuée pour réduire les données biométriques brutes et produire ainsi le modèle biométrique. Pour le stockage de ces modèles, il existe quatre emplacements principaux que sont le clé USB, la base centralisée, la machine individuelle de travail et le capteur biométrique. Chacun de ces emplacements présente des avantages et faiblesses en termes de temps de traitement, confidentialité et respect de la vie privée, [2].

I.3 Les limitations des systèmes biométriques

Malgré les avantages des systèmes biométriques par rapport aux systèmes traditionnels, leur utilisation est toujours limitée à des applications spécifiques (comme le passeport biométrique). Ces systèmes souffrent de plusieurs limitations qui peuvent dégrader considérablement leur intérêt.

La première limitation se situe dans la performance. Contrairement aux systèmes d'authentification traditionnels, les systèmes d'authentification basés sur la biométrie sont moins précis (i.e., pourcentage de similarité entre 0% et 100%, le 100% n'étant quasiment jamais atteint). Ce manque de précision est dû à plusieurs facteurs : la variabilité lors de la capture (i.e., bruits d'acquisition, utilisation de plusieurs capteurs d'acquisition, etc.), la variabilité intra-classe (variabilité des données biométriques pour un individu) et la similarité inter-classe (i.e., similarité des données biométriques de plusieurs individus).

Une autre limitation de la biométrie est la limitation d'usage ou culturelle. La biométrie et particulièrement les empreintes digitales ont une mauvaise réputation et sont associées à la surveillance des personnes et à l'identification de criminels. Dépendant de la modalité utilisée, l'acquisition de données biométriques est effectuée sans ou avec contact avec le capteur biométrique. Ce contact est une source d'inquiétudes pour certains utilisateurs pour des raisons d'hygiène et d'intrusion physique. Prenons le cas de reconnaissance par la rétine : cette technologie assure une bonne fiabilité et une haute barrière contre la fraude. Malgré l'efficacité de cette technologie, elle est considérée comme intrusive et elle est très peu utilisée dans les milieux de la sécurité privée. Le recours à la biométrie présente également des risques en termes de respect des droits et des libertés fondamentales.

Enfin, les systèmes biométriques sont vulnérables à des attaques spécifiques. Car du point de vue du système informatique, ce ne sont rien d'autres que des séries de bits comme toute donnée (on peut attaquer les bases de données contenant toutes les données biométriques de référence), [2].

I.4 Conclusion

Dans ce chapitre nous avons présenté l'intérêt et le besoin de l'identification des personnes dans la société, et la biométrie est un moyen efficace pour accomplir cet objectif et peut aussi remplacer les méthodes traditionnelles d'authentification qui peuvent être oublié, volés ou perdus. Et nous avons mentionné les différentes modalités de la biométrie. Enfin, nous avons cité les limitations de la biométrie.

Systèmes de Reconnaissance Biométriques

II.1 Introduction

Les systèmes biométriques constituent un assemblage de composants matériels (capteurs, ordinateurs, etc.) et logiciels (algorithmes, drivers des capteurs, etc.). Les systèmes biométriques sont de plus en plus utilisés pour vérifier ou déterminer l'identité d'un individu. Ces systèmes comportent un avantage primordial sur les systèmes d'authentification traditionnels, dans la mesure ou la relation entre l'authentifiant et l'individu ne peut pas être plus étroite, [2].

Dans ce chapitre nous allons présenter l'architecture des systèmes biométriques, et comment évaluer ces systèmes et nous passerons sur les systèmes de reconnaissance par la géométrie de la main.

II.2 Architecture d'un système biométrique

Un système biométrique est un système de reconnaissance de formes se divisant en quatre modules :

- **Module d'acquisition :** il capture la donnée biométrique d'un individu. Il s'agit d'un capteur biométrique qui peut être de type sans ou avec contact ;
- **Module d'extraction des caractéristiques :** il détermine un ensemble de caractéristiques biométriques à partir de la donnée acquise.
- **Module de comparaison :** il compare les caractéristiques extraites durant la phase de reconnaissance avec des caractéristiques enregistrées afin de déterminer un score de similarité. Ce module est aussi un module de décision dans lequel un utilisateur indique son identité qui est confirmé ou non (authentification). Dans un autre mode (identification), l'identifiant d'un utilisateur est établi à partir du score de similarité.
- **Module de base de données :** il stocke les modèles biométriques des utilisateurs enrôlés. Suivant l'application, le modèle est stocké dans une base de données centrale ou, pour plus de sécurité, enregistrée dans une carte individuelle, [3].

II.2.1 Enrôlement, vérification et identification

Les systèmes biométriques fonctionnent selon trois modes qui sont l'enrôlement, la vérification d'identité et l'identification [3] :

- **Enrôlement**

La donnée biométrique est capturée par le module d'acquisition, figure (II.1). Suivant la qualité de l'acquisition, la donnée biométrique peut être rejetée et une autre capture désirée. Si la donnée est de bonne qualité, les caractéristiques biométriques extraites sont nommées modèle (référence) ou gabarit (template). Généralement, plusieurs modèles sont enregistrés pour chaque individu et celles-ci peuvent être mises à jour pendant l'utilisation. Pour des raisons de sécurité, les modèles de chaque individu sont cryptés. Cette sécurité permet de rendre impossible la reconstitution des caractéristiques physiques et limite l'utilisation d'un modèle à l'application visée.

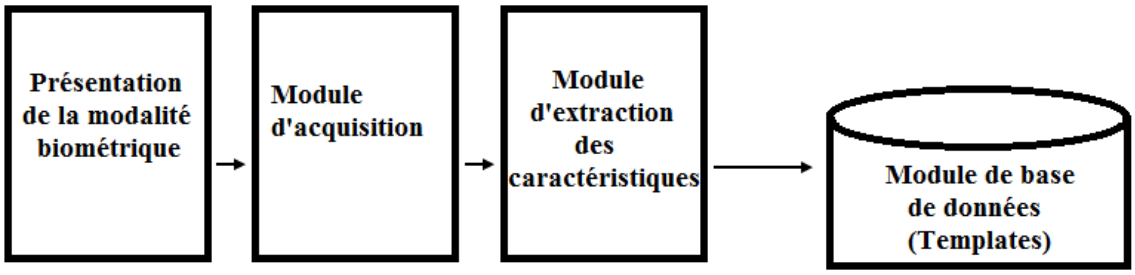

Figure II.1 : Le processus d'enrôlement.

- **Vérification (authentification)**

La vérification d'identité consiste à contrôler, figure (II.2), si l'individu utilisant le système est bien la personne qu'il prétend être. Le système compare l'information biométrique acquise avec le modèle biométrique correspondant stocké dans la base de données, on parle de test (1:1). Dans ce cas, le système renvoie uniquement une décision binaire (oui ou non) pouvant être pondérée. Le processus de vérification peut être formalisé comme suit :

Soit le vecteur d'entrée C_U définissant les caractéristiques biométriques de l'utilisateur U extraites par le système, et M_U son modèle biométrique stocké dans la base de données, le système retourne une valeur booléenne suite au calcul de la fonction *f* définie par :

$$f(C_U, M_U) = \begin{cases} 1 & si\ S(C_U, M_U) \geq \tau \\ 0 & sinon \end{cases} \qquad \text{(II.1).}$$

Ou S est la fonction de similarité définissant la correspondance entre les deux vecteurs biométriques, et τ le seuil de décision (fixé) à partir duquel les deux vecteurs sont considérés comme identiques.

- **Identification**

En mode identification, figure (II.2), le système biométrique détermine l'identité d'un individu inconnu en cherchant parmi les modèles de tous les individus dans la base de données, on parle de test (1 : N). Dans ce cas, le système peut alors soit attribuer à l'individu inconnu l'identité correspondant au profil le plus proche retrouvé dans la base (ou une liste des profils proches), soit rejeter l'individu. Le processus d'identification peut être formalisé ainsi :

Soit le vecteur d'entrée C_U définissant les caractéristiques biométriques extraites par le système lorsqu'un utilisateur U se présente devant celui-ci, l'identification revient à déterminer l'identité de I_k, $k \in \{0, 1, \cdots, N\}$ ou $I_1, \cdots, I_N$ sont les identités des utilisateurs préalablement enrôlés dans le système, et I_0 indique une identité inconnue. La fonction d'identification f peut ainsi être définie par :

$$f(C_U) = \begin{cases} I_k & si\ S(C_U, M_k) \geq \tau \\ I_0 & sinon \end{cases} \qquad \text{(II.2).}$$

Ou M_k est le modèle biométrique correspondant à l'identité I_k, S est la fonction de similarité, et τ le seuil de décision.

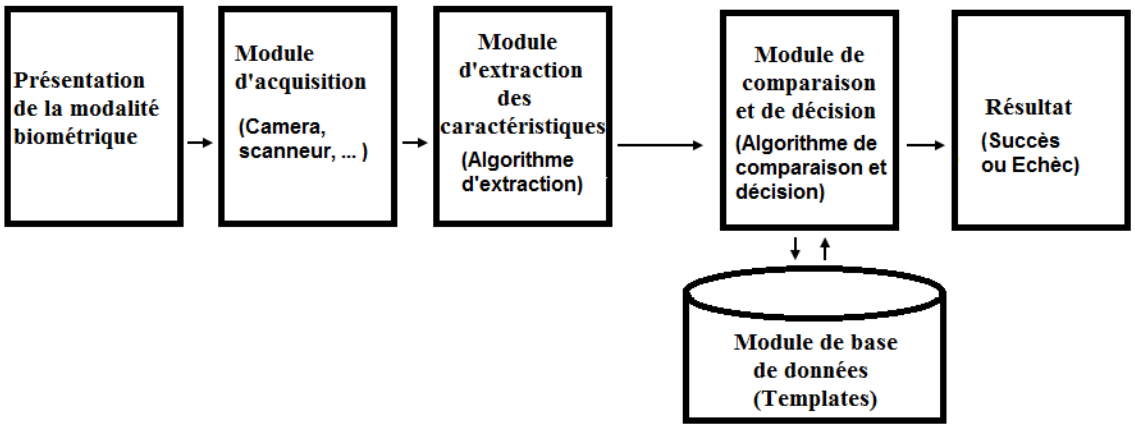

Figure II.2 : Processus de vérification ou identification.

II.3 Evaluation de performances des systèmes biométriques

Les taux d'erreur sont l'une des caractéristiques d'un système biométrique. A cause des conditions ambiantes (température, luminosité...), de la qualité d'acquisition (bruit du capteur, positionnement de l'utilisateur...) et des changements physiques ou comportementales de l'utilisateur (coupures, prise de poids...), deux caractéristiques biométriques provenant de la même personne ne sont pas exactement identiques. Comme indiqué dans les équations (II.1) et (II.2), un seuil τ permet d'effectuer la décision de classement : si le score de comparaison est supérieur à τ alors les deux caractéristiques proviennent de la même personne, sinon elles sont déclarées comme provenant de personnes différentes. Afin d'évaluer la qualité d'un système biométrique, la distribution des scores de comparaison déterminée à partir de couples d'exemples provenant de la même personne nommée distribution des authentiques est spécifiée. De même, la distribution des imposteurs est spécifiée à partir de couples d'exemples provenant de personnes différentes. Ces deux courbes de distribution sont illustrées à la Figure (II.3).

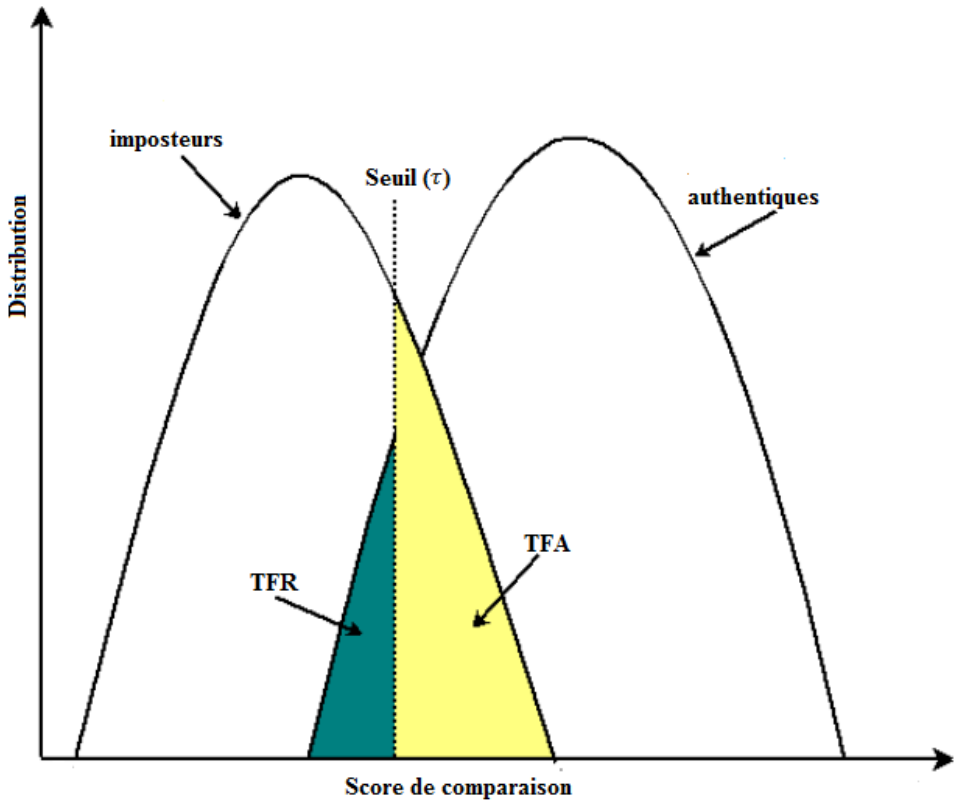

Figure II.3 : Courbes de distribution des authentiques et des imposteurs, [3].

Un système biométrique se caractérise par deux types d'erreur, les faux rejetés et les faux acceptés :

- **Faux accepté :** deux caractéristiques biométriques provenant de deux personnes différentes sont indiquées comme provenant de la même personne.
- **Faux rejeté :** deux caractéristiques biométriques provenant de la même personne sont classées comme provenant de deux personnes différentes.

Le taux de faux rejetés (TFR) défini par le rapport entre le nombre de personnes (authentiques) rejetées à tort (par erreur) et le nombre de tentatives d'accès, (II.3).

$$TFR = \frac{Nombre\ des\ utilisateurs\ authentiques\ rejeté}{Nombre\ de\ tentatives\ des\ utilisateurs\ authentiques} \times 100\% \qquad \text{(II.3)}$$

Le taux de faux acceptés (TFA) défini par le rapport entre le nombre de personnes (imposteurs) acceptées à tort et le nombre de tentatives d'accès, (II.4).

$$TFA = \frac{Nombre\ des\ imposteurs\ acceptés}{Nombre\ de\ tentatives\ des\ imposteurs} \times 100\% \qquad \text{(II.4)}$$

Les deux taux d'erreur correspondants, le taux de faux acceptés (TFA) et le taux de faux rejetés (TFR) respectivement, sont ambivalents. Il est ainsi nécessaire d'établir un compromis entre ces deux taux d'erreur. Ce compromis est effectué en ajustant le seuil τ ; si τ augmente pour avoir un système plus sécurisé alors le TFR augmente et le TFA baisse. Inversement, si le seuil τ est diminué afin d'avoir un système plus tolérant alors le TFR baisse et le TFA augmente. Les performances des systèmes biométrique sont reportés sur un graphe nommé Receiver Operating Curve (ROC) déterminé par l'ensemble des points du TFA contre les points du TFR en faisant varier le seuil τ, Figure (II.4).

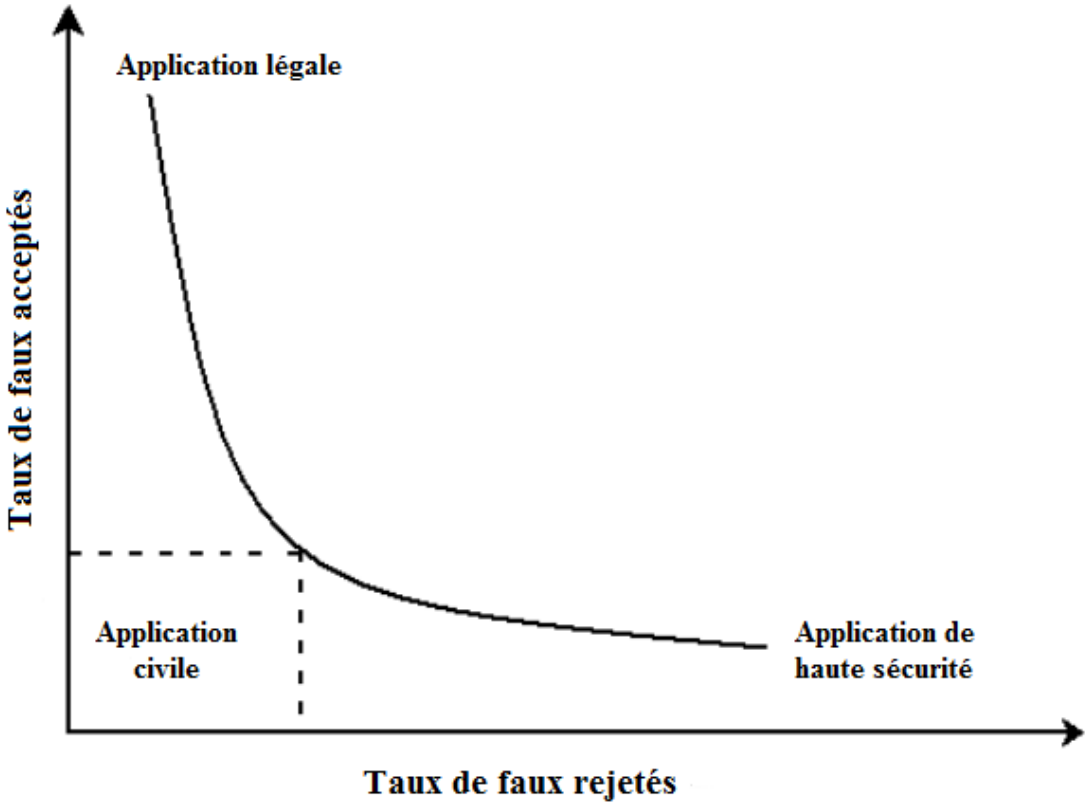

Figure II.4 : Courbe ROC (Receiver Operating Curve), [3].

La sécurité souhaitée d'un système biométrique est très dépendante de l'utilisation. Dans des systèmes de très haute sécurité tels que les centrales nucléaires par exemple, il est impératif qu'aucun imposteur ne puisse se faire autoriser l'accès par erreur ; le TFA doit être le plus faible possible. Par contre, dans les systèmes d'identification par les empreintes digitales dans les enquêtes policières, le TFR doit être très proche de zéro (même s'il est nécessaire ensuite que les fausses détections soient examinées manuellement) afin de limiter le risque de ne pas sélectionner un individu présent dans la base. Un TFR faible est également souhaité dans les applications grand public pour privilégier les côtés ergonomique et d'acceptation du service. Plus généralement, dans les applications civiles un compromis est effectué entre les deux erreurs. Le compromis absolu, lorsque le taux de faux acceptés et le taux de faux rejetés sont identiques, est nommé le niveau d'égale erreur du système (EER).

- **Le Taux d'Egale Erreur (TEE),** Le taux auquel à la fois les erreurs d'acceptation et de rejet sont égaux.

Le TEE est un moyen rapide de comparer la précision des appareils (La performance optimale du système), d'une manière générale, le dispositif avec le TEE le plus bas est le plus précis.

- **Le taux d'identification (TI)** est le taux auquel un sujet (utilisateur authentique) dans une base de données biométriques est correctement identifié, (II-5).

$$TI_{seuil\ optimal} = \frac{Nombre\ des\ utilisateurs\ authentiques\ correctement\ identifiés}{Nombre\ de\ tentatives\ des\ utilisateurs\ authentiques} \times 100 \quad \text{(II.5)}$$

On obtient le taux d'identification du système, quand en fixant le seuil à la valeur optimale. Le seuil optimal est déterminé à partir de la valeur de TEE (TFR est égale à TFA), [3].

II.4 Systèmes de reconnaissance par la géométrie de la main

Les systèmes de reconnaissance par la géométrie de la main mesurent et analysent la structure globale, la forme et les proportions de la main, par exemple longueur, largeur et épaisseur de la main, les doigts et les articulations, les caractéristiques de la surface de la peau telles que les rides et les crêtes. Certains systèmes biométriques de géométrie de la main mesurent jusqu'à 90 paramètres, [4].

Les approches de reconnaissance par la géométrie de la main peuvent être classés en trois catégories en fonction de la nature d'acquisition des images :

II.4.1 Systèmes avec contrainte et avec contact

Ces systèmes utilisent des chevilles (pegs) sur la surface de dispositif pour guider le placement de la main, figure (II.5). Au cours de l'étape d'acquisition, l'utilisateur s'est invité de mettre sa main sur la surface, plusieurs fois ou les chevilles qui sortent de la surface de dispositif serrent à placer les doigts dans la position correcte. De cette façon, ces systèmes permettent une meilleure mesure par rapport aux systèmes sans chevillés, parce que la main est fixée à la surface et ne peut pas être déplacée, [4].

Figure II.5 : Lecteur biométrique de reconnaissance par la géométrie de la main, [5].

L'avantage de ce système, par rapport au système sans chevillés, est que ces chevillés sont des bases prédéfinies pour la mesure des caractéristiques. Tandis que le plus grand inconvénient est que le système peut déformer, dans une certaine mesure, l'apparition de la main figure (II.6.A), de sorte que les mesures ne sont pas très précises. Il doit être mentionné que les diverses positions des doigts figure (II.6.B,C) peuvent effectuer sur la mesure des caractéristiques, [6].

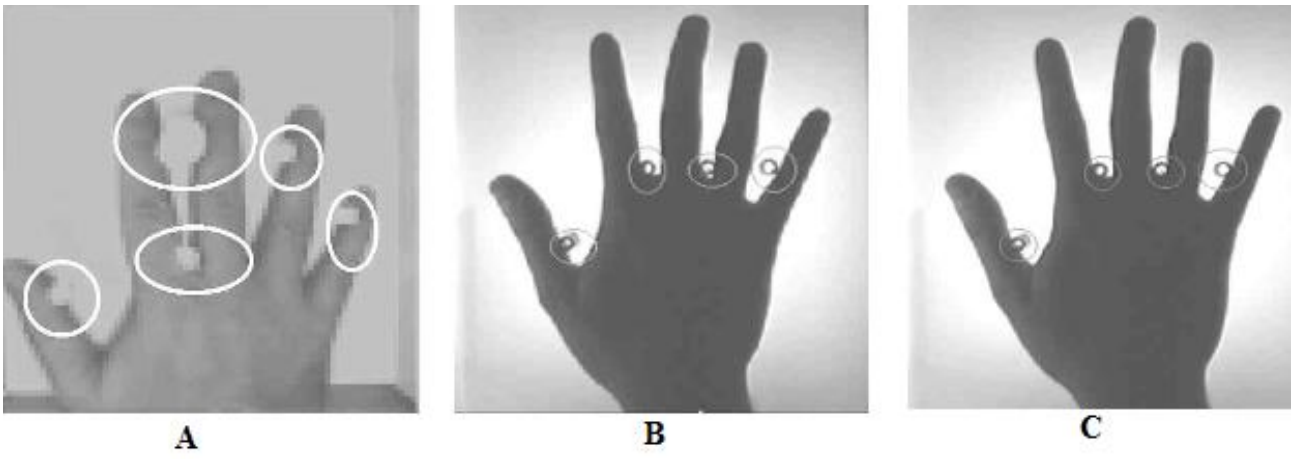

Figure II.6 : Système avec chevillés, A- La forme de la main est déformé. B, C- différents placements de la même main, [6].

II.4.2 Système sans contrainte et avec contact

Les images de la main sont acquises d'une manière sans contrainte, nécessitant souvent les utilisateurs de placer leur main sur une surface sans chevillés. Des points de repère (bouts des doigts et des vallées de doigt) sur l'image de la main sont couramment utilisés pour l'extraction de caractéristiques, [4].

II.4.3 Système sans contrainte et sans contact

Cette approche élimine la nécessité pour toutes les chevilles ou la surface lors de l'acquisition d'images de la main. Les utilisateurs ont la liberté à tenir leur main librement dans l'espace, généralement à une distance (approximativement) fixe de la caméra. Les images acquises dans ce milieu encombrés peuvent également exiger des algorithmes de segmentation sophistiqués pour localiser la main dans l'image. Ce mode d'acquisition d'image est considéré comme plus aimable à l'utilisateur, [4].

II.5 Conclusion

Les systèmes biométriques peuvent être utilisé comme une méthode automatisée pour identifier et vérifier l'identité d'un individu. Les systèmes de reconnaissance par la géométrie de la main, sans contrainte et avec contacte sont plus acceptés par les utilisateurs que les systèmes avec contrainte et avec contacte. Et la rapidité de d'identification et la simplicité des algorithmes utilisées par les systèmes de reconnaissances par la géométrie de la main, sans contrainte et avec contact, donnent des avantages à ces systèmes par rapport aux systèmes sans contrainte et sans contact.

Implémentation

III.1 Introduction

Les systèmes d'identification biométrique par la géométrie de la main fournissent des estimations de certaines mesures de la main, tels que la longueur et la largeur des doigts.

L'identification par la géométrie de la main est basée sur le fait que la main de chaque personne a une forme presque différente et que la forme de la main d'une personne ne change pas après un certain âge, [7]. En pratique, l'identification par la géométrie de la main est normalement basée sur la détection des cinq points qui correspondent aux bouts des doigts et quatre points entre eux (points de la vallée), figure (III.1).

La principale difficulté dans la détection de ces points est souvent à cause des doigts qui ne sont pas écartés, figure (III.2). Des méthodes spécifiques souvent doivent être mises en œuvre lors de l'étape d'acquisition et de prétraitement afin de rendre la détection de ces points plus facile. Une fois les points ont été localisés, les caractéristiques biométriques nécessaires à l'identification ont été extraites, [8].

La méthodologie utilisée dans ce travail pour la conception d'un système d'identification par la géométrie de la main a été mis en œuvre dans l'environnement MATLAB R2016a. Les principales idées derrière ce système sont divisées en deux phases : Enrôlement et Identification.

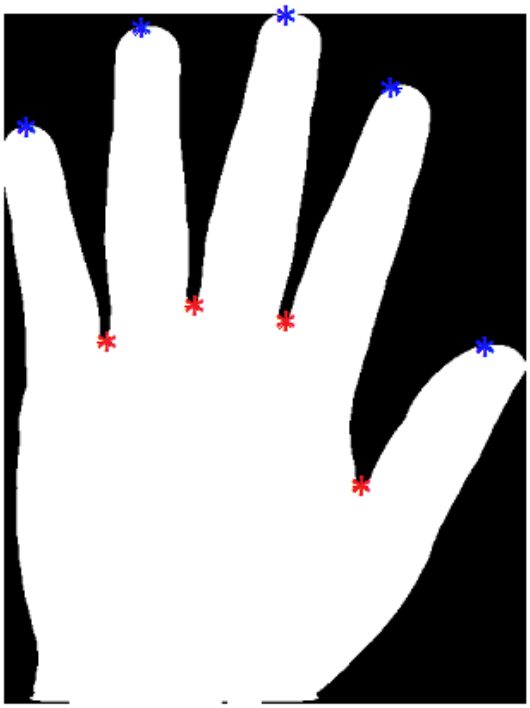

Figure III.1 : Détection correcte des points de repère.

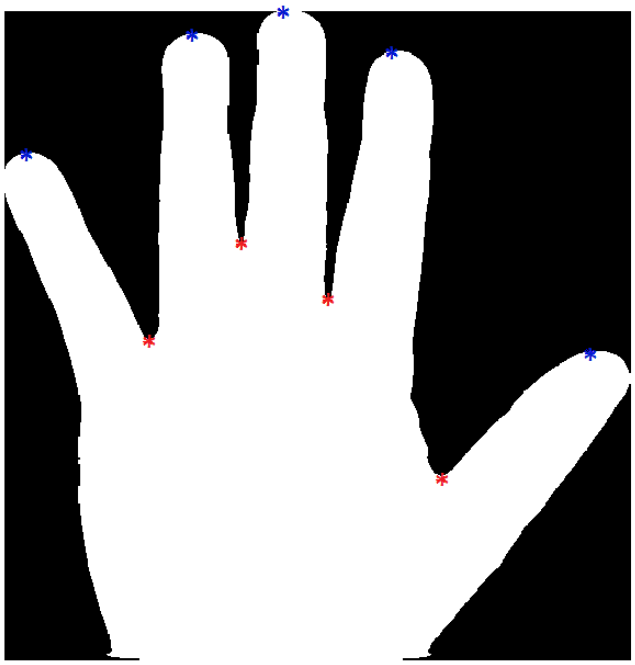

Figure III.2 : détection incorrecte des points de repère.

III.2 Phase d'enrôlement

Dans la première phase d'enrôlement (figure III.3), nous avons recueilli les images de la main droite des utilisateurs et nous les avons regroupés dans une base de données nommée « base de données des images des utilisateurs ». Le système prétraite toutes les images de chaque utilisateur, extrait les caractéristiques biométriques pour chaque utilisateur, et store la moyenne des caractéristiques biométriques (Template) de chaque utilisateur dans une autre base de données nommée « base de données de templates ».

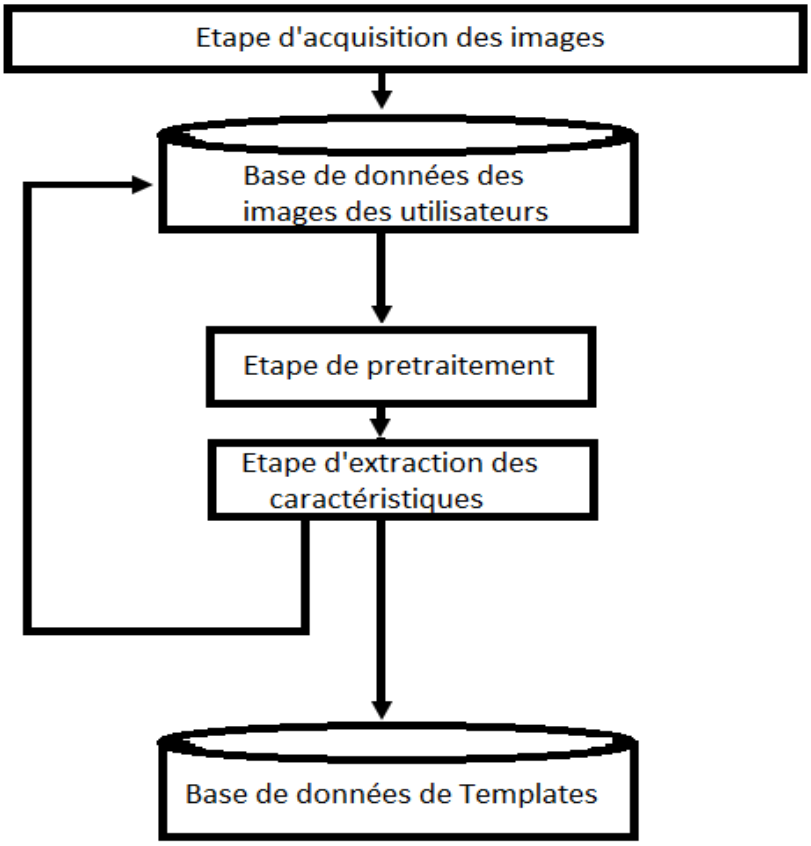

Figure III.3 : Schéma synoptique du processus d'enrôlement.

III.2.1 Etape d'acquisition et de collection des images

Les images de la main sont obtenues à partir du groupe d'utilisateurs et stockées dans la base de données « Base de données des images des utilisateurs ». A cet effet, Un scanner normale à plat a été utilisé ' Canon i-SENSYS MF3010'. Nous avons réglé le scanneur à ces paramètres :

- Format papier : (215.9 x 215.9 millimètres) (Résolution de pixel 637 x 637).
- Mode de numérisation : Couleur.

- Qualité de l'image : 75 ppp (minimale qualité fournée par le scanneur).
- Type de l'image : TIFF.

Pour que la localisation des points de repère (pics et vallées des doigts) soit précise, il faut respecter les conditions suivantes :

- L'arrière-plan doit être noir (cette condition assure que l'histogramme de l'image grise sera bimodal, et ça facilite la détection du contour où se situent les points de repère), Nous avons utilisé une boite noire (comme arrière-plan) pour couvrir la main de l'utilisateur pendant l'acquisition.
- Les doigts de l'utilisateur ne se touchent pas entre eux.
- La surface du scanner doit être claire (par le nettoyage des traces due à la multiple pose des mains)

En cas de non-respect des conditions décrites, une image de mauvaise qualité sera générée. Pour cela notre système néglige cette image et invite l'utilisateur à prendre une autre.

III.2.2 Description de la base de données des images des utilisateurs

Pour tester les performances de ce système, il faut avoir des images des utilisateurs authentiques et des images des imposteurs.

Le contenu de cette base est :

12 utilisateurs authentiques (10 images de la main droite par utilisateurs), Nous avons utilisé les cinq premières images des utilisateurs authentiques pour la phase d'enrôlement et les dernières cinq images pour la phase d'identification.

03 imposteurs (5 images de la main droite par personnes) pour tester les performances.

Au total, nous avons (60 images) des utilisateurs authentiques utilisées dans la phase d'enrôlement et [(60 images) des utilisateurs authentiques + (15 images) des imposteurs = (75 images) utilisées pour tester les performances].

Note :

Utilisateur authentique est une personne autorisée à accéder à la zone protégée par le système biométriques.

Imposteur, il n'est pas autorisé d'accéder à la zone protégée, mais il va essayer.

La figure (III.4) suivante montre des exemples des images de la main droite des utilisateurs enregistrés dans la base.

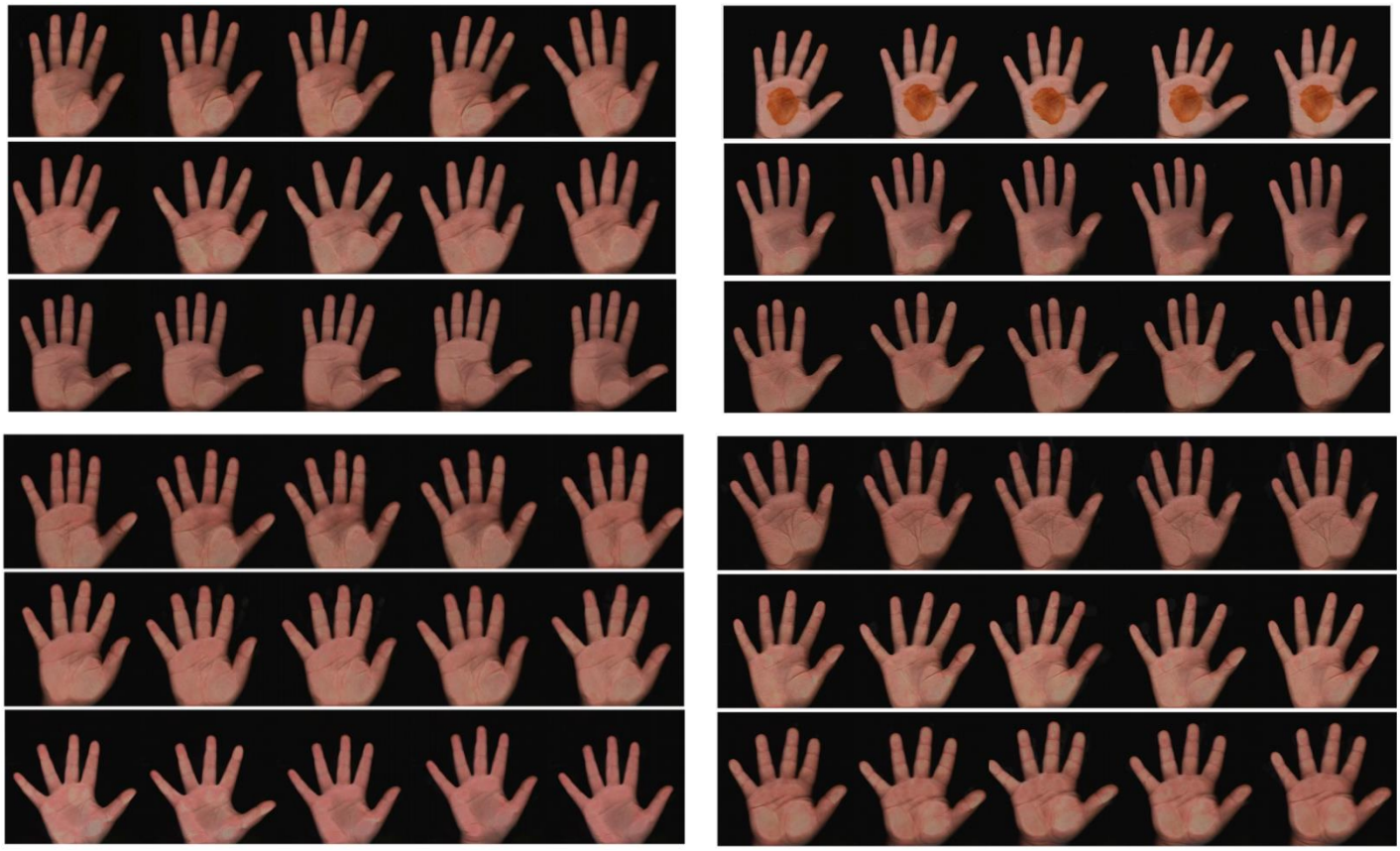

Figure III.4 : Echantillons des images de la base de données des utilisateurs.

III.2.3 Etape de prétraitement de l'image

Le prétraitement de l'image se rapporte à la préparation de l'image pour l'analyse et l'utilisation ultérieure (extraction de caractéristiques), figure (III.5). Cette est étape est cruciale afin d'obtenir une image sortante de qualité avec contour de la main (où se trouve les pics et vallée des doigts) qui n'est pas déformé.

Dans l'étape de prétraitement, l'image de la main d'entrée est prétraitée en réglant le contraste pour obtenir une image binaire acceptable. Ensuite, l'image est filtrée en utilisant le filtre médian pour éliminer le bruit impulsionnel de type « sel et poivre ». En outre, la suppression de certaine pixels indésirables dans l'arrière-plan, donne des images de fond claires. Finalement nous sélectionnons la région d'intérêt ROI (La main).

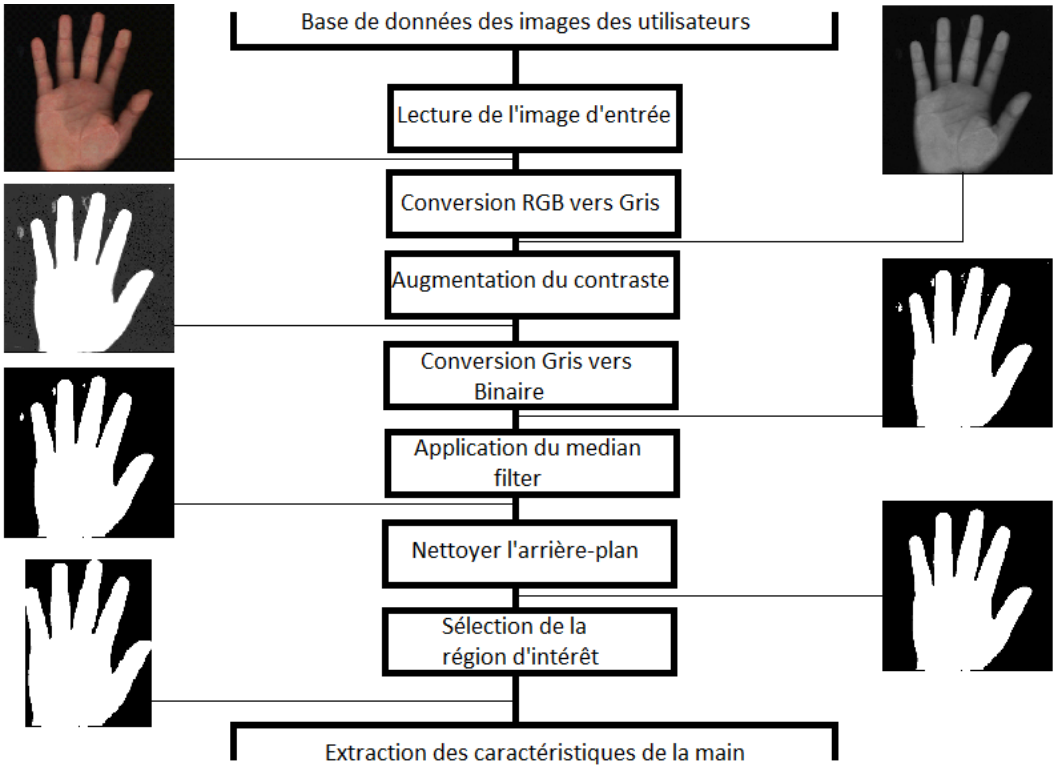

Figure III.5 : Schéma synoptique du processus du prétraitement.

Les opérations impliquées dans l'étape de prétraitement sont les suivantes :

III.2.3.1 Lecture de l'image d'entrée

Premièrement l'image d'entrée doit être lue Figure (III.6.A) pour des traitements futurs.

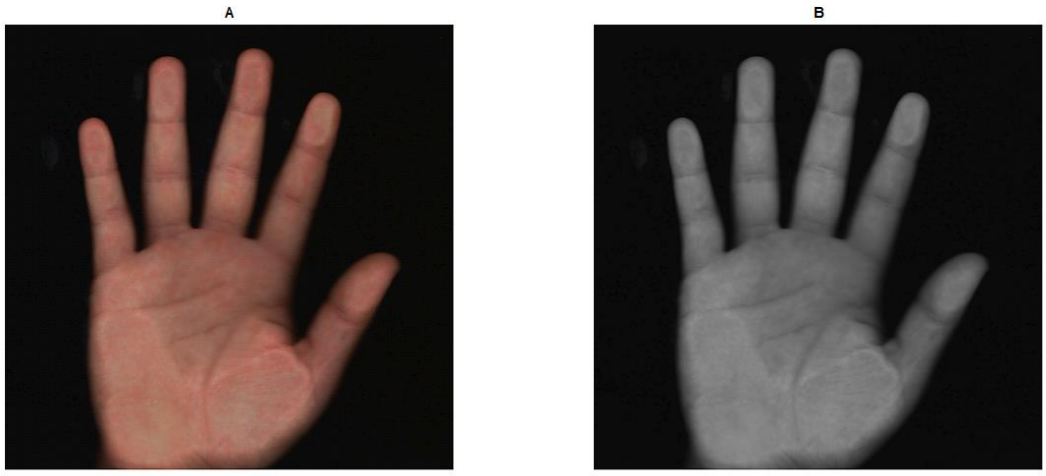

Figure III.6 : Lecture de l'image. A- Image couleur, B- Image grise.

III.2.3.2 Conversion RGB vers Gris

L'image capturée par le scanneur est en couleur Figure (III.6.A), et pour pouvoir traiter l'image, il est nécessaire de convertir l'image couleur en image à niveaux gris Figure (III.6.B).

Une image couleur RGB, $I_{couleur}$, est convertie en niveaux de gris, I_{grise}, en utilisant la transformation suivante:

$$I_{grise}(n,m) = \alpha I_{couleur}(n,m,r) + \beta I_{couleur}(n,m,g) + \gamma I_{couleur}(n,m,b) \qquad \text{(III.1)}$$

Ou (n,m) Indexe un pixel individuel dans l'image en niveaux de gris, et r, g et b représentent les canaux de l'image couleur rouge, vert et bleu.

Les coefficients de pondération (α, β et γ) sont établis proportionnellement à la réponse perceptive de l'œil humain à chacun des canaux de couleur rouge, vert et bleu et une pondération normalisée assure l'uniformité (Norme de télévision NTSC (National Television System Committee), α =0,2989, β = 0,5870 et γ = 0,1140), [14].

III.2.3.3 Augmentation du contraste

Le contraste peut être expliqué simplement comme étant la différence entre l'intensité du pixel maximale et minimale dans une image, [10].

Pourquoi augmenter le contraste ? La détection du contour, où se situent les points de repère (pics et vallée), sera impossible si on convertie directement l'image grise vers une image binaire, figure (III.7).

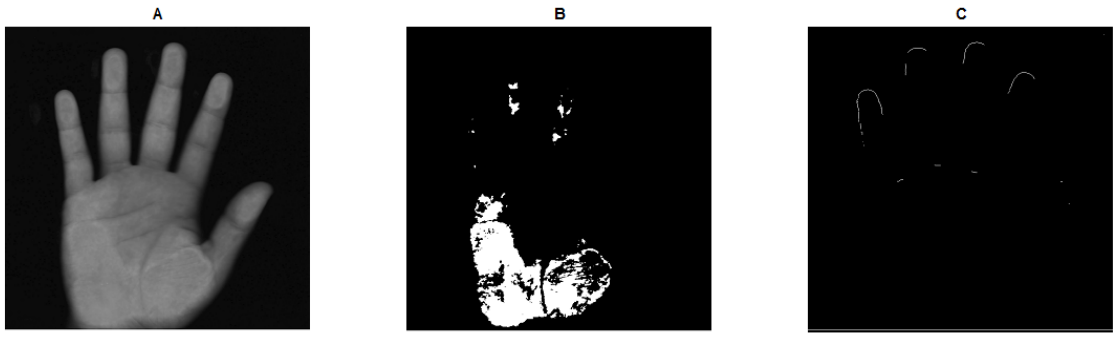

Figure III.7 : A- image grise sans modifier le contraste, B- conversion binaire de l'image A, C- détection de contour de l'image B.

Dans la figure (III.7.C), nous remarquons que le contour de la main est déformé. Pour pallier ce problème il faut augmenter le contraste de l'image à niveaux de gris, pour obtenir un contour visible. La méthode utilisée nommée « étirement de l'histogramme ».

Un histogramme est un graphique statistique permettant de représenter la distribution des intensités des pixels d'une image, c'est-à-dire le nombre de pixels pour chaque intensité lumineuse, figure (III.10). Par convention un histogramme représente le niveau d'intensité en abscisse en allant du plus foncé (à gauche) au plus clair (à droite), [11].

L'histogramme est un outil très utile pour étudier la répartition des composantes d'une image. En outre sa modification n'altère pas les informations contenues dans l'image mais les rend plus ou moins visibles.

L'étirement d'histogramme (aussi appelé "linéarisation d'histogramme" ou "expansion de la dynamique") consiste à répartir les fréquences d'apparition des pixels sur la largeur de l'histogramme, exemple figure (III.10.B). Ainsi il s'agit d'une opération consistant à modifier l'histogramme de telle manière à répartir au mieux les intensités sur l'échelle des valeurs disponibles. Ceci revient à étendre l'histogramme afin que la valeur d'intensité la plus faible soit à zéro et que la plus haute soit à la valeur maximale. Cette technique permet d'augmenter le contraste de l'image grise, [11].

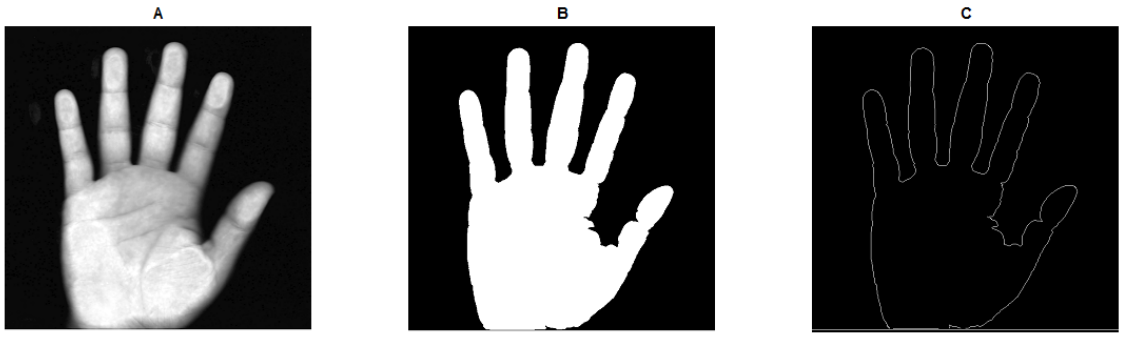

Figure III-8 : Détection de contour. A- contraste augmenté de l'image grise (III-7-A), B- image binaire de l'image A, C- détection du contour de l'image B.

Le contour obtenu à partir de l'image grise (III-8-A) est encore déformé. Puisque nous avons un histogramme bimodale (deux modes, mode à gauche et mode à droite, figure(III.10.B)), nous avons encore étalé la première partie de l'histogramme (mode à gauche) sur tous le rangé disponible, et ça nous donne un contour visible.

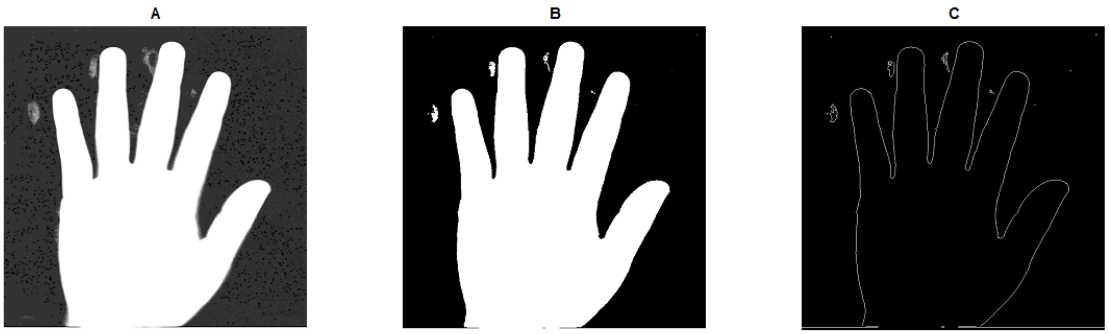

Figure III.9 : Détection de contour. A- contraste augmenté de l'image grise (III.8.A), B- image binaire de l'image A, C- détection du contour de l'image B.

Le contour obtenu à partir de l'image à niveaux de gris (III.9.A) est clair.

Nous avons utilisé la détection de contour et l'histogramme comme outils d'observation de l'état du contour et la distribution des intensités des pixels.

Le nombre de bins (niveaux de gris) dans l'histogramme est déterminé par le type de l'image. Si l'image est une image en niveaux de gris (codée sur 8 bits), MATLAB utilise une valeur par défaut de 256 bins. Si l'image est une image binaire, cette valeur sera de deux bins, [9].

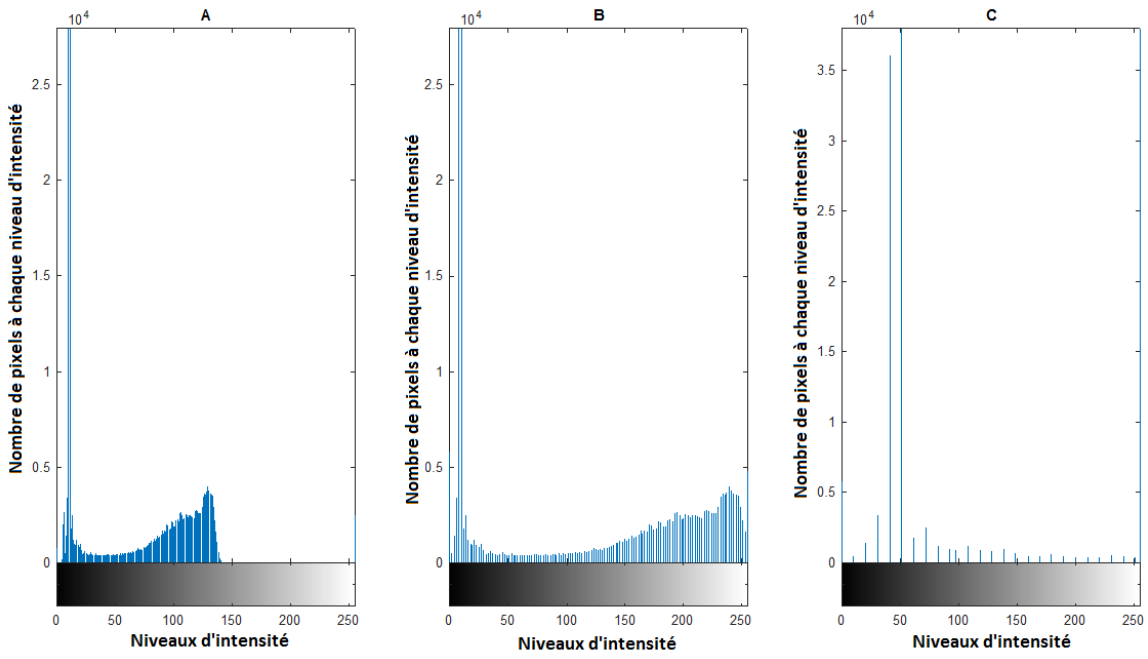

Figure III.10 : A- Histogramme de l'image (III.7.A). B- Histogramme de l'image (III.8.A).

C- Histogramme de l'image (III.9.A).

III.2.3.4 Conversion gris vers binaire

Après le choix de l'image grise appropriée, figure (III.11.A), nous avons converti cette image vers une image binaire, figure (III.11.B).

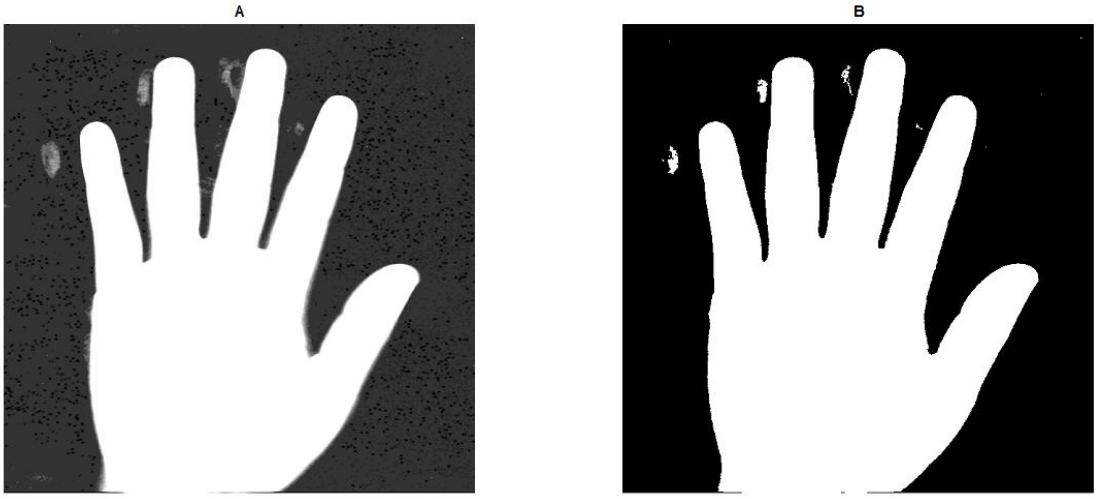

Figure III.11 : Binarisation de l'image. A- image grise appropriée, B- image binarisée.

La binarisation de l'image à niveaux de gris se fait par le remplacement de tous les pixels de l'image d'entrée avec luminance supérieure au seuil par la valeur 1 (blanc) et les pixels dont les niveaux de gris est inférieur au seuil choisi, par la valeur 0 (noir). La détermination du seuil se fait par la méthode d'Otsu.

La méthode d'OTSU est utilisée pour effectuer un seuillage automatique à partir de la forme de l'histogramme de l'image.Cette méthode nécessite donc le calcul préalable de l'histogramme de l'image. L'algorithme suppose alors que l'image à binariser ne contient que deux classes, (Les objets et l'arrière-plan). L'algorithme itératif calcule, le seuil optimal T qui sépare ces deux classes afin que la variance intra-classe soit minimale et que la variance inter-classe soit maximale, [13].

III.2.3.5 Application du filtre médian

Après le processus de rehaussement du contraste, il y a quelques pixels en dehors de la région d'intérêt (la main), leurs valeurs ont aussi changé ayant pris les mêmes valeurs que l'objet d'intérêt figure (III.12.A), ces points sont connus comme bruit de type « sel et poivre ».

Selon les conditions décrites précédemment, l'arrière-plan doit être clair pour que la détection du contour (points de repère - pics et vallées-) soit précise.

Nous avons utilisé le filtre médian pour supprimer ce bruit figure (III.12.B). Le filtre médian est une opération non linéaire souvent utilisé dans le traitement de l'image pour réduire le bruit de type « sel et poivre ». Un filtre médian est plus efficace lorsque l'objectif est simultanément de réduire le bruit et préserver les bords, [9].

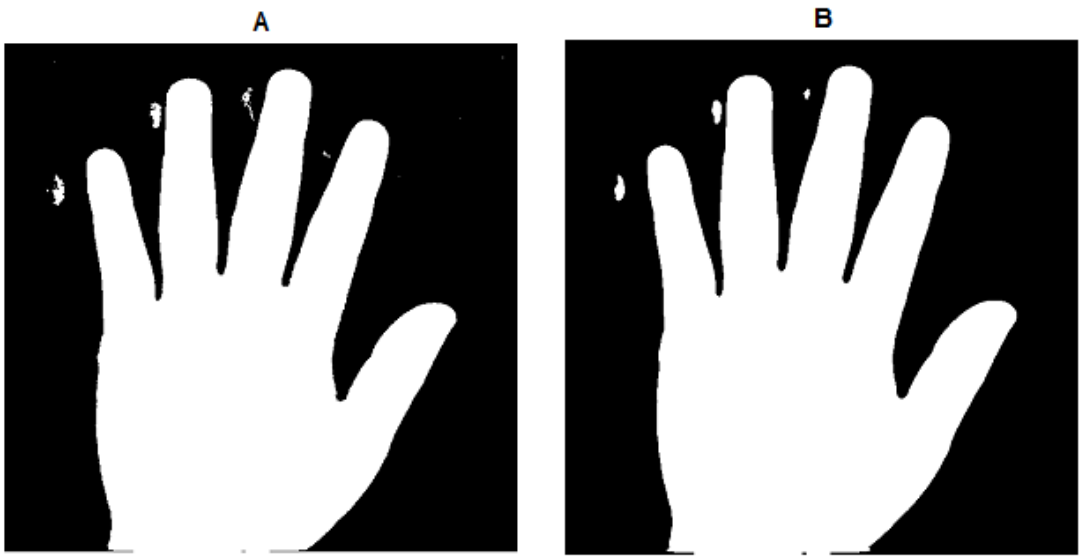

Figure III.12 : Application du filtre médian. A- image binaire, B- image filtrée par le médian filtre.

III.2.3.6 Nettoyage de l'arrière-plan

Lors de l'étape d'acquisition, et en raison de la multiple pose des mains des utilisateurs, il y a apparence de quelques traces sur la surface du scanner figure (III.13.A). Pour cela il faut procéder à la suppression de quelques pixels indésirables de l'image binaire, figure (III.13.B).

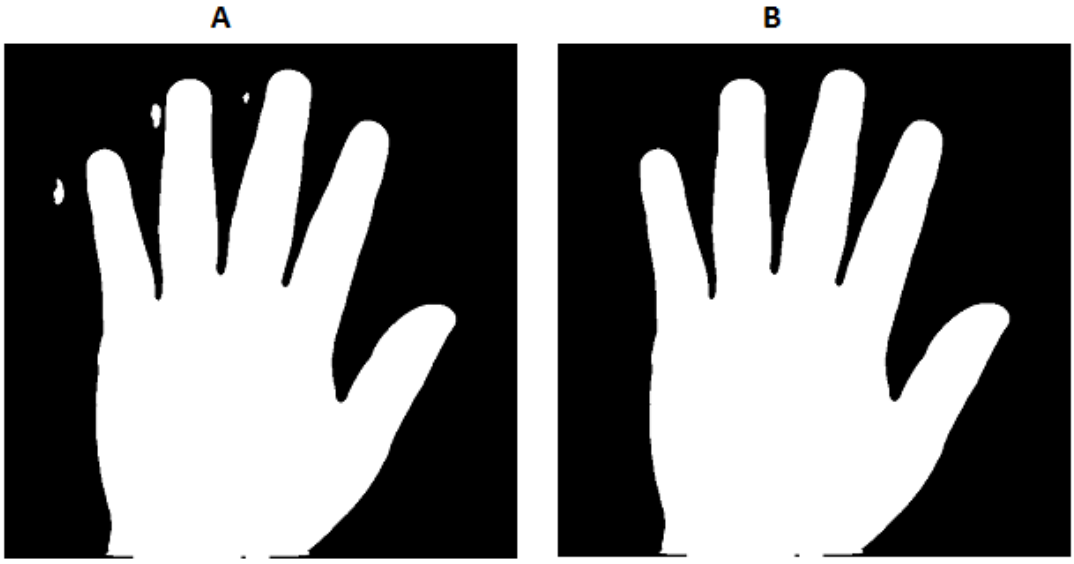

Figure III.13 : Suppression des pixels indésirables. A- image filtrée, B- nettoyage de l'arrière-plan.

III.2.3.7 Sélection de la région d'intérêt

Pour faciliter l'utilisation des images et réduire le temps de calcul, il faut travailler sur une image contenant seulement l'objet d'intérêt (la main), figure (III.14).

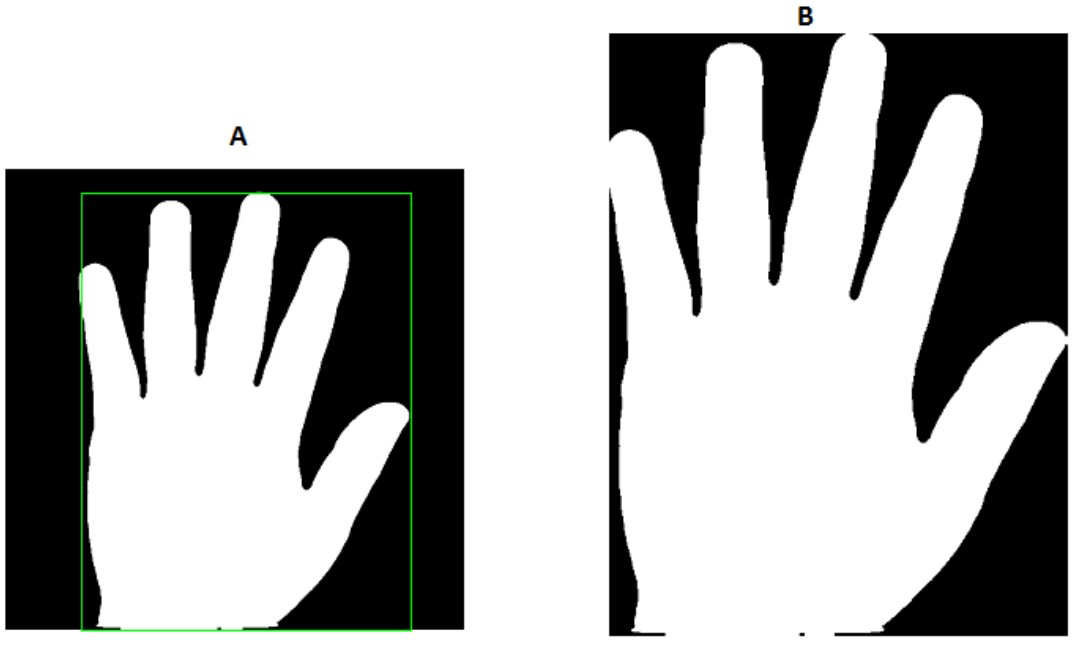

Figure III.14 : A- image prétraitée, B- sélection de l'objet d'intérêt.

III.2.4 Etape de l'extraction des caractéristiques de la main

Le rôle de cette étape est de créer un vecteur qui contient les mesures de caractéristiques biométriques discriminatives (la longueur des doigts, la largeur de doigts à des places différentes) à partir de l'image binaire créée précédemment, figure (III.15).

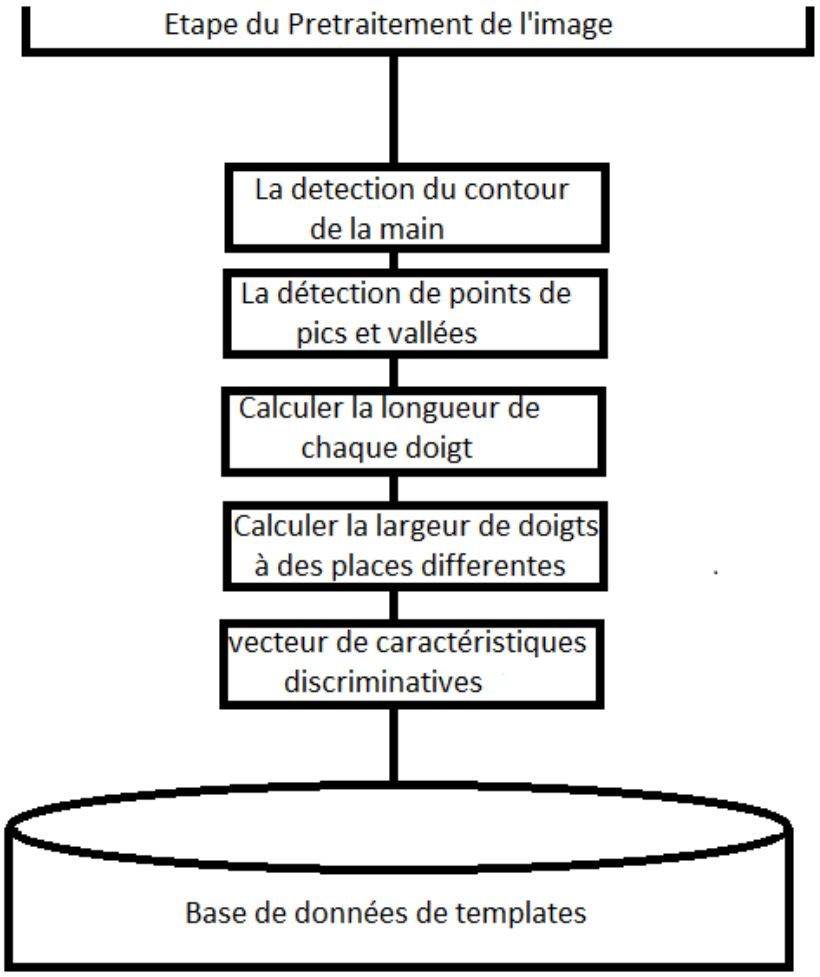

Figure III.15 : Schéma synoptique du processus d'extraction des caractéristiques.

III.2.4.1 La détection du contour de la main

Pour mesurer les longueurs et les largeurs des doigts, nous n'avons pas besoin de tous les pixels de l'image, nous avons besoin de localiser seulement les pixels de frontière de notre objet, figure (III.16). Dans notre méthode nous créons une matrice qui contient les coordonnées (lignes et colonnes) de tous les pixels à la frontière (contour) de la main.

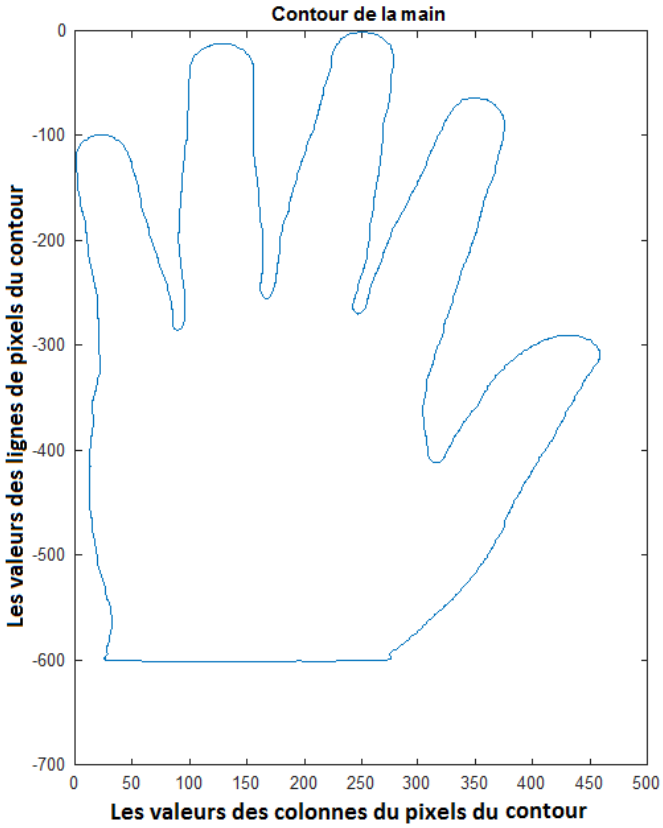

Figure III.16 : Les valeurs de la 2 ieme colonne en fonction des valeurs de 1ère colonne de la matrice de contour.

III.2.4.2 La détection de points de pics et vallées

La matrice créée précédemment, contient Q lignes et 2 colonnes. Q lignes représentent le nombre de pixels du contour et dépend de la taille de la main de l'utilisateur. 2 colonnes représentent les cordonnées (ligne et colonne), respectives, de chaque pixel du contour. Le graph suivant, figure (III.17), représente toutes les valeurs des lignes (Q lignes) de la matrice de contour en fonction des valeurs de la première colonne de la même matrice.

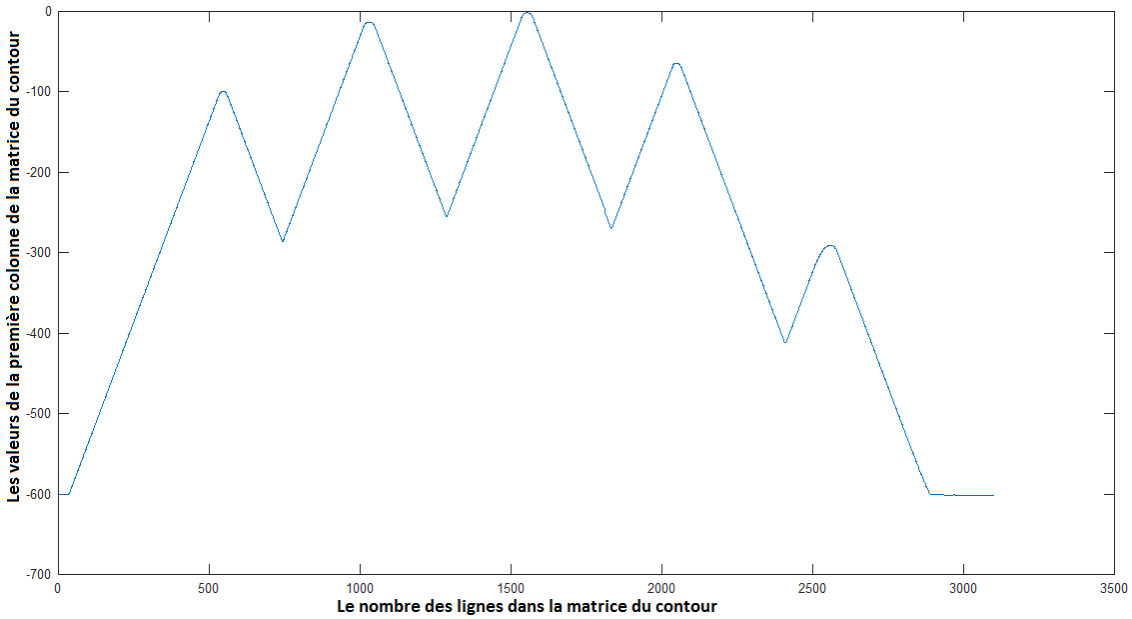

Figure III.17 : Le nombre de pixels du contour en fonction de leurs premières cordonnées (ligne).

La figure (III.17), illustre le pic de chaque doigt (Cinq pics, Cinq doigt) et les vallées entre chaque doigt (Quatre vallées).

III.2.4.3 Calcul de la longueur de chaque doigt

Pour calculer la longueur des doigts, figure (III.19), nous avons ajouté des points supplémentaires (E1 et E2) pour effectuer des mesures précises à partir des points repère (Pics et vallées), figure (III.18). Le nombre de pixels du contour entre P1 et E1 est égale au nombre de pixels entre P1 et V1. Le nombre de pixels du contour entre P4 et E2 est égale au nombre de pixels entre P4 et V3.

Les points de M1, M2, M3, M4 représentent les points milieux entre (E1, V1) et (V1, V2) et (V2, V3) et (V3, E2) respectivement.

Le point milieu ‘M(x, y)’entre deux point ‘p(x_1, y_1)’ et ‘q(x_2, y_2)’ est donné par l’équation (III.2) :

$$M = \left(\frac{x_1+x_2}{2}, \frac{y_1+y_2}{2}\right) \qquad \text{(III.2)}$$

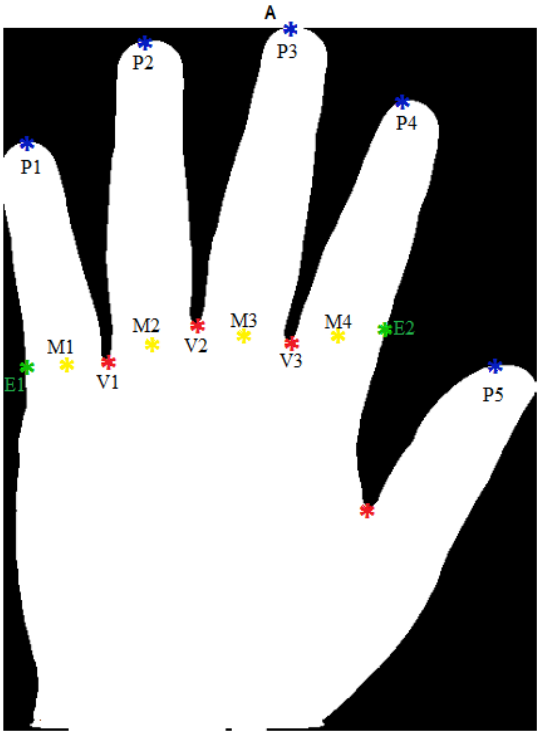

Figure III.18 : Les points supplémentaires sur l'image binaire.

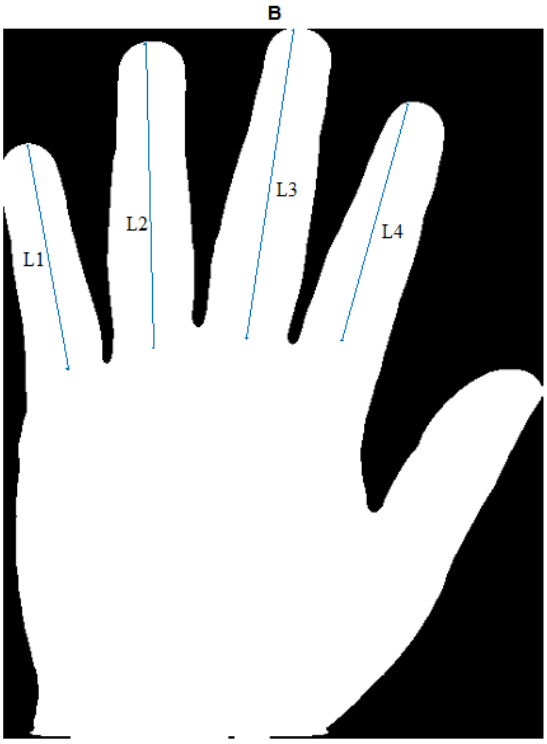

Figure III.19 : Les longueurs de doigts.

L1 représente la distance entre P1 et M1, et L2 représente la distance entre P2 et M2

L3 représente la distance entre P3 et M3, et L4 représente la distance entre P4 et M4

Nous avons utilisé la formule (III.3) pour le calcul de la distance euclidienne entre deux points p (x_1, y_1) et q (x_2, y_2) dans un espace à deux dimensions

$$d(p,q) = \sqrt{((x_2 - x_1)^2 + (y_2 - y_1)^2)} \qquad \text{(III.3).}$$

III.2.4.4 Calcul de la largeur des doigts à des places différentes

Pour calculer la largeur des doigts à des places différentes, nous avons créé d'autres points supplémentaires à partir des points de repère (points pics et vallées), comme le montre la figure (III.20).

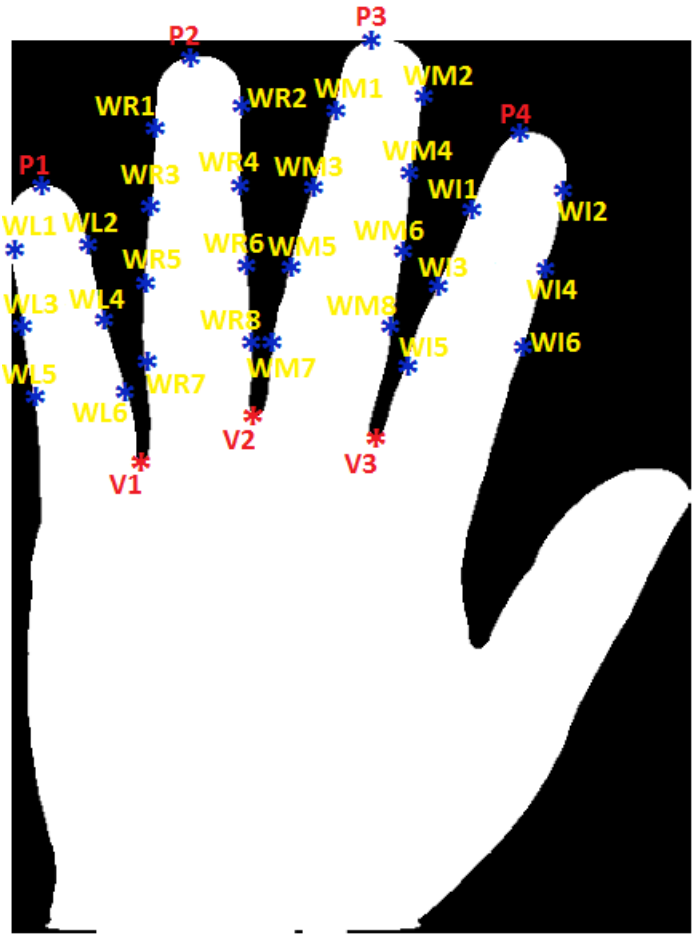

Figure III.20 : Les points supplémentaires pour calculer les largeurs.

Procédure : pour l'auriculaire, nous avons divisé la portion du contour entre (P1, V1) en trois, alors le nombre de pixel entre (P1, WL2) est égale au nombre de pixels entre (P1, WL1). Même chose entre (P1, WL4) et (P1, WL3), et entre (P1, WL6) et (P1, WL5).

La procédure se répète pour les autres doigts, à noter que nous avons divisé l'annulaire et le majeur en quatre portions, et l'auriculaire et l'index en trois portions.

Nous avons utilisé l'équation (III.3), pour calculer la distance euclidienne entre deux points, alors on a :

Les largeurs mesurées pour l'auriculaire :

WL12 = d(WL1, WL2), WL34 = d(WL3, WL4), WL56 = d(WL5, WL6).

Les largeurs mesurées pour l'annulaire :

WR12 = d(WR1, WR2), WR34 = d(WR3, WR4), WR56 = d(WR5, WR6).

WR78 = d(WR7, WR8).

Les largeurs mesurées pour le majeur :

WM12 = d(WM1, WM2), WM34 = d(WM3, WM4), WM56 = d(WM5, WM6).

WM78 = d(WM7, WM8).

Les largeurs mesurées pour l'index :

WI12 = d(WI1, WI2), WI34 = d(WI3, WI4), WI56 = d(WI5, WI6).

Nous avons remarqué que nous pouvons travailler sur le nombre des largeurs, pour cela nous avons divisé notre travail en deux expériences.

Groupe N°1 :

Le nombre total des largeurs mesurées dans ce groupe, figure (III.21), est 14 largeurs (3 largeurs pour l'auriculaire, 4 largeurs pour l'annulaire, 4 largeurs pour le majeur, et 3 largeurs pour l'index).

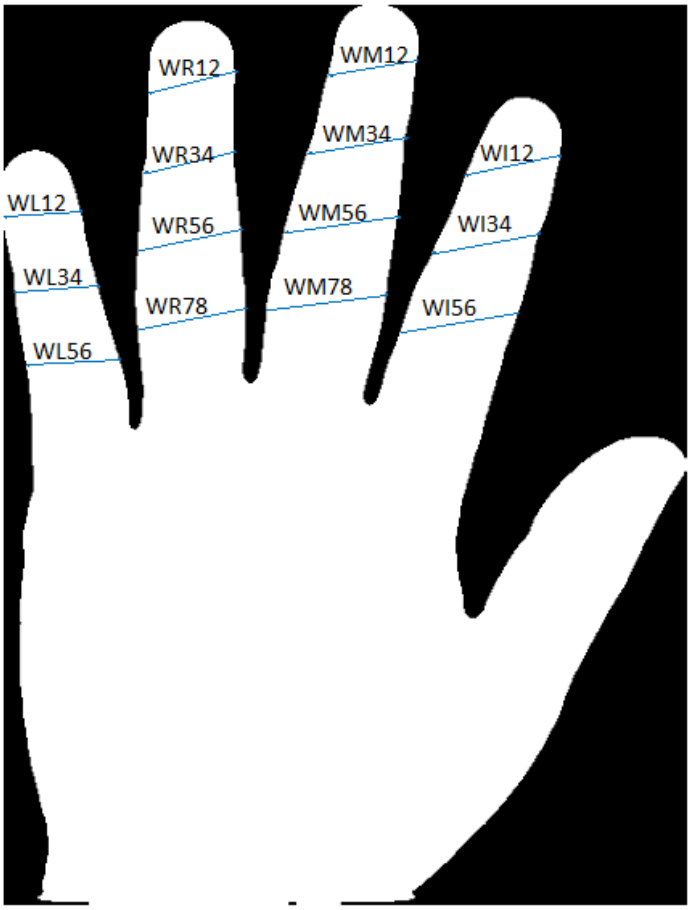

Figure III.21 : Les largeurs des doigts (groupe 1).

Groupe N°2 :

Dans ce groupe, nous avons minimisé le nombre des largeurs mesurées, figure (III.22). Le nombre total des largeurs est 6 largeurs (1 largeurs pour l'auriculaire, 2 largeurs pour l'annulaire, 2 largeurs pour le majeur, et 1 largeurs pour l'index).

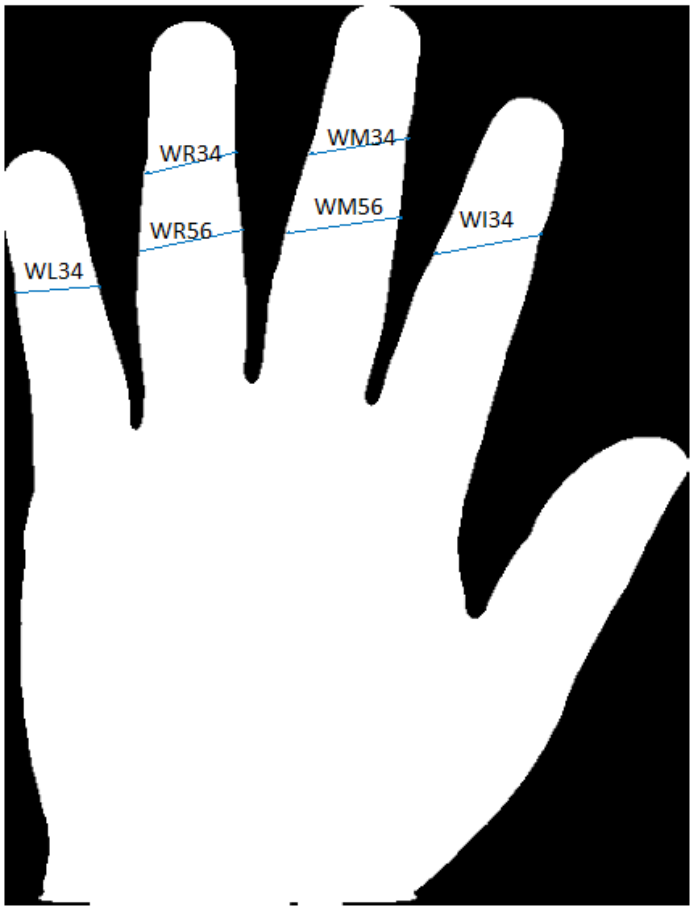

Figure (III.22) : Les largeurs des doigts (groupe 2).

III.2.4.5 Vecteur de caractéristiques discriminatives

Notre système d'identification par géométrie de la main utilise les longueurs des doigts et les largeurs des doigts de la main comme un moyen pour identifier (ou classer) les utilisateurs.

Le vecteur caractéristique de groupe 1 « contient 18 distances » est :

Vecteur_groupe1 = [L1, L2, L3, L4, WL12, WL34, WL56, WR12, WR34, WR56, WR78, WM12, WM34, WM56, WM78, WI12, WI34, WI56] ;

Le vecteur caractéristique de groupe 2 « contient 13 distances » est :

Vecteur_groupe2 = [L1, L2, L3, L4, L3/L1, L2/L4, (L1+L2+L3+L4)/4, WL34, WR34, WR56, WM34, WM56, WI34];

III.2.5 Création de la base de données de Templates

Lors de l'étape d'acquisition, le système prend plusieurs images de la main pour chaque personne. Ces images, de la même personne, sont utilisées pour faire l'enrôlement des utilisateurs dans le système. Les étapes de prétraitement et d'extraction de caractéristiques se répètent pour chaque image de cette personne, qui nous donne plusieurs vecteurs (un vecteur pour chaque image), figure (III.3).

Pour créer un vecteur représentant qui sera utilisé pour l'étape de comparaison, nous avons utilisé la moyenne des vecteurs des images choisi pour l'étape d'enrôlement et le stocker dans la base de données « Base de données de templates ». Ce processus se répète pour chaque utilisateur.

III.3 Phase d'identification

Un système biométrique est comme les autres systèmes d'authentification, dans laquelle un utilisateur authentique doit s'inscrire au système avant l'identification, [7]. Dans la phase d'identification, figure III.23, le système demande à l'utilisateur de fournir une image de sa main droite pour faire l'identification. Le système prétraite l'image sélectionnée, extrait les caractéristiques biométriques et crée un seul vecteur de caractéristiques biométriques. Ensuite, le système compare ce vecteur avec tous les vecteurs (templates) enregistrés dans la base de données des templates. Finalement il prend une décision selon un seuil prédéfini pour accepter ou rejeter cet utilisateur.

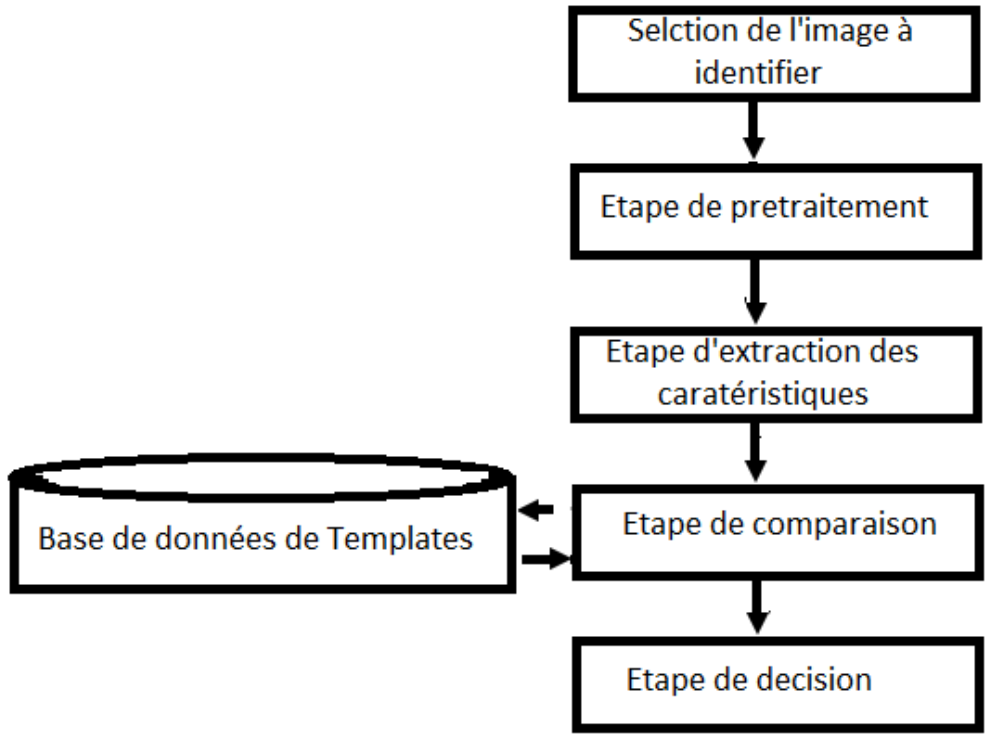

Figure III.23 : Schéma synoptique du processus d'identification.

III.3.1 Etape de comparaison

Pour autoriser un utilisateur, le système compare les données biométriques du prétendant avec les modèles (Templates) dans la base de données des templates. Des fonctions de similarité sont utilisées dans le processus de la comparaison pour aider à différencier (ou classifier) les personnes autorisées et non autorisées. Nous avons choisi de classifier les utilisateurs avec la fonction de distance euclidienne (équation III.4).

La Distance euclidienne, est donnée par l'équation suivante :

$$d = \sqrt{\sum_{i=1}^{L}(t_i - x_i)^2} \qquad \text{(III.4).}$$

Où 'L' est la dimension du vecteur de caractéristique, x_i est la i^{ième} composante du vecteur de caractéristique du prétendant, et t_i est le la i^{ième} composante du vecteur de caractéristiques du modèle (template).

Même dans les meilleures conditions, il ne peut pas être prévu que les caractéristiques obtenues de l'utilisateur à identifier correspondent exactement avec les caractéristiques de son

template (du même individu). Pour cela, le minimum de la distance euclidienne représente la meilleure similarité.

III.3.3 Etape de décision

Si on laisse le système calculer le minimum de la distance euclidienne des caractéristiques biométriques du prétendant avec les templates des utilisateurs enregistrés dans la base, le système va accepter toute personne comme un utilisateur enregistré.

Pour limiter l'accès aux utilisateurs enregistrés, nous avons utilisé un seuil, le seuil est déterminé à partir des différentes images de test (seuil optimale). Si la distance minimale est inférieure au seuil, le système déclare que le prétendant est un utilisateur enregistré dans la base. Si la distance minimale est supérieure au seuil, le système déclare que le prétendant n'est pas enregistré dans la base.

III.4 Conclusion

Dans ce chapitre, nous avons présenté l'extraction des caractéristiques biométriques des individus (longueur et largeur des doigts). Nous avons conclu que la détection des points de repère n'est jamais succédée, si nous n'avons pas pris en compte les conditions choisies lors de l'étape d'acquisition et de binarisation. Nous avons utilisé le minimum de la distance euclidienne comme outil de mesure de similarité entre deux vecteurs. Cette méthode de classification est simple (pas de complexité), rapide (temps de traitement court) et donne des résultats précis.

Résultats et Interprétations

IV.1 Introduction

Les performances du système proposé sont évaluées sur la base d'images que nous avons créée, voir description de la base dans le paragraphe (III.2.2). Les images sont acquises par un scanneur de bureau, Il n'y a pas des chevilles (pegs) pour guider la pose de la main, mais les doigts sont éloignés les uns des autres.

Dix images par personne, nous avons mis 5 images de chaque personne pour la phase de l'enrôlement et les autres cinq pour tester les performances (taux de faux rejetés). Nous avons mis une autre base, nommée base de données des imposteurs, qui contient 15 images (5 images par personne) pour tester les performances (taux de faux acceptés).

IV.2 Résultats

IV.2.1 Expérience 1

Tester les performances du système avec les caractéristiques extraites (groupe 1).

Vecteur_groupe1 = [L1, L2, L3, L4, WL12, WL34, WL56, WR12, WR34, WR56, WR78, WM12, WM34, WM56, WM78, WI12, WI34, WI56] ;

Après l'étape de l'enrôlement des utilisateurs authentiques avec les caractéristiques biométriques du groupe 1 (Vecteur_groupe1), nous avons varié le seuil à des valeurs descendantes pour voir comment le système réagit (accepté ou rejeté l'utilisateur) avec les images de tests des utilisateurs authentiques. Par l'utilisation de la formule (II.3), nous avons obtenu le tableau (IV.1) (Seuil, TFR (%)). Nous avons fait la même chose pour tester le système avec les imposteurs avec la formule (II.4), et nous avons obtenu le tableau (IV.1) (Seuil, TFA (%)).

Tableau IV.1 : Les performances mesurées (TFR et TFA) à différentes valeurs de seuil pour les caractéristiques biométriques de groupe 1.

N° d'essai	Seuil	TFR (%)	TFA (%)	N° d'essai	Seuil	TFR (%)	TFA (%)
01	22	0	100	**12**	11	30	0
02	21	1,66	93, 33	**13**	10	33,33	0
03	20	1,66	86,66	**14**	09	45	0
04	19	5	73,33	**15**	08	56,66	0
05	18	5	66,66	**16**	07	71,66	0
06	17	5	33,33	**17**	06	83,33	0
07	16	6,66	26,66	**18**	05	96,66	0
08	15	10	26,66	**19**	04	96,66	0
09	14	15	26,66	**20**	03	98,33	0
10	13	18,33	26,66	**21**	02	100	0
11	12	25	6,66				

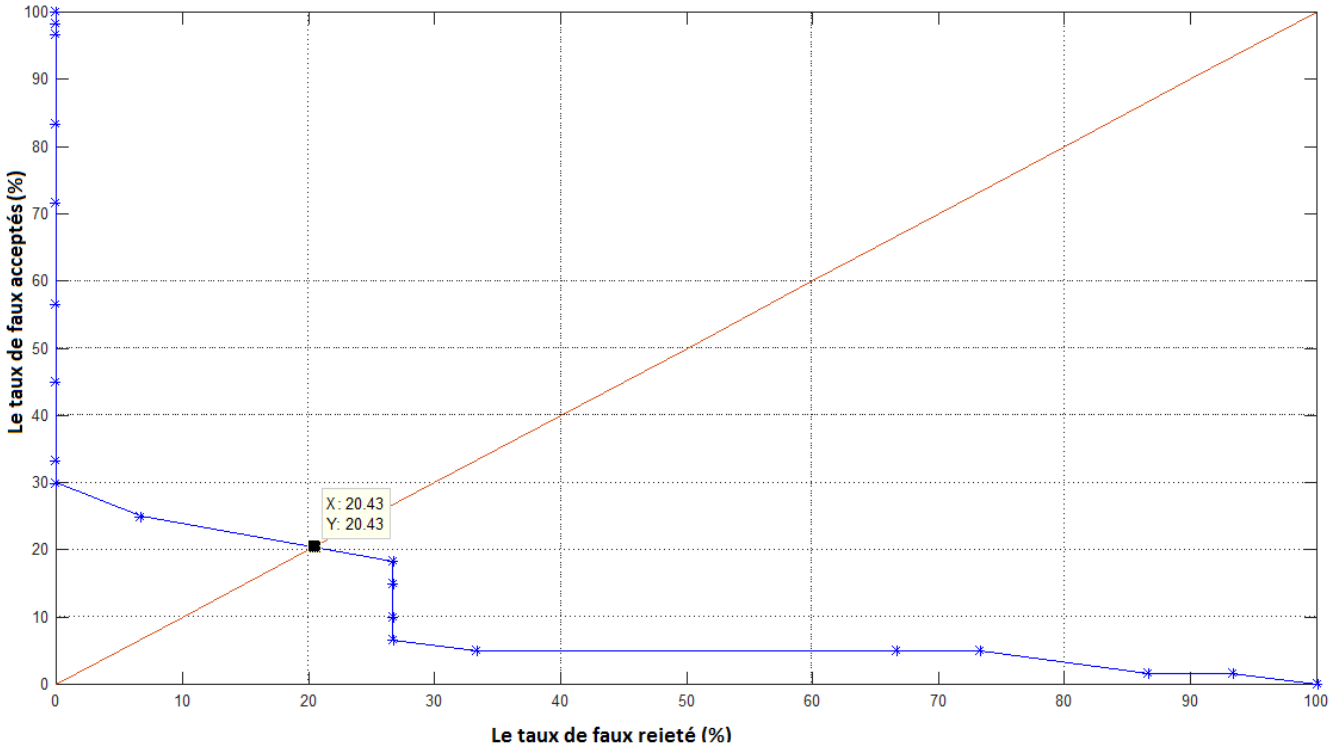

Figure IV.1 : Courbe ROC de groupe 1.

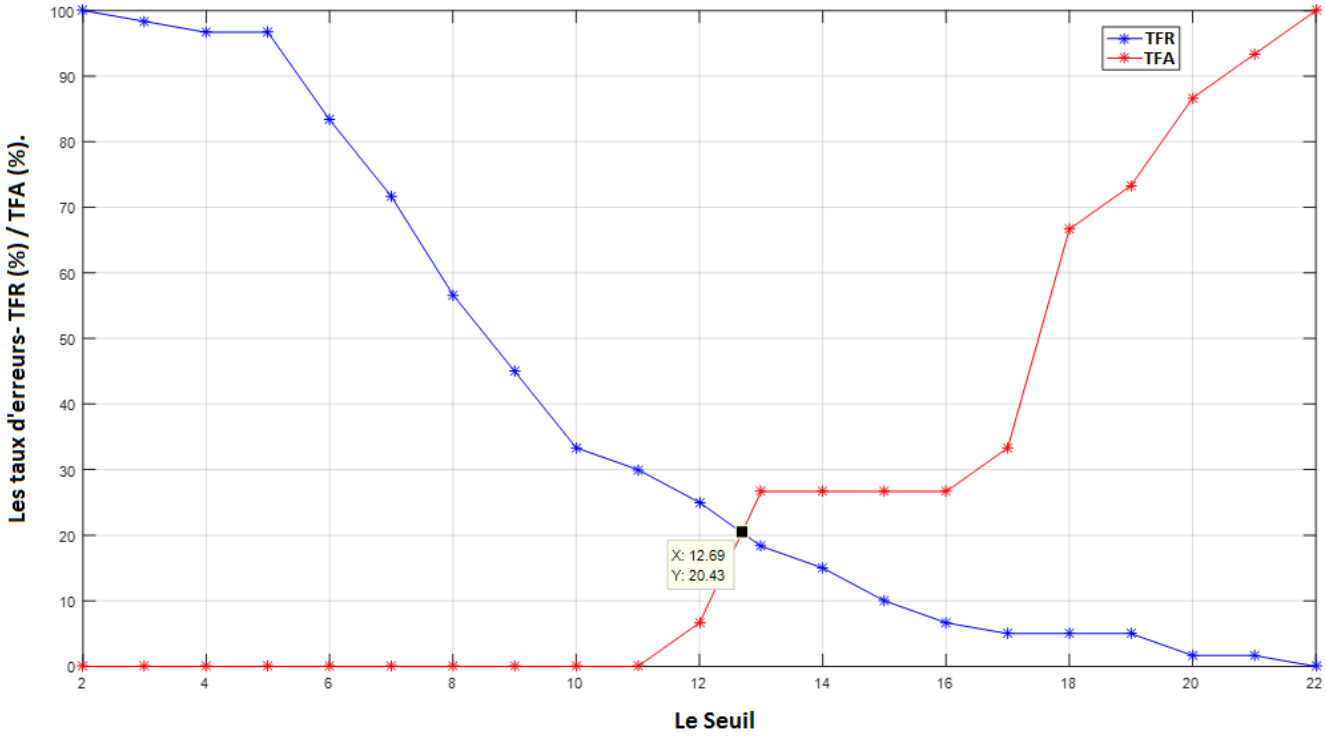

Figure IV.2 : La courbe TFR et TFA de groupe 1.

A partir de la courbe ROC du groupe 1 (figure IV.1), nous avons obtenu la valeur du taux d'égale erreur (TEE) ou TFR = TFA, TEE = 20,43 % ; et à partir de la courbe TFR et TFA du groupe 1 (figure IV.2), nous avons obtenu un seuil de 12,69. Le seuil $Seuil_{TEE} = 13$, est fixé à cette valeur qui est optimale pour ce système en utilisant les caractéristiques biométriques du groupe 1.

Nous pouvons calculer le taux d'identification à cette valeur de seuil pour les utilisateurs authentiques, nous avons fixé le seuil à 13 dans notre programme et avec la formule (II.5) nous avons obtenu :

49 utilisateurs authentiques ont été correctement identifiés parmi 60 images des utilisateurs authentiques réservées pour la phase de test.

$$TI_{Seuil=13} = \frac{49}{60} \times 100 = 81{,}66\ \%$$

Nous donnons ci-après un exemple d'un essai d'identification avec un utilisateur authentique. Nous avons fixé le seuil à 13 et nous avons choisi l'image d'un utilisateur (figure IV.3):

Figure IV.3 : Image test à identifier.

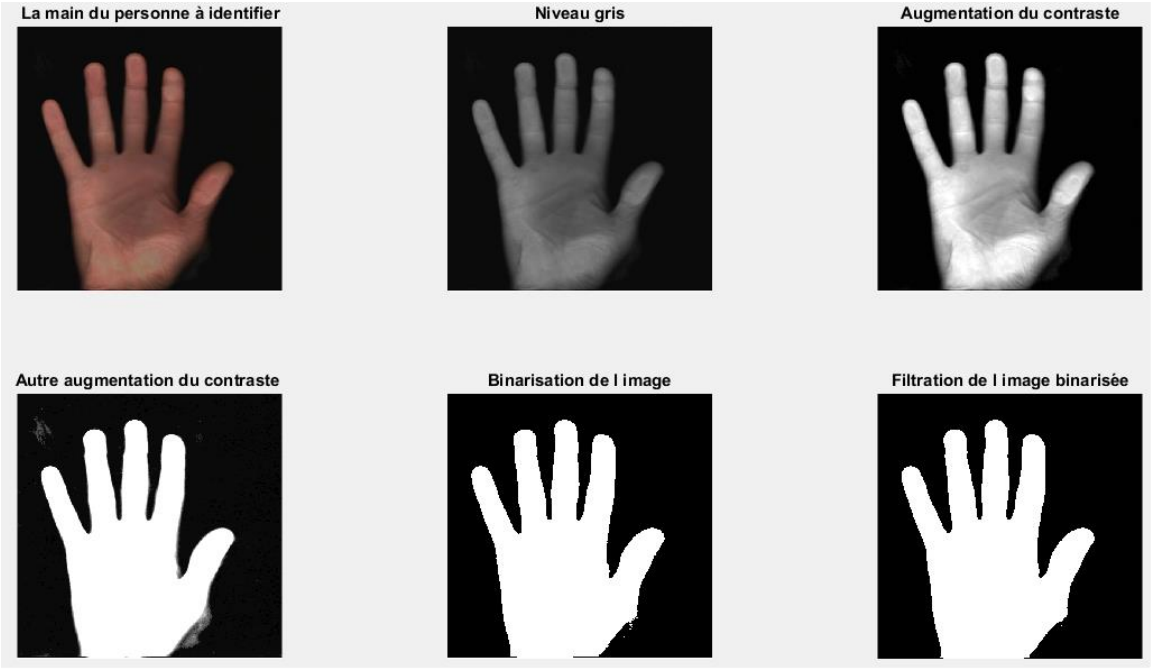

Figure IV.4 : Prétraitement de l'image à identifier.

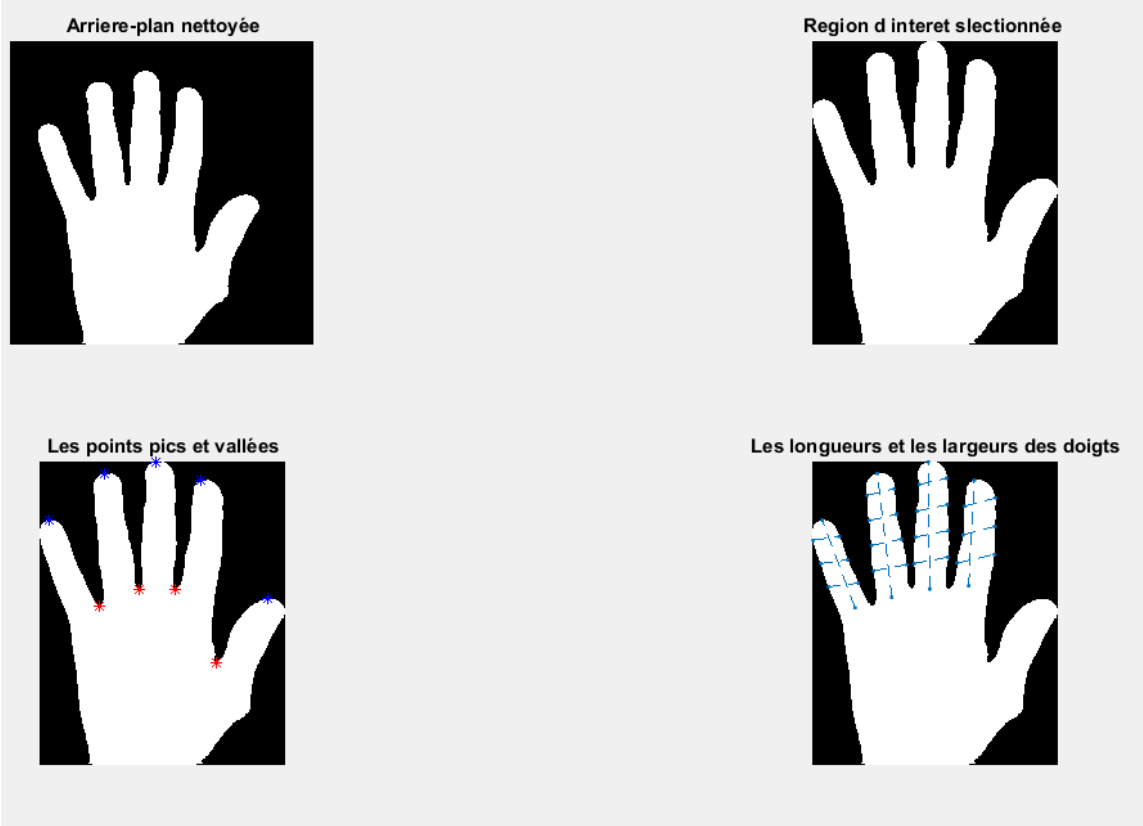

Figure IV.5 : Extraction des caractéristiques (groupe 1).

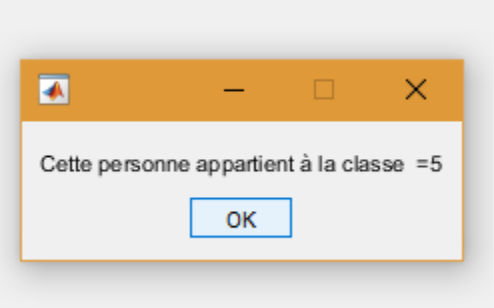

Figure IV.6 : La décision du système.

IV.2.2 Expérience 2

Tester la performance du système avec les caractéristiques extraites (groupe 2). Vecteur_groupe2 = [L1, L2, L3, L4, L3/L1, L2/L4, (L1+L2+L3+L4)/4, WL34, WR34, WR56, WM34, WM56, WI34];

Après l'étape de l'enrôlement des utilisateurs authentiques avec les caractéristiques biométriques du groupe 2 (Vecteur_groupe2), nous avons varié le seuil à des valeurs descendantes pour voir comment le système réagit (accepté ou rejeté

l'utilisateur) avec les images tests des utilisateurs authentiques. Par l'utilisation de la formule (II.3), nous avons obtenu le tableau (IV.2) (Seuil, TFR (%)). Nous avons fait la même chose pour tester le système avec les imposteurs avec la formule (II.4), et nous avons obtenu le tableau (IV.2) (Seuil, TFA (%)).

Tableau IV.2 : Les performances mesurées (TFR et TFA) à différentes valeurs de seuil pour les caractéristiques biométriques du groupe 2.

N° d'essai	Seuil	TFR (%)	TFA (%)	N° d'essai	Seuil	TFR (%)	TFA (%)
01	20	0	100	**11**	10	26,66	20
02	19	0	93,33	**12**	09	35	0
03	18	0	80	**13**	08	43,33	0
04	17	0	80	**14**	07	50	0
05	16	1,66	66,66	**15**	06	63,33	0
06	15	5	40	**16**	05	80	0
07	14	6,66	33,33	**17**	04	90	0
08	13	10	26,66	**18**	03	98,33	0
09	12	15	26,66	**19**	02	100	0
10	11	20	20				

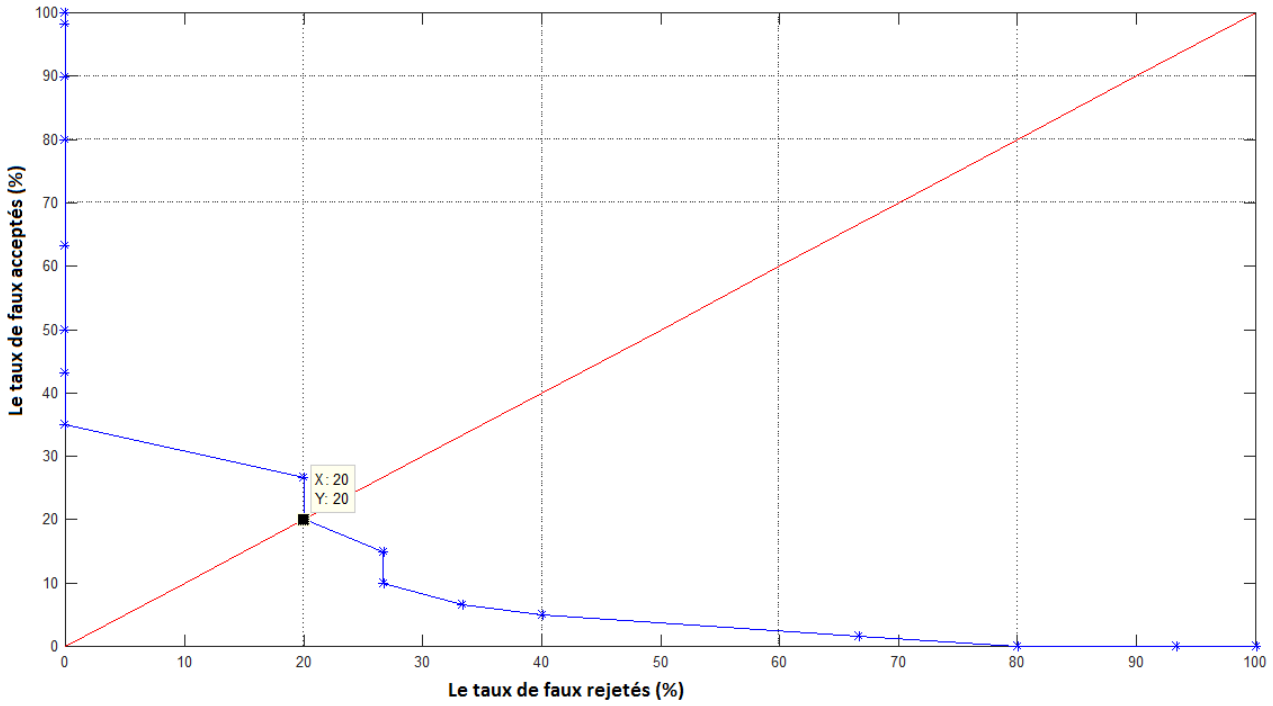

Figure IV.7 : Courbe ROC de groupe 2.

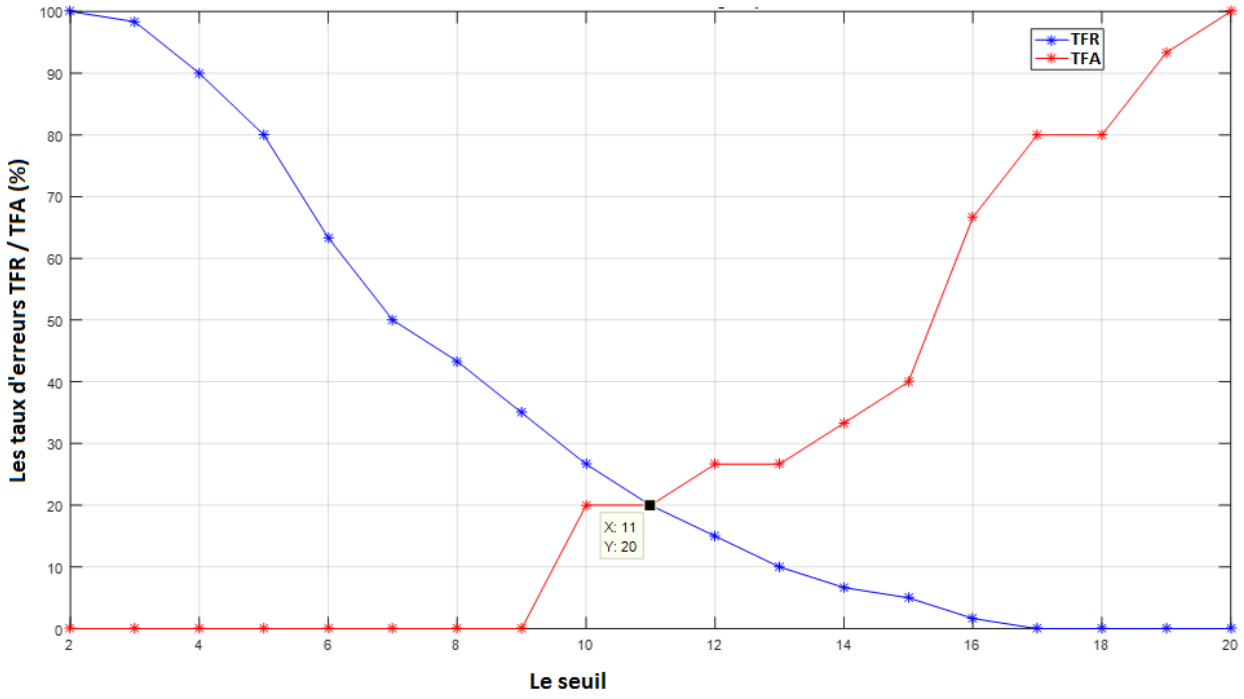

Figure IV.8 : La courbe TFR et TFA du groupe 2.

A partir de la courbe ROC du groupe 2 (figure IV.7), nous avons obtenu la valeur de taux d'égale erreur (TEE) ou TFR = TFA, TEE = 20 % ; et à partir de la courbe TFR et TFA du groupe 2 (figure IV.8), nous avons obtenu un seuil égal à 11. Nous avons fixé le $Seuil_{TEE} = 11$, qui est une valeur optimale pour ce système d'identification en utilisant les caractéristiques biométriques du groupe 2.

Nous pouvons calculer le taux d'identification à cette valeur de seuil pour les utilisateurs authentiques. Nous avons fixé le seul à 11 dans notre programme et avec la formule (II.5) nous avons obtenu :

48 utilisateurs authentiques ont été correctement identifié parmi 60 images des utilisateurs authentiques réservées pour la phase de test.

$$TI_{Seuil=11} = \frac{48}{60} \times 100 = 80\ \%$$

Les résultats suivants donnent un exemple d'un essai d'identification avec un imposteur, le seuil est fixé à 11 et nous avons choisi l'image de l'imposteur illustré en figure IV.9:

Figure IV.9 : Image d'un imposteur à tester.

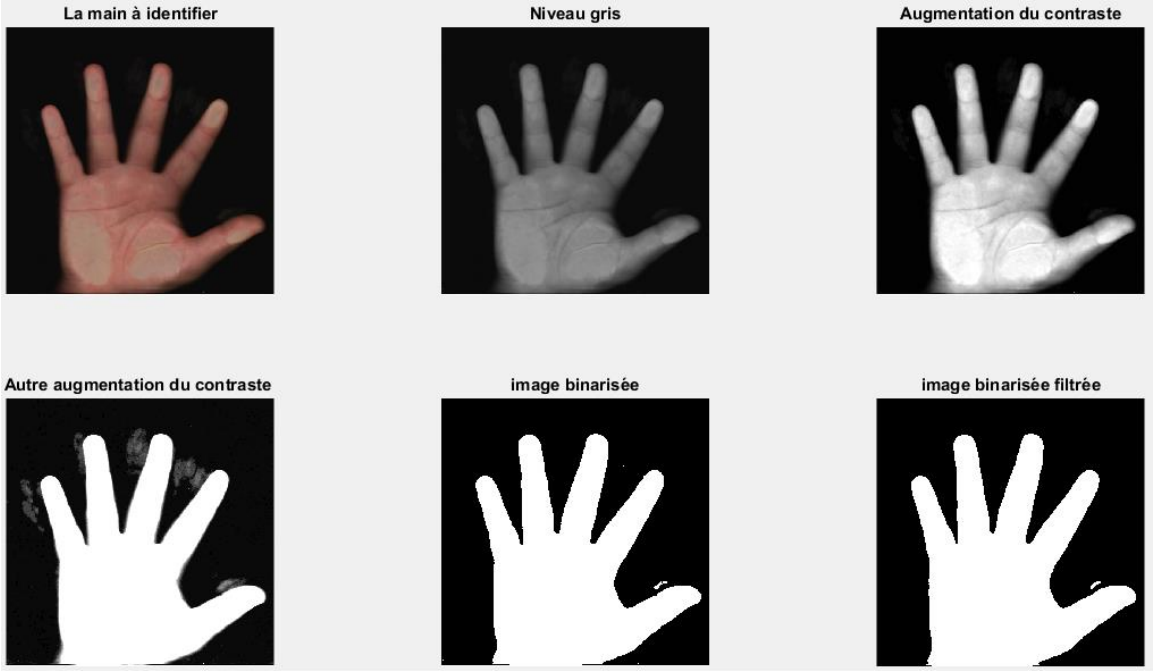

Figure IV.10 : Prétraitement de l'image à identifier.

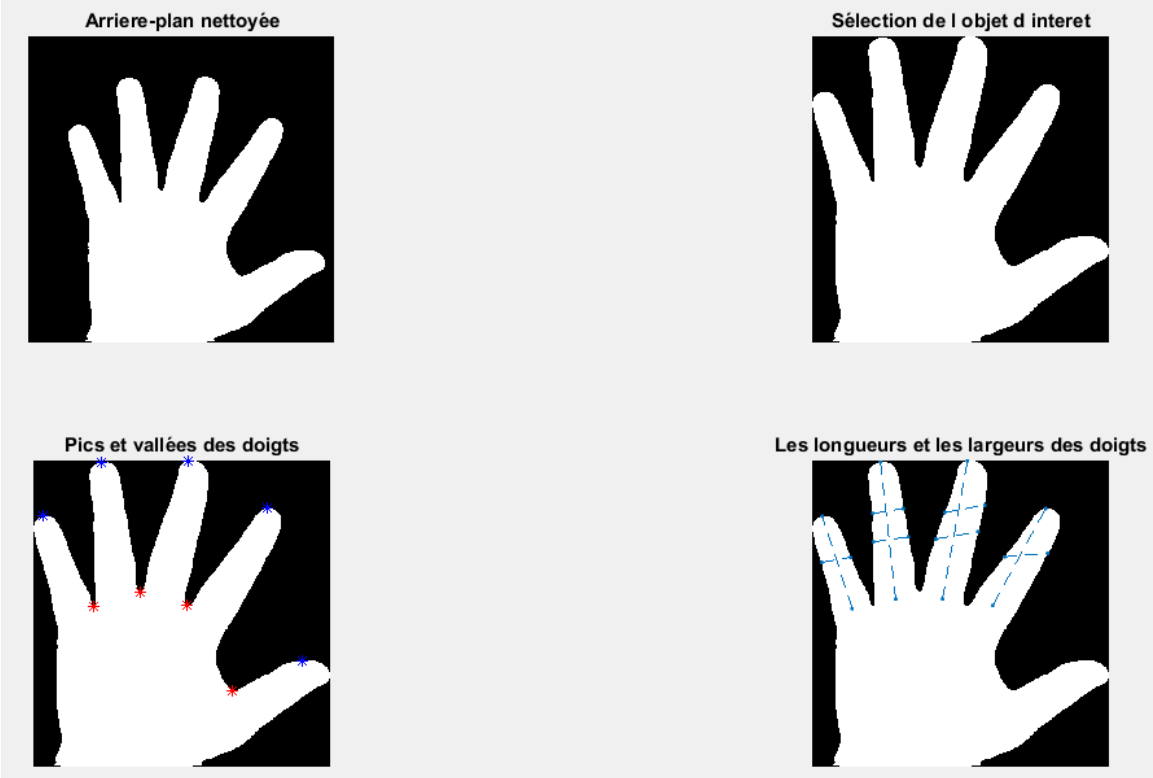

Figure IV.11 : Extraction des caractéristiques (groupe 2).

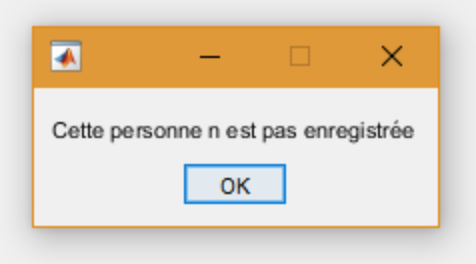

Figure IV.12 : La décision du système.

IV.3 Interprétation

Nous avons réalisé un système d'identification biométrique par la géométrie de la main développé sous MATLAB R2016a, et nous avons appliqué ce système sur une base d'images des utilisateurs (Totale : 120 images).

Le système a identifié 80 % des utilisateurs dans la base. Le système mesure les longueurs et les largeurs des doigts et les utilisent comme (caractéristiques biométriques) un moyen de discrimination. L'expérience 1 et 2 donnent à peu près le même taux d'identification.

Pour la comparaison entre l'expérience 1 et 2 :

Vecteur_groupe1 = [L1, L2, L3, L4, WL12, WL34, WL56, WR12, WR34, WR56, WR78, WM12, WM34, WM56, WM78, WI12, WI34, WI56] ;

Vecteur_groupe2 = [L1, L2, L3, L4, L3/L1, L2/L4, (L1+L2+L3+L4)/4, WL34, WR34, WR56, WM34, WM56, WI34];

Nous pouvons remarquer à partir de ces deux vecteurs, que les longueurs des doigts sont plus discriminatives que leurs largeurs. Ceci à cause de la pression des doigts appliquée par les utilisateurs lors de l'étape d'acquisition.

IV.4 Conclusion

Dans ce chapitre, nous avons mesuré les taux de faux rejetés et acceptés à différentes valeurs de seuil, et nous avons calculé le taux d'identification à la valeur de seuil optimale pour deux expériences. Nous avons conclu qu'à partir des résultats obtenus, les caractéristiques biométriques se distinguent entre elles et chacun a un degré de discrimination. Ainsi, les longueurs des doigts sont plus discriminatives que les largeurs.

Conclusion Générale

Nous avons réalisé un système biométrique d'identification par la géométrie de la main développé sous MATLAB R2016a. Nous avons utilisé les longueurs et les largeurs des doigts comme caractéristiques biométriques. Nous avons utilisé le minimum de la distance euclidienne comme outil de classification qui est simple, rapide et donne des résultats précis. Nous avons appliqué ce système sur une base d'images des utilisateurs que nous avons créée nous-mêmes (Totale : 120 images).

L'expérience montre que la mesure des caractéristiques géométriques (longueurs et largeurs des doigts) de la main à partir des points de repère (point pics et vallées des doigts) peut générer des caractéristiques discriminantes, et chacune de ces caractéristiques possède un degré de discrimination. Ainsi, l'expérience montre que les longueurs des doigts de la main sont plus discriminatives que les largeurs.

Après avoir effectué des expériences sur notre système, nous avons conclu que la géométrie de la main peut être utilisée comme une bonne technique pour la vérification d'identité et non pas pour l'identification. Par ailleurs, les systèmes d'identification par la géométrie de la main sont adaptés seulement dans des applications à petite échelle et de niveau de sécurité moyenne et faible.

Ce système utilise la géométrie de la main. La palme et même les empreintes peuvent être extraites de l'image d'entrée. Combinant l'ensemble de ces données biométriques résulterait un système multimodal avec une très grande précision.

Références Bibliographique

[1] I. Benchennane. « Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus ». Thèse de Doctorat, USTOMB, Algérie, 2016.

[2] M. Mohamed El Abed. « Evaluation de systèmes biométriques ». Thèse de Doctorat, Université de Caen Normandie France, 2011.

[3] J. Doublet. « Etude de nouveaux caractères biométriques de la main dans un contexte Télécom ». Thèse de Doctorat, Université de Caen Basse-Normandie France, 2009.

[4] B. Miroslav, P. Grd and T. Fotak. (2012, Nov 28). *New Trends and Developments in Biometrics, Chapter 4: Basic Principles and Trends in Hand Geometry and Hand Shape Biometrics.* [On-line]. Available: http://www.intechopen.com/books/new-trends-and-developments-in-biometrics. [June 2016].

[5] APIS Ltd. Biometric Hand Geometry Reader HandKey II. Internet: http://www.biometria.sk/en/hk2.html. [Sep 2016].

[6] M. P. Dale. « Multimodal Analysis Based On Hand Features ». Thèse de Doctorat, Université de Pune India, 2012.

[7] M. Firas, Z. Salih. (2014, Aug). « Authentication system depend on hand geometry using back propagation neural network ». *International Journal of Information Technology & Business Management*. [On-line]. 28(1). Available: http://www.jitbm.com/JITBM%2028th%20Volume/6zainab.pdf . [June 2016].

[8] H. Matos, H. Oliveira, M. Filipe. « Hand-Geometry based recognition system - a non restricted acquisition approach ». International Conference o n Image Analysis and Recognition, pp.38-45, Aveiro, Portugal, July, 2012.

[9] The MathWorks, Inc. "Documentation". Internet : https://www.mathworks.com/help. [June 2016].

[10] Tutorials point. « Brightness and Contrast ». Internet : https://www.tutorialspoint.com/dip/brightness_and_contrast.htm . [June 2016].

[11] CommentCaMarche. « Etirement de l'histogramme ». Internet : http://www.commentcamarche.net/contents/1216-traitement-d-images. [June 2016].

[12] M. K. Ahuja1, A. Singh. (2015, Mar). « A survey of hand geometry recognition». *International Journal of Advance Research in Computer Science and Management Studies.*[On-line] .3(3). Available: http://www.ijarcsms.com/docs/paper/volume3/issue3/V3I3-0055.pdf. [Mar 2016].

[13] Christopher. "Méthode d'OTSU". Internet: https://sites.google.com/site/lizantchristopher/services/binarisation-1. [Sep 2016].

[14] C.Solomon, T. Breckon. (2011). *Fundamentals of Digital Image Processing.* [On-line]. Available: http://onlinelibrary.wiley.com/book/10.1002/9780470689776 [August 2016].